A Systematic Review of Post-Quantum Cryptography for Healthcare Data Protection: Performance, Readiness, and Deployment Challenges

Taboka Ngwenya [1]*, Belinda Ndlovu [2]**
*, **Informatics Department, National University of Science and Technology, Bulawayo, Zimbabwe
[1]n02214080p@students.nust.ac.zw [1], belinda.ndlovu@nust.ac.zw [2]

Article Info

Article history:

Received 2025-11-23
Revised 2026-01-12
Accepted 2026-01-17

Keyword:

Post Quantum Cryptography,
Medical Imaging Security,
Lattice Based Cryptography,
Cloud Storage,
Healthcare Data Protection,
Quantum Resilience.

ABSTRACT

The traditional cryptographic methods used to protect healthcare data, especially for the long-term storage of medical imaging records, are becoming increasingly threatened by the quick development of quantum computing. The purpose of this study is to assess the challenges, efficacy, and preparedness of integrating Post-Quantum Cryptography (PQC) into healthcare information systems. Twenty peer-reviewed studies published between 2020 and 2025 were analysed following the Preferred Reporting Items for Systematic Reviews and Meta Analyses (PRISMA) protocol. The review was conducted using a systematic research design that included qualitative thematic synthesis, predetermined eligibility criteria, and database searching. According to the results, lattice-based PQC schemes, specifically, CRYSTALS-Kyber for encryption and CRYSTALS-Dilithium for authentication, show great promise because of their effectiveness, resilience, and suitability for decentralized architectures like blockchain and Internet-of-Medical-Things environments. Nonetheless, the review points out a notable deficiency of empirical assessment in actual healthcare settings, particularly with regard to cloud-based platforms and Picture Archiving and Communication Systems utilized in medical imaging processes. Scalability limitations, intricate key-management specifications, system interoperability restrictions, and the requirement for conformity with regulatory and compliance frameworks are some of the major issues noted. The results indicate that lattice-based PQC schemes have great promise, deployment readiness remains largely at the conceptual and experimental stage, particularly for cloud-based PACS environments. Real-world implementation validation in a healthcare setting has not been achieved.

I. INTRODUCTION

Healthcare data, such as imaging data, is known to be amongst the most discretion-sensitive, information-concentrated categories of digital data in present-day healthcare [1]. Medical imaging data is produced using different technologies, including Magnetic Resonance Imaging (MRI), Computed Tomography (CT), ultrasound, and X-ray scanning equipment, which produce images of biological objects containing information critical to patient healthcare [2], [3]. These pictures are stored in standard file formats, as per specifications of Digital Imaging and Communications in Medicine (DICOM) standards, and they hold a vast amount of patient data specific to an individual, including names, dates of birth, patient identification numbers, time stamps, as well as institutional identifiers [4].The files of such images are archived, transmitted, as well as received using an unique server known as a Pictures Archiving and Communication System (PACS) that healthcare professionals use to provide remote collaborative healthcare services for diagnoses, as well as for planning treatments for patients in need of them [5]. Healthcare data faces distinct cryptographic challenges due to its nature, in particular, DICOM files because they contain large amounts of metadata [4] and must be retained for long-term, making them particularly susceptible to the ‘harvest now, decrypt later' quantum attack model [6], [7]. Also, the nature of the PACS requires fast data retrieval, which would result in rapid decryption times, diminishing the viability of using cryptographic solutions [5]. Thus, the healthcare sector requires PQC solutions to have compact ciphertext, low latency in decryption, and maintain system backward compatibility. Blockchain technology is emerging as an alternative method of addressing the issues of interoperability in the healthcare system [8]. But when such decentralized technology is deployed for the long-term storage of medical information, then the need for quantum-resistant cryptography arises. The high value of data placed in this format, as well as its sensitivity, makes it susceptible to malicious manipulation, as the image metadata may reveal even the most hidden, intimate facts about an individual's health, as well as their identity [9].

