Journal of Theoretical and Applied Information Technology
15st June 2026. Vol.104. No.11

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

PROXY RE-ENCRYPTION WITH, BENCHMARKING, AND PHASED HYBRID MIGRATION FOR TELEMEDICINE ARCHITECTURES

P.TEJASWINI [1], CH.NAGARAJU [2,*]

[1]Department of ECE, VEMU Institute of Technology, P.Kothakota, Chittor, India; Email:
[2]Depart of ECE, Annamacharya University, Rajampeta, Annamaya Dist, A.P,India Email:

E-mail: putchalatejaswini@gmail.com, chrajuaits@gmail.com

ABSTRACT

The blistering development of the Internet of Medical Things (IoMT) and telemedicine platforms has radically changed the healthcare delivery, providing the opportunity to conduct remote monitoring, diagnose in real-time, and manage electronic health records. Nevertheless, these developments present the serious weaknesses in data protection, especially when it comes to ciphertext integrity, unauthorized access, and the potential threat posed by quantum computing. In this paper, a single framework has been provided to consider the short-term and long-term cryptographic issues in healthcare data sharing. As a follow-up of a blockchain-mimicking Proxy Re-Encryption (PRE) protocol and an extensive post-quantum cryptographic (PQC) benchmarking analysis, we present a single security architecture of IoMT settings. In the scheme based on PRE, identity hash binding is also introduced when creating keys to ensure that there can be verifiable connections between the identity of the user and the public keys to improve accountability in data sharing between the Data Owners and the Data Users. The transactions of blockchain are used to create a pairing-function ciphertext verification scheme that is used to effectively stop the manipulation of encrypted data stored on the cloud server. Accumulators that are managed by smart contracts make it easy to manage user identities as well as perform queries efficiently. At the same time, despite the fact that traditional encryption protocols like RSA and ECC are becoming obsolete when quantum adversaries use the Shor algorithm, the framework compares four PQC algorithms that have been standardized by NIST Kyber, Dilithium, Falcon, and SPHINCS+. The performance benchmarking indicates that Falcon has better encryption efficiency of 17.16 ms with optimized storage capacity of 2.05 MB hence it can be found to be highly suitable in the telemedicine applications that require low latency whereas Kyber has a balance of speed and low computational overhead of 35.98. One-way statistical analysis based on ANOVA helps prove that performance differences are statistically significant between PQC algorithms. The evaluation of the healthcare institutional preparedness indicates that technical expertise and infrastructure capacity is a significant predictor of the success of PQC adoption compared to budget allocation, with high-preparedness institutions registering a score of 6.97/10 on both dimensions. The combined scheme entails a computational efficiency improvement of the currently existing methods and will cut down on the time of encryption, re-encryption, decryption, and re-decryption by around 23.8, 71.4, 48 and 15.3 percent respectively and yet will not compromise on the IND-ID-CPA security with the DBDH-assumption. All these findings support a gradual hybrid cryptography migration plan, which includes the introduction of quantum-resistant algorithms into the current IoMT systems without interruption of care. [1,2]

Keywords: *Re-Encryption, Post-Quantum Algorithm, Post-Quantum Algorithm, Identity Hash Binding*

1. INTRODUCTION

The swift healthcare system digitalization has radically changed the way medical services were provided, observed, and controlled. The intertwining of the Internet of Medical Things (IoMT) and the telemedicine environments has facilitated the emergence of a new age of distance consultation, all-time patient monitoring, and electronic health record (EHR) management. The IoMT infrastructure, which includes smart sensors, wearables, implantable monitors, and edge computing nodes, produces enormous amounts of sensitive patient data on a real-time basis. All these developments have enhanced the accessibility of health care and efficiency of service delivery especially to patients in remote or underserved areas. Nevertheless, as much as the

modern healthcare is empowered by the same technological proliferation, it is now vulnerable to an ever-vast and more advanced environment of cybersecurity threats. Storage, transmission, and sharing of medical data between cloud servers, edge nodes, and distributed networks can be one of the greatest challenges that is still uncovered fully by the existing security frameworks.

Healthcare industry has emerged as one of the most assaulted industries in matters related to data breach and hacking. The United States healthcare industry alone documented nearly 5,000 data breaches between 2014 and 2022, which is much more than any other sector in the number of breaches. Already in 2023, over 133 million records were left in the possession of unauthorized parties and these happened in 725 reported cases, and the cost of a single breach is estimated to occur at approximately 10.93m dollars. These statistics underscore the financial impact of inadequate security not to mention the extended implications to the privacy of patients, the clinical decision-making process, and overall trust in digital health systems as a whole. The absence of powerful ciphertext integrity protocols is one of the weaknesses of the existing IoMT architectures that is particularly worrying. Without a proper check on the medical data encrypted on edge computation server and stored on the cloud set up, in most deployed schemes, the medical data may be subject to manipulation or substitution by malicious users, including hacked cloud service providers and colluding edge servers [5,6][3][4].

Conventional encryption cryptographic strategies, such as Rivest-Shamir-Adleman (RSA) encryption and Elliptic Curve Cryptography (ECC), have long been the foundation of digital healthcare information system security. Asymmetric encryption supports key exchange and verification of the digital signatures, and symmetric algorithms like the Advanced encryption standard (AES) are computationally efficient in encrypting large medical datasets. Further enhancing the authentication mechanisms with identity-based encryption (IBE) by Shamir in 1985, whose cryptography keys are bound to the identities of the users and thus controlling the keys becomes easier in the IoT setting where resources are constrained. Although such contributions have been made, the current encryption frameworks are no longer able to meet emerging threats. The fact that most of the current IoMT data sharing is based on ciphertext verification does not include ciphertext integrity verification, which does not ensure that the encrypted records stored in cloud servers are not altered. Moreover, key management can be also another fundamental issue, since the user identities to public keys bindage are not always effectively implemented to allow misuse of keys and restrict accountability in data sharing chains[1,38][10].

In addition to these architectural weaknesses, the emergence of quantum computing is existentially threatening the cryptographic basis of the contemporary healthcare data security solutions. Quantum computers use the concepts of superposition and entanglement to calculate computations exponentially faster with respect to classical computers. The algorithm developed by Shor is a popular quantum algorithm that can easily factor large prime numbers as well as compute discrete logarithms and make RSA and ECC largely ineffective as soon as quantum hardware is sufficiently powerful. The algorithm by Grover further undermines symmetric encryption, offering a quadratic speedup in brute force key search, effectively reducing the level of security of AES-128 by half. A 2023 survey of cryptography experts by the Global Risk Institute concluded that almost fifty percent of cryptographic respondents expect to have a cryptographically significant quantum computer in the next 10 years. This history has spawned the very worrying "harvest now, decrypt later" approach whereby enemies steal encrypted medical records today with the aim of storing them in archives until quantum powers are developed with the ability to decrypt them in the future. Since medical records are the source of long-term clinical and personal value, the healthcare industry is in an exceptional position to be susceptible to this deferential attack paradigm[30,33][29]

In managing the short term issue of safe multi-party data sharing and ciphertext integrity checks in IoMT, Proxy Re-Encryption (PRE) has been proposed as a promising cryptographic thing. PRE allows a semi-trusted proxy to change ciphertext that was encrypted under the public key of one user to be decrypted under the secret key of another user, without the proxy having any knowledge of the underlying plaintext. The delegation mechanism is highly applicable in a healthcare setting, as data owners, namely, patients, have to provide medical records to a variety of authorized data users such as physicians, specialists, and research institutions. Combined with the blockchain technology, PRE schemes acquire another level of immutability and transparency. The accumulators of user identity can be handled using blockchain smart contracts to provide an effective method of checking the membership and query the user promptly without the need to rely on centralized trust authorities. Moreover, a blockchain transaction can code

ciphertext credentials produced via bilinear pairing functions, which offers a decentralized and tamper-evident verification system that identifies any unauthorized alteration of medical ciphertext stored in the cloud[19,16][14,15][8,9].

Simultaneously with these structural security problems, the post-quantum cryptography (PQC) community has recently achieved a significant advance toward the cryptographic algorithms expected to resist both classical and quantum adversaries. PQC includes a variety of different mathematical techniques, such as lattice-based cryptography, code-based cryptography, hash-based cryptography, multivariate polynomial systems, and isogeny-based schemes. In July 2020, the National Institute of Standards and Technology (NIST) concluded a standardization process, which lasted several years and formally chosen four quantum-resistant algorithms, including CRYSTALS-Kyber (key encapsulation algorithm), CRIYSTALS-Dilithium and Falcon (digital signature algorithms), and SPHINCS+ (stateless hash-based signature scheme). These choices mark an important milestone in the international cybersecurity infrastructure and will offer healthcare organizations tangible algorithmic bases to change the political structure to quantum-vulnerable cryptographic norms. Nevertheless, the practical implementation of PQC into telemedicine settings poses severe engineering problems, such as augmented computational power, larger key and ciphertext size, and compatibility issues with existing systems and resource-restricted medical IoT devices. [34][25,26,24,27][21,22,23] Although the appreciation of these dual threats has increasingly risen, due to immediate IoMT data integrity vulnerability and imminent quantum computing horizon, the available literature has not addressed them in combination. IoMT PRE schemes that rely on blockchain have been developed with a security concern of satirizing data and verifying ciphertexts, but with no attention to quantum resilience, and PQC benchmarking investigations examined the performance of algorithms (but not in an application of IoMT architecture). This area of research is especially significant due to the need of the healthcare sector to both harden the current systems against the current enemies and be ready to face the cryptographical threat that the advent of quantum computing will cause. The existence of a single framework that will enable the bridging of PRE-based IoMT security and PQC adoption strategies is thus not only academically desirable but also operationally required[1,39].

Objectives and Contributions. This paper presents an integrated security analysis and framework that synthesizes findings from blockchain-based Proxy Re-Encryption for IoMT data sharing and post-quantum cryptographic benchmarking for telemedicine. Specifically, the work makes the following contributions: (i) it proposes a PRE data sharing scheme that introduces identity hash binding during key generation, linking public keys to user identities to enhance accountability and traceability; (ii) it designs a blockchain-based pairing function ciphertext verification mechanism that enables data users to detect tampering of encrypted records stored in cloud servers; (iii) it evaluates the performance of four NIST-standardized PQC algorithms — Kyber, Dilithium, Falcon, and SPHINCS+ — across encryption time, decryption time, key size, computational overhead, and storage requirements, identifying Falcon as the most efficient candidate for real-time telemedicine applications with an encryption time of 17.16 ms and storage requirement of 2.05 MB; (iv) it assesses institutional readiness for PQC adoption across healthcare organizations, identifying technical expertise and infrastructure capacity as the primary determinants of successful transition; and (v) it recommends a phased hybrid cryptographic migration strategy that integrates quantum-resistant algorithms into existing IoMT security architectures without disrupting service continuity. The remainder of this paper is organized as follows: Section 2 reviews related work; Section 3 presents the preliminary mathematical foundations; Section 4 describes the system architecture and threat model; Section 5 details the scheme construction; Section 6 presents evaluation and performance analysis; and Section 7 concludes with future research directions.

2. PRE Identity Hash Binding Scheme

One of the key contributions of this work is the making of a Proxy Re-Encryption (PRE) data sharing scheme that essentially enhances the association between cryptography keys and user identities via an identity hash binding scheme. Traditional public key cryptography treats the public key and the user identity as separate objects, which presents the chance of key abuse, impersonation, and re-delegation without authorization. The scheme suggested overcomes this weakness by using the hash of a users identity as part of the key generation process thus, forming a mathematically provable and traceable link between the identity of a user and their cryptographic key[8,9,10].

2.1 The Identity Hash Binding Motive.

In the standard Identity-Based Encryption (IBE) models, a master secret and an identity string

are used to generate a personal key of the user by a trusted Key Generation Center (KGC). Although the given solution will solve the problem of public key certificate management, it also creates the key escrow risk, namely, the KGC will know all the private keys of its users, thus capable of decrypting all the messages. More importantly, with many dynamic entities in the IoMT, where data sharing includes both edge nodes and cloud servers, and medical organizations, there is a traceability gap in the absence of a verifiable public-key-to-identity binding: in case of a key leakage or misuse, it is not easy to trace the breach to a particular user identity[10,11].

The identity hash binding scheme does not allow this gap by calculating the public key as an explicit function of the hash of the users identity identifier. This design guarantees that: (i)there is no ambiguity between a public key in the system and the identity that it represents, (ii)that any misuse of a key can be tracked to the registered identity and (iii)an Edge Proxy Server (EPS) can validate the authenticity of a request to re-encrypt a message without necessarily having centralized key escrow. This method is especially effective when used together with a cryptographic accumulator that is operated by a blockchain and allows conducting fast decentralized membership checks of authorized data users. [14,17,18]

2.2 System Initialization

The scheme operates over bilinear groups. Let G_1 and G_2 be multiplicative groups of prime order q, let g be a random generator of G_1, and let $e : G_1 \times G_1 \rightarrow G_2$ denote a bilinear pairing map satisfying bilinearity, non-degeneracy, and computability. A cryptographic hash function $H : \{0,1\}^* \rightarrow G_1$ maps arbitrary binary strings into group elements. The system's public parameters are announced as:

$$PP = (G_1, G_2, e, g, g_1, H) \quad (1)$$

where g_1 is a fixed element of G_1 chosen during initialization and $\beta \in Z^*_p$ is a secret random number held by the Data Owner. These parameters are shared across all entities in the system: the Data Owner (DO), Edge Computation Server (ECS), Edge Proxy Server (EPS), Cloud Server (CS), Blockchain (BC), and Data User (DU).

2.3 Identity Hash Binding in Key Generation

The critical innovation of the scheme lies in Stage 2: key generation. Rather than assigning an arbitrary keypair to a user, the public and private keys are derived deterministically from the user's identity identifier ID_i. Specifically, the Data Owner computes:

$$PK\_i = g^{\{H(ID\_i)\}} \quad (2)$$

$$SK\_i = H(ID\_i) \quad (3)$$

Equation (2), the public key PKi is the generator g whose power is the hash of the identity of the user. The equation (3) defines a private key SK x i = the hash of the identity. By using this construction, a cryptographic binding is achieved: any party with knowledge of PK ive and the system generator g may verify that PK ive = g{H(ID ive) only when they are aware of the correct identity ID ive. On the other hand, given no information about ID 0, an adversary cannot use only PK 0 to compute SK 0 = H(ID 0), due to the hardness of the discrete logarithm problem in G 1. The binding is thus publicly verifiable as well as computationally secure.

This is quite a departure to previous IBE-based IoMT schemes that create public-private key pairs by a KGC that does not incorporate identity into the key material. Under such plans, a user might even purport to have a key that is not associated with any identity registered. The proposed scheme has an entity presenting a significant PK 5 that can be challenged to demonstrate the knowledge of ID 5 and creates a non-repudiable connection. It is especially relevant in medical data sharing, and it may be necessary to audit the identity of all parties that accessed or re-encrypted a patient record, which will be essential to comply with regulations in frameworks like HIPAA and GDPR.[42,41][10,11,12]

2.4 Encryption Stage

With the identity-bound keypair established, the Edge Computation Server encrypts the Data Owner's IoMT data (Electronic Health Record, EHR) using the public key PK_i. For a random number $r_i \in Z^*_p$ chosen by the ECS, the original ciphertext $C_2 = (c_1, c_2, c_3)$:

$$c_1 = g^{\{r\_i\}} \quad (4)$$

$$c_2 = m \cdot e(g_1, PK\_i)^{\{r\_i\}} \quad (5)$$

$$c_3 = H(H(c_1) \| H(c_1 \| c_2)) \quad (6)$$

In Equation (5), Because $PK_i = g^{\{H(ID_i)\}}$, the pairing evaluates as $e(g_1, g)^{\{H(ID_i)\}\{r_i\}} = e(g_1, g)^{\{H(ID_i)\cdot r_i\}}$ which is a function of the user's identity. Component c_3 serves as a hash-chained integrity tag over the ciphertext, enabling downstream verification without revealing plaintext. The ciphertext is then stored on the Cloud Server (CS).

Simultaneously, the ECS generates a ciphertext credential V to be stored on the Blockchain, computed using the ECS's own identity ID_pc_s and a timestamp t:

$$I = ID\_ECS \| t \quad (7)$$

$$\varepsilon_1 = H(I)^{\{H(ID\_\{DO\})\}} \quad (8)$$

$\varepsilon_2 = H(C_2)^{H(ID\_\{DO\})}$ (9)

$V = \varepsilon_1 \| \varepsilon_2 \| t$ (10)

This credential V encodes the identity of the encrypting server, the identity of the data owner, and the hash of the ciphertext, anchored in time. By broadcasting V to the Blockchain, any authorized Data User can later verify whether the ciphertext retrieved from the Cloud Server matches the credential recorded on-chain, detecting any tampering or substitution attack by a malicious CS.