As such, securing healthcare data, most importantly imaging data, has emerged as a significant challenge for cybersecurity. The healthcare sector is faced with guaranteeing confidentiality, integrity, and availability of patient-related data in distributed systems, including those in the cloud, which support interoperability, financial savings, as well as scalability [10]. Data protection in the medical environment faces challenges in cryptography that are not only different from those in other fields but are uniquely challenging as well. Medical imaging applications like PACS often handle terabyte-sized data with an archival lifetime of several decades [4], [5]. This not only makes the system susceptible to the threat of "harvest-now, decrypt-later" attacks [6], [7], but the medical environment itself has latency constraints on the requirements of authentication and information transfer in the case of emergency and telemedicine applications [1], [11]. These characteristics place unique constraints on cryptographic schemes, requiring not only long-term quantum resistance but also acceptable key sizes, computational overhead, and interoperability with legacy healthcare systems [12], [13]. Post-quantum cryptography is therefore not merely a future-proofing measure in healthcare, but a response to structurally embedded domain-specific risks. However, as healthcare systems are increasingly digitized, they also acquire novel risks such as those from ransomware attacks, unauthorized access, as well as data exfiltration [11]. Traditional cryptographic systems, including Rivest Shamir Adleman (RSA), Elliptic Curve Cryptography (ECC), and Diffie Hellman, have been commonly used for securing confidential information, storing, as well as communicating sensitive information in relation to medical imaging data [6], [12]. However, such encrypted methods are currently faced with an imminent threat from the development of quantum computing [13].

Quantum computing (QC) embodies a groundbreaking computing standard that uses quantum mechanical concepts such as superposition and entanglement to perform computations at unprecedented levels [14]. Algorithms such as Shor's and Grover's have demonstrated the theoretical potential to break widely used cryptographic schemes by efficiently solving problems previously considered computationally obsolete [6], [15], [16]. The emergence of large scale quantum computers poses a direct threat to modern encryption methods, particularly those protecting long retention data like healthcare records and imaging archives that must remain confidential for decades [17]. As a result, there is an urgent need to transition toward Post Quantum Cryptography (PQC) algorithms designed to withstand both classical and quantum attacks [7].

Previous SLRs have reviewed PQC and quantum threats in cryptography [18], [19], [20], healthcare data management frameworks including block chain and AI [21], IoT and IoMT security with quantum considerations [22], [23], and PQC migration strategies for networked systems [24]. However, these studies are primarily focused on theoretical frameworks rather than practical implementation within clouds. This SLR therefore fills this research gap by exploring PQC integration in medical data infrastructure, especially in cloud-based and PACS systems, areas which are relatively uncharted, even though they are essentially core medical image archives.

Though there has been an increasing number of reviews on post-quantum cryptographic schemes, the existing reviews are dominantly domain-agnostic, with a focus on cryptographic security features irrespective of the operational requirements in the domain. For the healthcare domain, there are specific cryptographic requirements, including data warehousing, large-scale medical imaging, real-time processing, and regulatory compliance. The existing PQC reviews are dominantly non-domain-specific, with no emphasis on the specific requirements of the domain. The current study aims to fulfil this requirement by providing a healthcare-specific review on the readiness of PQC in blockchain, IoMT, cloud computing, and PACS, with emphasis on performance, readiness, and feasibility for integration in the healthcare domain, along with cryptographic security. The originality of the current study lies in providing domain-specific information for PQC adoption.

Research Questions

1. What practical barriers affect integrating medical imaging data and metadata into healthcare servers protected with post quantum cryptography?
2. How do lattice based and code based PQC families compare in efficiency and security when encrypting healthcare data in cloud environments?
3. Which digital health infrastructures (i.e., Blockchain, IoMT, Cloud, PACS) are currently integrated with quantum resilient cryptography?
4. Which quantum resistant algorithms demonstrate the lowest decryption cost and highest throughput for typical healthcare workloads?

The rest of this paper is structured as follows: Section 2 outlines the methodology, Section 3 the results and Section 4 the discussion that presents the detailed analysis of the research results and identifies research gaps for future study.