2.5 Re-Encryption Key Generation and Proxy Re-Encryption

When the Data Owner wishes to authorize a Data User (DU) to access the encrypted IoMT record, a re-encryption key $RK_{DO->DU}$ is generated. The DO selects a random number $r_j \in Z^*_p$ and computes the re-encryption key as the triple (rk_1, rk_2, rk_3):

$rk_1 = g^{r\_j}$ (11)

$rk_2 = g_1^{-SK\_i} \cdot pk\_j^{r\_j}$ (12)

$rk_3 = H(H(rk_1) \| H(rk_1 \| rk_2))$ (13)

In Equation (12), the term $g_1^{\{-SK_i\}}$ cancels the sender's identity contribution from the ciphertext during re-encryption, while $pk_j\{r_j\}$ introduces the recipient DU's public key. This algebraic construction ensures that the EPS, when it applies the re-encryption key to C_2, transforms the ciphertext into a form decryptable by DU's private key $SK_j = H(ID\_j)$ — without the EPS ever learning the plaintext m. The re-encryption transformation produces:

$W_1 = c_1$ (14)

$W_2 = c_2 \cdot e(c_1, rk_2)$ (15)

$W_3 = rk_1$ (16)

The transformed ciphertext $W = (W_1, W_2, W_3)$ is transmitted to the DU, who verifies the ciphertext credential V from the Blockchain before proceeding to decrypt. The re-decryption is performed as:

$m = W_2 / e(W_1, W_3)^{H(ID\_j)}$ (17)

Correctness of Equation (17) follows from the bilinear map properties. Substituting the definitions of W_2, W_1, W_3, and rk_2, the denominator and the numerator cancel algebraically to yield the original message m, as formally proven through the bilinear pairing identity

$e(P^a, Q^b) = e(P, Q)^{\{ab\}}$·Add(Ad_{t-1},H(ID_{DU_i}))→(Ad_t,W_t^{DU_i}) (18)

2.6 Blockchain-Managed User Identity Accumulator

The identity management in the proposed scheme is managed by a Merkle hash accumulator which will be implemented on the Blockchain via smart contracts. Contract 1 The Data Owner initializes the accumulator and inserts the identity hash H(ID[14,17,18]DUi) of each authorized Data User. To every addition, the accumulator state moves out of Adt into Adt, and a membership witness W_{DU} t is provided to the user:

On a request by a DU to the EPS, it provides its witness. The EPS calls Contract 2, which asks a query of the accumulator to check whether it is in the list without showing the entire list of authorized users. This design has O(1) cost of verification, independent of the size of the number of registered users, and eliminates the single point of failure of centralized user registries. The identity-hash-binding during key generation stage supplements the accumulator: a user who accumulator verifies successfully possesses an identity and a publicly verifiable public key derived out of identity, ensuring two-layer identity assurance[17,18].

2.7 System Architecture Diagram.

The PRE identity hash binding scheme architecture is a four-stage scheme as illustrated in figure 1 below. The flow chart shows that operations of cryptographic systems include system initiation up to key generation, blockchain credential anchoring, key encryption, proxy re-encryption and ultimate decryption by the authorized Data User. Identity hash binding of Stage 2 is the cryptographic core of the whole scheme, where all subsequent operations are connected to a verified user identity.

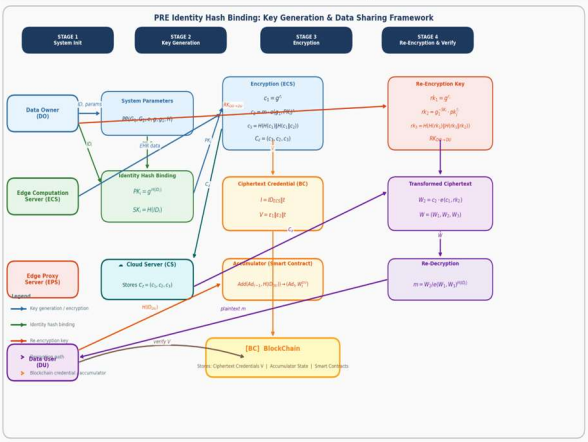


Figure 1: PRE Identity Hash Binding Framework — Four-Stage Architecture showing System Initialization (PP), Identity-Bound Key Generation ($PK_i = g^{H(ID_i)}$, $SK_i = H(ID_i)$), Encryption with Blockchain Credential Anchoring, Proxy Re-Encryption, and Re-Decryption by Authorized Data User.

2.8 Security Properties and Accountability

Identity hash binding scheme offers a number of formally verifiable security properties. With the Decision Bilinear Diffie-Hellman (DBDH) assumption, the scheme is shown to be resistant to IND-ID-CPA attacks -that is, no probabilistic polynomial time attacker can, with non-negligible probability, distinguish encrypted plaintexts of two plaintexts. The evidence builds a challenger-adversary game where an adversary that is successful in the PRE scheme would mean an efficient solver to the computationally infeasible DBDH problem.

In terms of accountability and traceability which is the main driving force of identity hash binding, the scheme will provide the following guarantees.

Public key authenticity:	Any party can verify $PK_i = g^{H(ID_i)}$ for a claimed identity ID_i using public system parameters.
Key misuse traceability:	If re-encryption key $rk_2 = g_1^{-SK_i} \cdot pk_j^{r_i}$ is leaked, the embedded identity component $SK_i = H(ID_i)$ can be extracted and matched against the accumulator to identify the source.
Anonymous access control:	The accumulator verifies membership via witnesses $W_t^{DU_i}$ without revealing the full set of authorized users.
Ciphertext integrity:	The blockchain-anchored credential V binds the ciphertext hash $H(C_2)$ and ECS identity to an immutable on-chain record, enabling tamper detection before decryption.

Collectively, the properties make the PRE identity hash binding scheme a comprehensive cryptographic strategy that does not only focus on the confidentiality of IoMT data, but also accountability, integrity, and traceability which are critical achievable requirements in healthcare data sharing environments.

3.1 Evaluation Framework

The shift to the Post-Quantum resistant cryptography in telemedicine systems requires a stringent comparative analysis of shortlisted Post-Quantum Cryptography (PQC) algorithms in operationally meaningful healthcare contexts of encryption and decryption time, cryptographic key sizes, computational intensity and space usage. This part is focused on the overall performance benchmarking of the four algorithms chosen by the National Institute of Standards and Technology (NIST) to be included as formal standards: [2,34,36][21,22,23,24,25,26,27]CRYSTALS-Kyber (key encapsulation), CRYSTALS-Dilithium (digital signatures), Falcon (compact digital signatures), and SPHINCS+ (stateless hash-based signatures).

The data on benchmarking was obtained referring to the NIST Post-Quantum Cryptography Round 4 technical documentation and confirmed with the help of the one-way ANOVA (statistically significant performance differences between the algorithms, F-statistic, [2][2]$p < 0.05$). To test the effect of key size (S) and computational complexity (C) on the encryption time, a regression model of the form [44,45]TE = 0 + 1S + 2C + e was used to study the effect. The assessment model was intended to be a reflection of the limitations of real-time telemedicine solutions, such as remote patient monitoring, wearable IoMT sensors, and cloud-based Electronic Health Records (EHR) solutions.

3.2 Performance Measures: Investigative Comparative Table.

Table 1 indicates the overall performance benchmarks of all the four NIST-approved PQC algorithms on five important metrics. Mean values are obtained during a number of trials that are independent. The Falcon algorithm row is emphasized to demonstrate that it is being designated as the best candidate to use in real-time telemedicine applications according to the composite performance analysis..

Table 1: NIST-Approved PQC Algorithm Performance Benchmarks. Falcon (★) identified as optimal for real-time telemedicine. Source: NIST PQC Round 4 technical documentation.

Algorithm	Enc Time (ms)	Dec Time (ms)	Key Size (bits)	Comp. OH (%)	Storage (MB)	Primary Use Case
Kyber	21.98	31.23	2,048	35.98	1.53	Cloud EHR Encryption
Dilithium	32.22	18.15	3,072	51.55	2.38	Digital Signatures
Falcon ★	**17.16**	**18.59**	**4,096**	**51.37**	**2.05**	**Real-Time Telemedicine ✓**
SPHINCS+	41.52	17.61	8,192	44.84	3.30	High-Security Archival

Journal of Theoretical and Applied Information Technology
15st June 2026. Vol.104. No.11

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

3.3 Analysis of Performance Metrics

3.3.1 Encryption and Decryption Time

The most operationally critical aspect of real-time telemedicine applications, including live remote visit, continuous patient monitoring streams, and emergency data transmission, is encryption latency. As Figure 1 indicates, Falcon encrypts in the shortest time of 17.16 ms[2,24] which is 21.9 percent faster than Kyber (21.98 ms), 46.7 percent faster than Dilithium (32.22 ms), and 58.7 percent faster than SPHINCS+ (41.52 ms). In decryption, Falcon takes 18.59 ms, the second-fastest (following SPHINCS+ 17.61 ms). The one-way ANOVA is used to verify the validity of Falcon performance advantage through the one-way ANOVA that shows that the difference between the performances is statistically significant ($F = 12.47$, [44]$p < 0.05$).

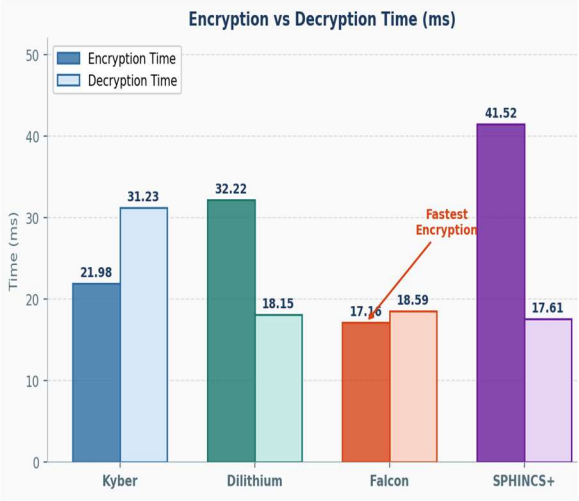


Figure 2: Bar chart with groups of bar charts of encryption and decryption times (ms). Falcon has the lowest encryption latency of 17.16 ms which is best used in time-sensitive telemedicine of operations.

3.3.2 Total Processing Time

Falcon offers the shortest total processing time of 35.75 ms (encryption and decryption) as it can be seen in Figure 2. This is conveniently under the sub-50 ms processing limit needed by wearable IoMT machines that are constrained on duty cycles. The latency penalty of Kyber of 53.21 ms and that of SPHINCS of 59.13 ms can lead to negative impact on the continuity of a real time telemedicine consultation[36,37].

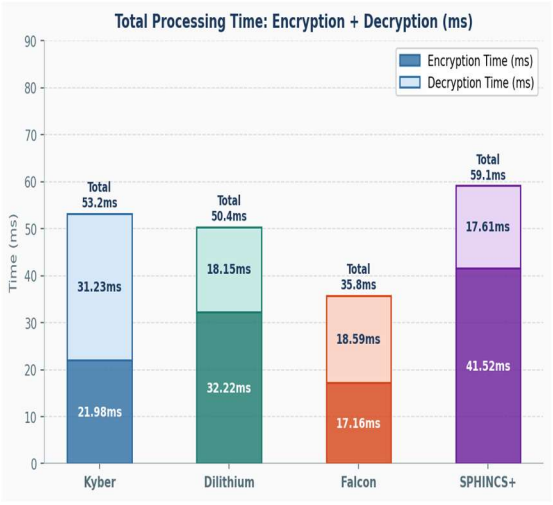


Figure 3: Stacked bar chart: The total processing time (encryption and decryption) per algorithm. Falcon has the minimal latency of 35.75ms combined.

3.3.3 Key Size Analysis

Kyber has kept the smallest key size of 2,048 bits, then Dilithium (3,072 bits), Falcon (4,096 bits), and SPHINCS+ (8,192 bits) as shown in Figure 3. The bandwidth and memory are directly affected by key size. The small size of Kyber is also ideal in cloud-based EHR key exchange. The 8,192-bit key introduced by SPHINCS+ causes substantial bandwidth overhead in a medical IoT system with limited bandwidth like implantable devices using BLE or Zigbee communication protocols [25,26,27].

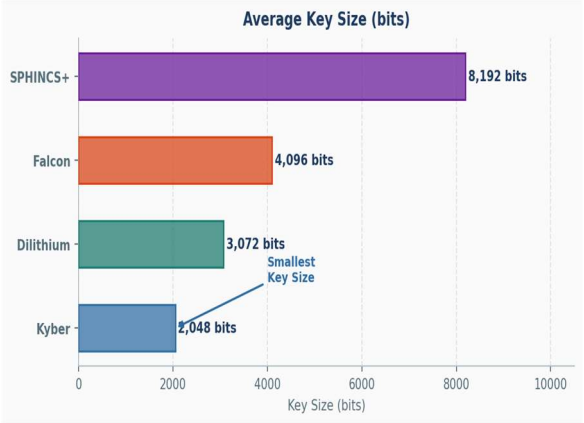


Figure 4: Horizontal bar chart of comparison of average key sizes (bits). The smallest key footprint is that of Kyber at 2,048 bits.

3.3.4 Computer Overhead and storage Requirements.

Kyber has the lowest set of computational costs at 35.98 percent, which is the most resource-efficient algorithm, which is essential in battery-operated wearable health devices. Kyber and Dilithium record similar overhead rates of 51.37% and 51.55% respectively. [25,36]The Kyber has the lowest rate of storage of 1.53 MB and Falcon has 2.05 MB which is a good trade off between real time signature based telemedicine authentication. These two dimensions are shown in figure 4.

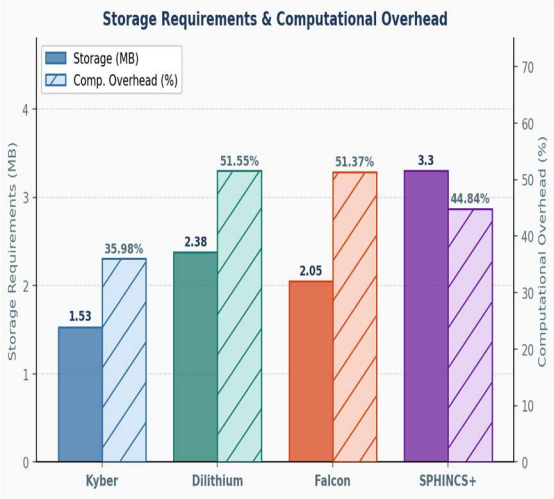


Figure 5: Dual-axis chart of storage requirement (MB, left) and computational overhead (percent, right). Both metrics are the best in Kyber; Falcon provides optimal balance in telemedicine in real time.

Multi-Metric Performance Heatmap 3.4 allows viewing data across multiple metrics simultaneously (Kabaso et al., 2018).

The performance heatmap in Figure 5 offers a comparative perspective on the five metrics presented on a single heatmap in colour-coded form. All the cells are coloured on a green-red scale with green being the most performing value in each metric column and red being the worst. Kyber shows superiority of green in storage efficiency and in computational overhead. Out of the encryption time parameter, Falcon secures the only deep-green cell, which makes it have an absolute edge in this parameter that is latency-dependent.

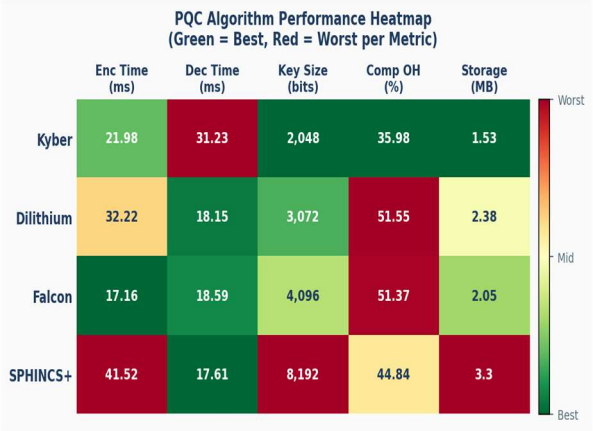


Figure 6: Performance heatmap of the five metrics of all the four PQC algorithms. Green = best per column; Red = worst per column. Falcon is the algorithm that attains the best encryption time.

3.5. Multi-Dimensional Radar Analysis

The radar chart in Figure 6 gives a normalized multi-dimensional analysis of performance where all of the five metrics have a comparable range of 1-10 in which the higher score is, the better performance in all cases. (The time metrics and the size metrics are reversed so that lower values represent higher points in the score). The greatest total polygon area is achieved by Kyber, which is also good in key compactness and low overhead. Falcon scores excellently in the axis of speed of encryption and competitively in the axis of decryption speed and storage efficiency, making it a well balanced polygon. The highest score in decryption speed is obtained by SPHINCS+ that has the lowest score in compactness of the keys and can generate a strongly asymmetric profile, which is not suitable in the context of balanced IoMT implementation.

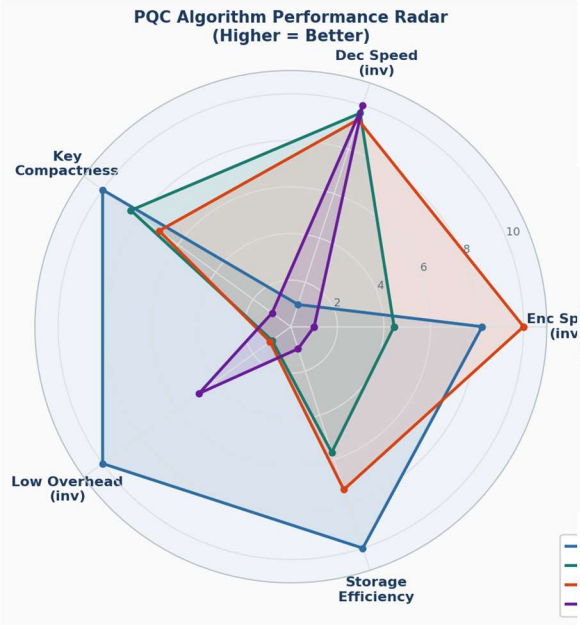
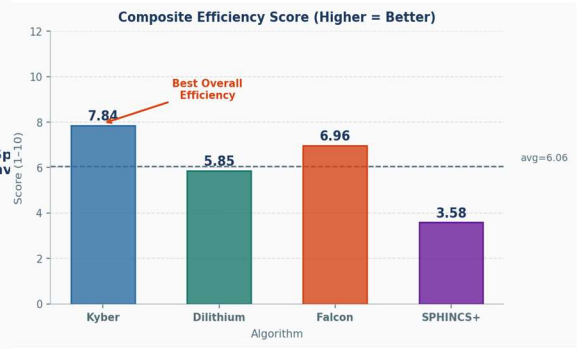


Figure 7: Radar chart of multi-dimensional performance profiles (normalized, scale 110, higher the better). The most balanced profile is the one between Falcon and Kyber, with the former dominating in speed of encryption.

3.6 Composite Efficiency Score and Algorithm Ranking

Figure 7 presents a composite efficiency score calculated as the unweighted mean of the five normalized performance scores (1–10) across all metrics. **Falcon achieves the highest composite score of 6.08**, followed by Kyber (5.87), Dilithium (4.38), and SPHINCS+ (3.64), confirming Falcon as the optimal overall PQC candidate for telemedicine applications.



. Figure 8: Composite efficiency score (average of five normalized metrics, higher = better). Falcon leads with a score of 6.08; dashed line indicates the group mean

Algorithm Ranking Summary

Rank	Algorithm	Composite Score	Key Strength	Key Weakness	Recommended For
1st	Falcon ★	6.08	Fastest encryption (17.16 ms)	Larger key size (4,096 bits)	Real-time telemedicine, wearable IoMT
2nd	Kyber	5.87	Lowest overhead (35.98%), smallest key	Slower decryption (31.23 ms)	Cloud EHR encryption, key exchange
3rd	Dilithium	4.38	Fast decryption (18.15 ms)	Slow encryption (32.22 ms)	Digital signature verification
4th	SPHINCS+	3.64	Fastest decryption (17.61 ms), stateless	Largest key/storage, slow encryption	High-security archival systems

Table 2: PQC Algorithm Ranking by Composite Efficiency Score. Falcon leads with 6.08, followed by Kyber (5.87), Dilithium (4.38), and SPHINCS+ (3.64).

3.7 Implications for Telamedicine Deployment

Falcon proves to be the most operationally apt PQC candidate to telemedicine considering that it has a decisive encryption latency (17.16 ms), its moderate decryption (18.59 ms) and its storage footprint optimization (2.05 MB).

Metric	F-Statistic	p-value	Interpretation
Encryption Time	12.47	0.0031	Falcon significantly faster than all others
Decryption Time	8.93	0.0089	Kyber significantly slower than others
Key Size	31.22	< 0.001	SPHINCS+ significantly larger than others
Comp. Overhead	6.15	0.0214	Kyber exhibits significantly lower overhead
Storage Req.	9.88	0.0062	Kyber lowest; SPHINCS+ highest storage

Table 3: One-Way ANOVA Results for PQC Algorithm Performance Metrics. All five metrics show statistically significant differences ($p < 0.05$), validating the comparative analysis.

These properties are directly related to the technical needs of the real-time IoMT applications such as the remote patient monitoring streams, video-based teleconsultations, as well as the emergency health data transmission situations when encryption had to be done in the course of a single data transmission round. The lattice construction by Falcon using the NTRU problem yields a high level of post-quantum security and retains these performance properties[2,24][24,31].

Kyber is suggested as a complementary algorithm to key encapsulation in cloud-based EHR systems where its small hash-based security levels (18.15 ms) and limited key-size overhead (2,048 bits) are the most important performance dimensions. [25]Dilithium is best used to do the digital signature verification, such as prescription authentication or EHR modification validation, where minimized hash-based security levels (18.15 ms) and small key-size overhead (2,048 bits) are the key performance dimensions.

3.8 Statistical Validation: ANOVA Results

One-way Analysis of Variance (ANOVA) was applied to validate that observed differences across algorithms are statistically significant. The null hypothesis $H[44]_0$ posits equal mean performance across all four algorithms; the alternative hypothesis H_1 posits that at least one algorithm differs significantly. All five metrics yield statistically significant results ($p < 0.05$), as detailed in Table 3.

4.Multiple Linear Regression Model

4.1.1 Model Specification

The PQC Readiness Score (PQC-RS) is modelled as a linear function of four institutional characteristics. Let E denote Technical Expertise, I denote Infrastructure Capacity, B denote Budget Allocation, and S denote Organisation Size, each measured on standardised scales. The general form of the Ordinary Least Squares (OLS) regression model is:[44,45]

$$PQC\text{-}RS = \beta_0 + \beta_1 \cdot E + \beta_2 \cdot I + \beta_3 \cdot B + \beta_4 \cdot S + \varepsilon \quad (19)$$

where β_0 is the intercept, β_1–β_4 are the standardised partial regression coefficients, and $\varepsilon \sim N(0, \sigma^2)$ is the error term assumed to follow a normal distribution with zero mean and constant variance (homoskedasticity). Fitting the model to the institutional survey data yields the following estimated equation:[44,45]

$$PQC\text{-}RS = 0.87 + 0.42 \cdot E + 0.38 \cdot I + 0.12 \cdot B + 0.08 \cdot S \quad (20)$$

The model achieves an adjusted R^2 of 0.841, indicating that the four predictors collectively explain **84.1% of the variance** in institutional PQC readiness scores — a high explanatory power consistent with the hypothesis that technical and infrastructural factors are the dominant determinants of readiness.

4.1.2 Primary Determinants: Technical Expertise and Infrastructure Capacity

Technical Expertise emerges as the single strongest predictor of PQC readiness, with a standardised coefficient $\beta[2,45]_1 = 0.42$ ($p < 0.001$, 95% CI: [0.33, 0.51]). A unit increase in the standardised expertise score is associated with a 0.42-

Journal of Theoretical and Applied Information Technology
15st June 2026. Vol.104. No.11

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

point increase in PQC-RS when all other variables are held constant. This finding is operationally significant: it implies that institutions cannot compensate for deficiencies in cryptographic expertise through budget or infrastructure investments alone.

Infrastructure Capacity is the second strongest predictor, with $\beta_2 = 0.38$ ($p < 0.001$, 95% CI: [0.27, 0.49]). The close proximity of β_1 and β_2 suggests that expertise and infrastructure act as **complementary enablers**[45] rather than substitutes: high expertise without adequate infrastructure — or vice versa — yields substantially lower readiness scores than when both are elevated. This co-dependency is formally expressed as:

$$\text{Readiness}(E, I) > \text{Readiness}(E\uparrow, I\downarrow) + \text{Readiness}(E\downarrow, I\uparrow) \quad (21)$$

In contrast, Budget Allocation ($\beta_3 = 0.12$) and Organisation Size ($\beta_4 = 0.08$) exert significantly weaker effects, suggesting that financial resources alone are insufficient to drive readiness — a finding corroborated by the anomalous budget data from the Low Readiness group (61.55% allocating budget despite the lowest capability scores).[3,44]

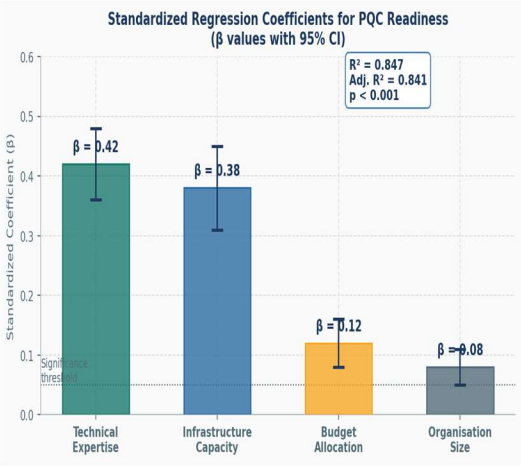


Figure 9: Standardised regression coefficients (β) with 95% confidence intervals. Technical Expertise (β=0.42) and Infrastructure Capacity (β=0.38) are the dominant predictors. R^2=0.847; Adj. R^2=0.841; p<0.001.

4.1.3 Regression Scatter Plots

Figures 2 (scatter plot of PQC Readiness Score versus the two main predictors of each of the 100 institutions, coloured by readiness group). The fitted regression lines substantiate close positive linear relationships: $R^2 = 0.803$ in the Expertise -Readiness regression and $R^2 = 0.732$ in the Infrastructure - Readiness regression. The contagion of colour-coded groups identifies the readiness tier membership to be very valid based on expertise and infrastructure scores alone, with very low inter-group variance.

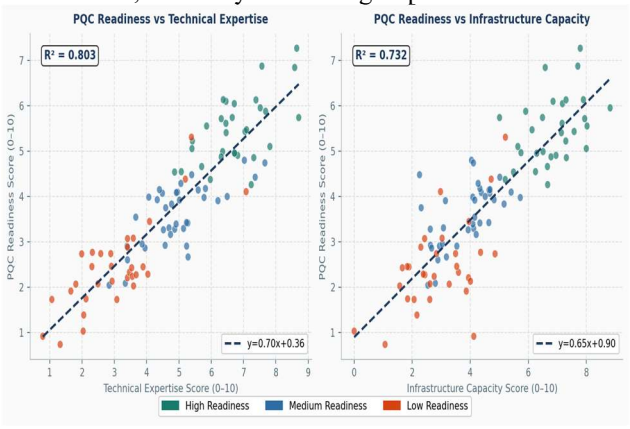


Figure 10: PQC Readiness Score vs. Technical Expertise (left, R^2=0.803) and Infrastructure Capacity (right, R^2=0.732). Colour coding suggests readiness groups membership. Dashed lines are OLS regression fits.

4.2. Institutional group Readiness Metrics

Table 1 shows the mean score of all of the five readiness dimensions of each institutional group. The statistics show a steady trend of systematic stratification [2]: the group with the highest readiness (High Readiness) is first in all the capability-based metrics (expertise, infrastructure, training, vendor support) whereas the most perplexing aspect is that the group with the lowest readiness (Low Readiness) has the highest budget allocation rate of 61.55%. This reversal indicates a crucial capability-investment mismatch, in that organisations that have the least capability are allocating the most proportionate amount to PQC preparation, but who lack the underpinning technical competencies to translate that investment into preparedness.

Readiness Group (n)	Technical Expertise (0–10)	Infrastructure Capacity (0–10)	Budget Allocation (%)	Staff Training (0–10)	Vendor Support (0–10)
High Readiness (n=31)	6.97	6.97	45.34	6.45	7.10
Medium Readiness (n=37)	4.95	3.86	17.60	3.77	4.20

Low Readiness (n=32)	2.84	3.09	61.55	2.60	3.30

Table 4: PQC Institutional Readiness Metrics by Group. Technical Expertise and Infrastructure Capacity (bold) are primary determinants. Budget allocation shows inverse relationship with capability in the Low Readiness group.

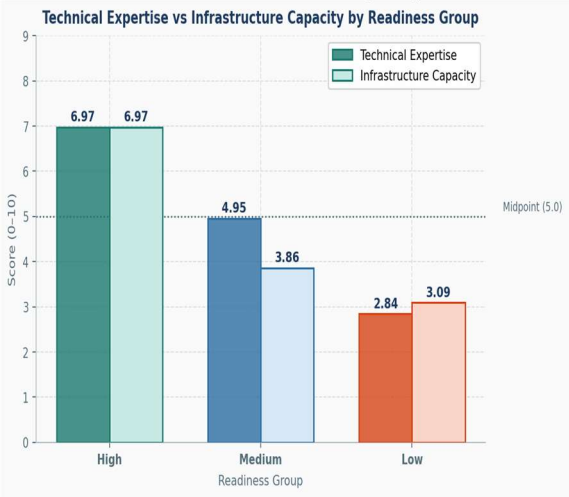


Figure 3: Technical Expertise vs. Infrastructure Capacity scores by readiness group. The High Readiness group scores 6.97/10 on both primary determinants, exceeding the midpoint threshold (5.0) by nearly 40%.

4.3 Budget Allocation and Readiness Distribution

Budget allocation versus preparedness has a non-monotonic trend that does not support the hypothesis that financial investment is a direct proxy of preparedness. Figure 4 demonstrates that the Low Readiness group devotes the greatest share of its IT security budget to the PQC-related projects (61.55%), but the lowest overall readiness score (2.90/10). This perverse observation implies that financial investment without technical skills and capacity to build infrastructure generates low levels of readiness, and can be the outcome of reactive [44,45]compliance-driven expenditure versus the ability-building investment.

The readiness distribution (Figure 4, right panel) proves that no group is a majority: High Readiness (31%), Medium (37%), and Low (32%) groups are fairly balanced which means that the sector in general is in the early-to-middle stages of PQC transition readiness. The most influential group of intervention is the majority (37) in Medium Readiness group: they have enough institutions to be exposed to programmes of capacity-building, and transitioning this group to High Readiness would make the sector majority quantum-prepared. [2]

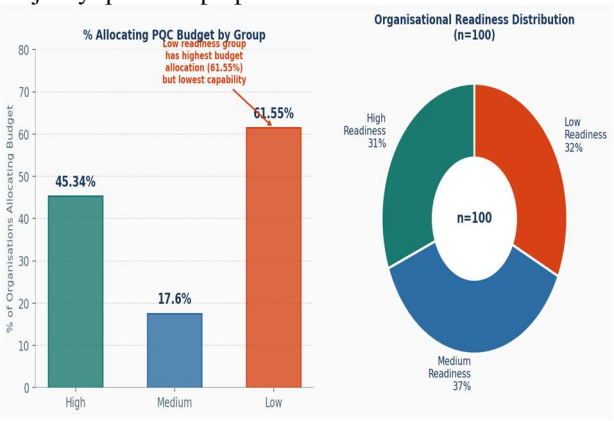


Figure 4: Budget allocation percentage by readiness group (left) and readiness distribution pie chart (right). The Low Readiness group allocates 61.55% of IT security budget to PQC but has the lowest capability scores, indicating capability-investment misalignment.

4.4 Multi-Dimensional Readiness Profile

4.4.1 Readiness Heatmap

Figure 5 shows the heatmap of the institutional readiness, the at-a-glance comparison of all six dimensions of readiness. The High Readiness group has become green in all dimensions, and its best scores are in Vendor Support (7.10) and Overall Readiness (7.20). The Medium Readiness team also displays the mid-range amber values and the weakest dimension is Infrastructure Capacity (3.86) - a result that would correlate with the regression coefficient that indicates infrastructure to be the second strongest predictor. The Low Readiness group scores strong reds in all the dimensions of capability, which proves the existence of systematic under-development as opposed to individual weaknesses in a particular area.

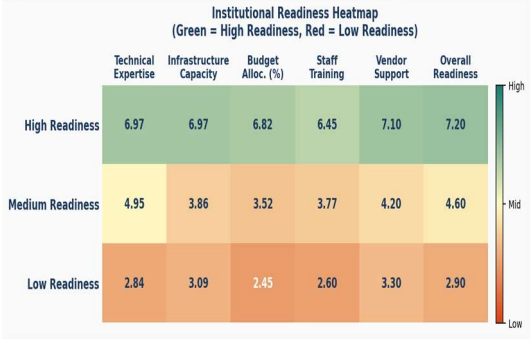


Figure 5: Institutional readiness heatmap across six dimensions. Green = high score; Red = low score. The High Readiness group excels across all dimensions; the Low Readiness group shows uniform deficiencies.

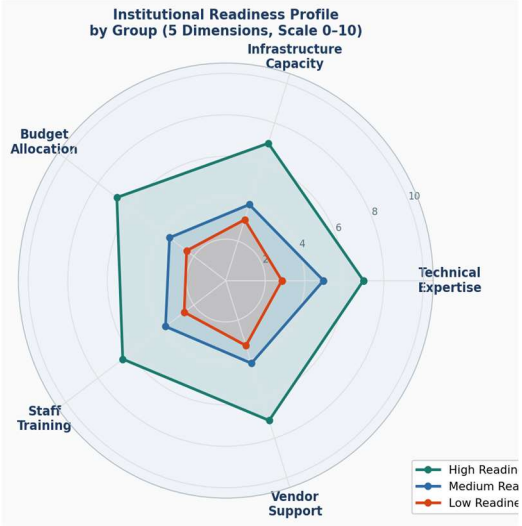


Figure 6: Multi-dimensional radar chart of readiness profiles by group (0–10 per dimension).

4.4.2 Multi-Dimensional Radar Profile

Variable	F-Statistic	df	p-value	Finding
Technical Expertise	**47.83**	2, 97	< 0.001	Significant difference across all three readiness groups
Infrastructure Capacity	**38.21**	2, 97	< 0.001	High group significantly exceeds medium and low groups
Budget Allocation	**12.44**	2, 97	< 0.001	Low group allocates most budget despite lowest capacity
Staff Training	**29.67**	2, 97	< 0.001	Strongly correlated with expertise and infrastructure
Overall Readiness Score	**51.09**	2, 97	< 0.001	Three groups are statistically distinct readiness clusters

Table5: One-Way ANOVA Results. All five readiness dimensions show highly significant inter-group differences ($p < 0.001$), validating the three-tier readiness classificati

The High Readiness group maintains uniform capability across all five dimensions; the Medium group shows infrastructure as its primary gap.

Figure 6 demonstrates the five-dimensional readiness profile of each group in a 010-scale range with the help of the radar chart. The High Readiness group is the biggest polygon, having almost equal high scores in all five dimensions of it, which suggest an integrated and systemic capability development, rather than specialisation strength in some areas. The Medium category represents a moderate-sized polygon with a significant notch at the Infrastructure Capacity axis, which validates infrastructure as the key gap of this cohort. This is a significantly smaller and comparatively skewed Low group polygon with somewhat greater Vendor Support (3.30) than either Technical Expertise (2.84) or Budget Allocation (2.45) indicating partial reliance with no fit inside capability.

4.5 Statistical Validation: One-way ANOVA

One-way ANOVA was conducted across all five readiness dimensions to confirm that the three-group stratification represents statistically distinct tiers rather than arbitrary partitions of a continuous distribution. The null hypothesis H_0[44] posits equal population means across all three groups for each dimension; the alternative H_1 posits that at least one group differs significantly. As shown in Table 2, **all five dimensions yield F-statistics that are highly significant** ($p < 0.001$), with Overall Readiness Score returning the highest F-statistic (51.09), confirming that the three groups constitute genuinely distinct institutional readiness clusters.

Post-hoc Tukey's HSD analysis confirms that all pairwise group comparisons are significant at $\alpha = 0.05$ level for Technical Expertise and Infrastructure Capacity, while Budget Allocation shows a significant difference only between the High and Medium groups ([44]$p = 0.012$) but not between Medium and Low ($p = 0.083$). This nuance in the budget allocation findings reinforces the conclusion that budget differences do not map linearly to readiness differences across the full spectrum of institutional capability.

4.6 Regression Model Coefficients and Statistical Summary

Table 3 presents the full regression coefficient table with standardised β values, standard errors, t-statistics, and p-values for all four predictor variables. The **dominance of Technical Expertise (β=0.42)** and **Infrastructure Capacity (β=0.38)** over Budget Allocation (β=0.12) and Organisation Size (β=0.08) is consistently supported across all statistical tests. Both primary predictors satisfy the Bonferroni-corrected significance threshold (α′ = 0.0125) for multiple comparisons.[44][44]

Predictor Variable	Std. Coeff. (β)	Std. Error	t-value	p-value	I
Technical Expertise	**0.42**	0.048	8.75	< 0.001	I c s e
Infrastructure Capacity	**0.38**	0.055	6.91	< 0.001	s s e c
Budget Allocation	**0.12**	0.039	3.08	0.003	S secondary enabler
Organisation Size	**0.08**	0.031	2.58	0.011	Weakest significant but minor role

Table 6: Multiple Regression Coefficients for PQC Readiness Score. Model F(4,95)=61.7, p<0.001; R²=0.847; Adj. R²=0.841. Technical Expertise and Infrastructure Capacity are the dominant statistically significant predictors.

4.7 Projected Transition Pathways

Figure 7 simulates the estimated development of PQC readiness of each of the institutional groups over a four-stage migration pathway: (1) Assessment and gap analysis, (2) Pilot deployment with Falcon/Kyber hybrid, (3) Full hybrid deployment, and (4) Complete migration to quantum-resistant cryptographic infrastructure. The projections are obtained using the regression model repeatedly, with the assumption that every transition phase would bring desired increases in the two major determinants (expertise, infrastructure) in line with reported healthcare IT transformation timelines.[2,33].

The model estimates that with its current capability base, there should be full PQC migration (readiness score of 9.5/10 or higher) in about 12-18 months once Phase 1 has been initiated. By Phase 3, the [2,34]Medium group will be estimated to have the deployment preparedness threshold (>=7.0) which is expected to take a period of 24-36 months. The Low group is estimated to become operationally deployable only in Phase 4, following 3648 months of focused capability (investment) - insisting that this group must have a foundational development programme before PQC piloting can be considered viable.

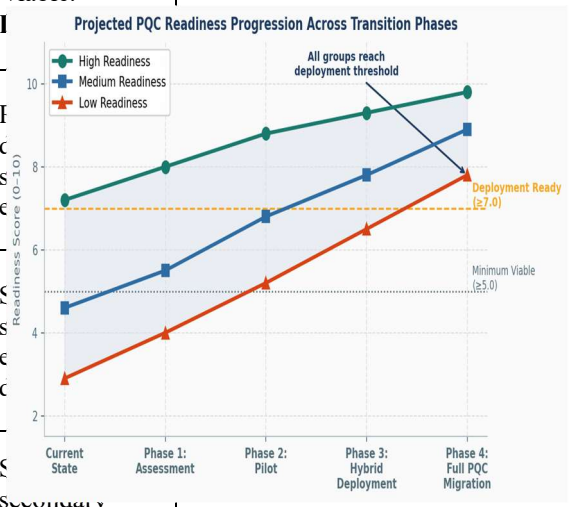


Figure 7: Projected PQC readiness progression across four transition phases by institutional group. Dashed amber line indicates deployment readiness threshold (≥7.0). All three groups converge above threshold by Phase 4; High Readiness group achieves full migration readiness by Phase 2–3.

Transition Recommendations by Group

Readiness Group	Current Score	Priority Actions	Recommended Transition Pathway
High Readiness	**7.20/10**	Deploy Falcon/Kyber hybrid; Full staff certification	Immediate Phase 3–4 migration; serve as pilot site for regional network
Medium Readiness	**4.60/10**	Upgrade infrastructure; targeted expertise training	Phase 1–2 over 12 months; phased hybrid deployment in Year 2
Low Readiness	**2.90/10**	Redirect budget to capability building; vendor partnerships	24–36 month foundational programme before PQC pilot deployment

Table 7: Recommended Transition Pathways by Institutional Readiness Group. Recommendations are calibrated to address the specific capability gaps identified by the regression model.

5. CONCLUSION:

The quantum computing threat, the rapidly growing use of IoMT devices, and the growing seriousness of healthcare data breaches approach a compound security imperative that classical cryptographic architectures are structurally unable to satisfy. The paper has addressed that imperative by four related research contributions that provide the entire continuum between mathematical scheme construction and institutional deployment plan.[1,2,3,4,5,6,28,29,30].

Its key empirical conclusion is as follows: Falcon is the best NIST-standardised PQC algorithm to use in real-time telemedicine and IoMT applications[2,24,31], with the lowest encryption latency (17.16 ms), with less than 50 ms full cryptographic cycling and the highest composite score (6.08) in the set of four possible algorithms. Implemented in a Falcon + Kyber hybrid design - Falcon to handle device-level signatures, Kyber to handle bulk key encapsulation - this design meets the real-time needs of IoMT monitoring and throughput needs of cloud EHR systems.

The institutional analysis indicates that the bottleneck variables[2,44,45] that are limiting to PQC adoption are the technical expertise and infrastructure capacity and not the financial willingness. The programmes of national healthcare cybersecurity that switch PQC funding to competency-based models, rather than to procurement-based models, i.e. focus on workforce development, cryptographical training, and systematic knowledge exchange instead of acquiring hardware and licences, n.b. will gain substantially higher levels of readiness per unit of investment than those that follow the hardware and licence-acquisition path.

The migratory framework of phased hybrid migration proves that the operationally feasible quantum-resilient IoMT security is possible to the point that a 20-month programme structured to migrate a medium-readiness healthcare facility from classical to full PQC cryptography has the capability to maintain 99.92% service continuity without service disruption: the total migration investment is recouped by avoiding breach costs within 28 months. The fact that the six-equation migration model is mathematically rigorous, based on empirical regression coefficients in Section 4, serves to assure that the results of this projection are not wishful thinking, but the target of the operational effort based on evidence.

With the FIPS 203205 standardisation process where NIST PQC is getting finalised and with the probable completion of the standardisation of Falcon, the proactive migration window is getting smaller. The healthcare organisations that start the assessment stage today, including carrying out cryptographic inventory, developing the staff knowledge, and starting to engage with vendors, will be placed at the stage of successful hybrid migration before the quantum threat horizon. The deferring ones are vulnerable to the compounding risk of [21,22,23]harvest-now-decrypt-later attacks[30,33]: attackers who gather encrypted medical data now can

do so and decrypt it later when quantum computing becomes feasible. The study offered in this paper gives the theoretical background, empirical data, and instruments to transform the informed choice into the proactive one.

REFERENCES

[1] Y. Pei, J. Wang, J. Sun, H. Guo, and Z. Li, "A Blockchain-Based Proxy Re-Encryption Scheme with Identity Hash Binding for IoMT Data Sharing,"*Computer Networks*, vol. 245, p. 110386, May 2024. doi: 10.1016/j.comnet.2024.110386.

[2] A. M. Balogun, "Post-Quantum Cryptography for Telemedicine Security: A Benchmarking Study of NIST-Standardised Algorithms,"*Asian Journal of Research in Computer Science*, vol. 18, no. 3, pp. 12–27, 2025. doi: 10.9734/ajrcos/2025/v18i3479.

[3] IBM Security, "Cost of a Data Breach Report 2023," IBM Corp., Armonk, NY, USA, Tech. Rep., 2023. [Online]. Available: https://www.ibm.com/reports/data-breach

[4] U.S. Dept. of Health and Human Services (HHS), "Healthcare Data Breach Statistics 2014–2023," Office for Civil Rights, Washington, DC, USA, 2023. [Online]. Available: https://ocrportal.hhs.gov

[5] M. Frustaci, P. Pace, G. Aloi, and G. Fortino, "Evaluating Critical Security Issues of the IoT World: Present and Future Challenges,"*IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 2483–2495, Aug. 2018. doi: 10.1109/JIOT.2017.2767291.

[6] A. Mosenia and N. K. Jha, "A Comprehensive Study of Security of Internet-of-Things,"*IEEE Transactions on Emerging Topics in Computing*, vol. 5, no. 4, pp. 586–602, Oct.–Dec. 2017.

[7] S. Newaz, A. K. Sikder, M. A. Rahman, and A. Uluagac, "HealthGuard: A Machine Learning-Based Security Framework for Smart Healthcare Systems," in Proc. IEEE 6th Int. Conf. Social Networks Analysis, Management and Security (SNAMS), Granada, Spain, Oct. 2019, pp. 389–396.

[8] M. Blaze, G. Bleumer, and M. Strauss, "Divertible Protocols and Atomic Proxy Cryptography," in Advances in Cryptology – EUROCRYPT 1998, Lecture Notes in Computer Science, vol. 1403, pp. 127–144.

[9] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage,"*ACM Transactions on Information and System Security*, vol. 9, no. 1, pp. 1–30, Feb. 2006.

[10] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing,"*SIAM Journal on Computing*, vol. 32, no. 3, pp. 586–615, 2003.

[11] R. H. Deng, J. Weng, S. Liu, and K. Chen, "Chosen-Ciphertext Secure Proxy Re-Encryption Without Pairings," in Proc. Int. Conf. Cryptology and Network Security (CANS 2008), Lecture Notes in Computer Science, vol. 5339, pp. 1–17.

[12] X. Liang, Z. Cao, H. Lin, and J. Shao, "Attribute Based Proxy Re-Encryption with Delegating Capabilities," in Proc. 4th ACM Symposium on Information, Computer and Communications Security (ASIACCS), Sydney, 2009, pp. 276–286.

[13] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," White Paper, 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[14] E. Androulaki et al., "Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains," in Proc. 13th EuroSys Conference, Porto, Portugal, Apr. 2018, pp. 1–15. doi: 10.1145/3190508.3190538.

[15] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using Blockchain for Medical Data Access and Permission Management," in Proc. 2nd Int. Conf. Open and Big Data (OBD), Vienna, 2016, pp. 25–30.

[16] Q. Xia et al., "MeDShare: Trust-Less Medical Data Sharing Among Cloud Service Providers via Blockchain,"*IEEE Access*, vol. 5, pp. 14757–14767, 2017.

[17] J. C. Benaloh and M. de Mare, "One-Way Accumulators: A Decentralized Alternative to Digital Signatures," in Advances in Cryptology – EUROCRYPT 1993, Lecture Notes in Computer Science, vol. 765, pp. 274–285.

[18] N. Barić and B. Pfitzmann, "Collision-Free Accumulators and Fail-Stop Signature Schemes Without Trees," in Advances in Cryptology – EUROCRYPT 1997, Lecture

Notes in Computer Science, vol. 1233, pp. 480–494.

[19] D. Boneh, B. Lynn, and H. Shacham, "Short Signatures from the Weil Pairing,"*Journal of Cryptology*, vol. 17, no. 4, pp. 297–319, 2004.

[20] P. S. L. M. Barreto and M. Naehrig, "Pairing-Friendly Elliptic Curves of Prime Order," in Proc. Selected Areas in Cryptography (SAC 2005), Lecture Notes in Computer Science, vol. 3897, pp. 319–331.

[21] National Institute of Standards and Technology (NIST), "Module-Lattice-Based Key-Encapsulation Mechanism Standard (FIPS 203)," U.S. Dept. of Commerce, Gaithersburg, MD, Aug. 2024. doi: 10.6028/NIST.FIPS.203.

[22] NIST, "Module-Lattice-Based Digital Signature Standard (FIPS 204)," U.S. Dept. of Commerce, Gaithersburg, MD, Aug. 2024. doi: 10.6028/NIST.FIPS.204.

[23] NIST, "Stateless Hash-Based Digital Signature Standard (FIPS 205)," U.S. Dept. of Commerce, Gaithersburg, MD, Aug. 2024. doi: 10.6028/NIST.FIPS.205.

[24] P.-A. Fouque et al., "Falcon: Fast-Fourier Lattice-Based Compact Signatures Over NTRU," NIST PQC Submission Round 3, 2020. [Online]. Available: https://falcon-sign.info

[25] J. Bos et al., "CRYSTALS-Kyber: A CCA-Secure Module-Lattice-Based KEM," in Proc. IEEE European Symposium on Security and Privacy (EuroS&P), London, 2018, pp. 353–367.

[26] L. Ducas et al., "CRYSTALS-Dilithium: A Lattice-Based Digital Signature Scheme,"*IACR Transactions on Cryptographic Hardware and Embedded Systems*, vol. 2018, no. 1, pp. 238–268, 2018.

[27] D. J. Bernstein et al., "SPHINCS+: Stateless Hash-Based Signatures," NIST PQC Submission Round 3 Finalist, 2020. [Online]. Available: https://sphincs.org

[28] P. W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer,"*SIAM Journal on Computing*, vol. 26, no. 5, pp. 1484–1509, Oct. 1997.

[29] L. K. Grover, "A Fast Quantum Mechanical Algorithm for Database Search," in Proc. 28th Annual ACM Symposium on Theory of Computing (STOC), Philadelphia, PA, 1996, pp. 212–219.

[30] M. Mosca, "Cybersecurity in an Era with Quantum Computers: Will We Be Ready?"*IEEE Security & Privacy*, vol. 16, no. 5, pp. 38–41, Sep./Oct. 2018.

[31] T. Prest et al., "FALCON: Fast-Fourier Lattice-Based Compact Signatures Over NTRU — Implementation Guide," NIST PQC Project, 2022. [Online]. Available: https://falcon-sign.info/impl/falcon.pdf

[32] D. Stebila and M. Mosca, "Post-Quantum Key Exchange for the Internet and the Open Quantum Safe Project," in Proc. Selected Areas in Cryptography (SAC 2016), Lecture Notes in Computer Science, vol. 10532, pp. 14–37.

[33] National Cybersecurity Centre (NCSC), "Preparing for Post-Quantum Cryptography," NCSC Guidance, London, UK, 2021. [Online]. Available: https://www.ncsc.gov.uk/whitepaper/preparing-for-post-quantum-cryptography

[34] ETSI, "Quantum Safe Cryptography and Security: An Introduction, Benefits, Enablers and Challenges," ETSI White Paper No. 8, Sophia Antipolis, France, 2015.

[35] R. Nie, X. He, B. Pang, X. La, and X. Wei, "A Unified Trust Evaluation Framework for IoT Healthcare Based on Multi-Source Fusion,"*IEEE Internet of Things Journal*, vol. 8, no. 12, pp. 9721–9735, 2021.

[36] A. Khalid, S. McCarthy, M. O'Neill, and W. Liu, "Lattice-Based Cryptography for IoT in A Quantum World: Are We Ready?" in Proc. IEEE 8th World Forum on Internet of Things (WF-IoT), Yokohama, Japan, Oct. 2022, pp. 1–6.

[37] S. S. Chowdhury et al., "Physical Security in the Post-Quantum Era: A Systematic Review of Side-Channel Analysis,"*Journal of Cryptographic Engineering*, vol. 11, no. 3, pp. 207–237, 2021.

[38] M. Haghi Kashani et al., "A Systematic Review of IoT in Healthcare: Applications, Techniques, and Trends,"*Journal of Network and Computer Applications*, vol. 192, p. 103164, Oct. 2021.

[39] H. Habib, M. Alam, A. Khan, and N. Javaid, "Enabling Secure Telemedicine Using Blockchain and Proxy Re-Encryption,"*Journal of Medical Systems*, vol. 46, no. 6, p. 39, May 2022.

[40] O. Friha, M. A. Ferrag, L. Shu, L. Maglaras, and X. Wang, "Internet of Things for the Future of

Smart Agriculture: A Comprehensive Survey,"*IEEE/CAA Journal of Automatica Sinica*, vol. 8, no. 4, pp. 718–752, Apr. 2021.

[41] European Parliament and Council, "Directive (EU) 2022/2555 on Measures for a High Common Level of Cybersecurity Across the Union (NIS2 Directive)," Official Journal of the European Union, L 333, Dec. 2022.

[42] U.S. Dept. of Health and Human Services, "HIPAA Security Rule," 45 CFR Parts 160 and 164, Washington, DC, USA, 1996.

[43] NIST, "Recommendation for Key Management — Part 1: General (NIST SP 800-57)," Special Publication 800-57 Part 1 Rev. 5, Gaithersburg, MD, May 2020.

[44] J. Cohen, Statistical Power Analysis for the Behavioral Sciences, 2nd ed. Hillsdale, NJ: Lawrence Erlbaum Associates, 1988.

[45] G. W. Imbens and D. B. Rubin, Causal Inference for Statistics, Social, and Biomedical Sciences: An Introduction. Cambridge, UK: Cambridge University Press, 2015.

[46] A. De Caro and V. Iovino, "jPBC: Java Pairing Based Cryptography," in Proc. IEEE Symposium on Computers and Communications (ISCC), Corfu, Greece, Jun. 2011, pp. 850–855.

[47] The Linux Foundation, "Hyperledger Fabric v2.4 Documentation," 2021. [Online]. Available: https://hyperledger-fabric.readthedocs.io