II. METHODS

This study adopted the Preferred Reporting Items for Systematic Reviews and Meta Analyses (PRISMA) protocol to ensure rigor, transparency, and reproducibility. The methodology follows the structured stages of identification, screening, eligibility, and inclusion of studies, supported by clearly defined criteria and systematic analysis of the findings [25].

A. Search Strategy

An extensive search for academic literature was performed on 09 October 2025 on the following four databases: IEEEXplore, Springer Nature, PubMed and Science Direct. A combination of keywords and their alternative expressions was used to frame a search strategy which was modified where necessary to suit each database syntax. The keywords used were as follows: ("Post Quantum Cryptography" OR "Quantum Resilient Encryption" OR "Lattice Based Cryptography" OR "Code Based Cryptography") AND ("Medical Imaging" OR "Healthcare Data" OR "Electronic Health Records" OR "PACS Server") AND ("Cloud Storage" OR "Digital Health Infrastructure" OR "Blockchain" OR "IoMT") AND ("Quantum Computing" OR "Quantum Threat" OR "Harvest Now Decrypt Later"). The searches covered the period January 01, 2020 to October 09, 2025 across a number of peer reviewed academic databases using database specific syntax. We excluded grey literature by design to prioritise peer reviewed evidence. Titles, abstracts and full texts were separately screened by two reviewers, with disagreements resolved by discussion. Data extraction was dual checked.

B. Inclusion and Exclusion Criteria

Inclusion criteria included studies that empirically investigated post-quantum cryptographic schemes within a healthcare setting or related to healthcare, including electronic healthcare records, medical imaging, cloud healthcare, and Internet of Medical Things. The studies included information about performance, key size, computational complexity, or integration within the cryptographic scheme. The exclusion criteria included if the study presented a cryptographic proof that was non-healthcare related and did not involve cryptographic schemes within a healthcare setting, as well as if it was non-healthcare related.

TABLE I
INCLUSION AND EXCLUSION CRITERIA

Time Frame	Studies published between 2020 and 2025.	Studies published before 2020.
Language	Strictly English	Non English publications.
Publication Type	Peer reviewed journal articles and conference papers.	Grey literature, dissertations, book chapters, commentary pieces, editorials, blog posts, white papers.
Relevance to Research Area	Studies focused on implementation, evaluation, or application of Post Quantum Cryptography (PQC) in securing healthcare or medical data systems.	Studies focused on PQC in non-health sectors such as finance, manufacturing, or general cryptography not related to healthcare data protection.
Research Focus	Studies that address quantum resilient architectures, PQC based encryption, or hybrid cryptographic frameworks within healthcare infrastructures such as cloud systems, IoMT, PACS, Blockchain or EHRs.	Studies that only mention PQC conceptually without analysis, implementation, or healthcare focus.
Type of Study	Empirical research that demonstrates or analyses PQC based data protection mechanism on healthcare data systems.	Theoretical research that has no technical exploration or analysis on PQC based data protection, and has no healthcare relevance.
Accessibility	Full text available through institutional access or open access.	Unavailable or pay walled papers without retrievable content.

Only the studies that dealt with the evaluation or experimental analysis of post-quantum cryptography schemes applied or implemented in practical healthcare settings, like Electronic Health Record (EHR) systems, Picture Archiving and Communication Systems (PACS), cloud healthcare platforms, blockchain health records, or Internet of Medical Things (IoMT) frameworks, were used to compile the final results.

C. Screening

The search results from the search terms used yielded a total of n=7068 peer reviewed academic journals and conference papers were identified. From the 7068 papers, n=5165 were from IEEEXplore, n=1736 were from PubMed, n=150 were from Springer Nature, and n=17 were from Science Direct. After the initial search, a total of n=112 duplicate literature were found, leaving us with n=6956 papers. As we were screening the papers by title and abstract, we noted n=3682 papers for exclusion. These studies were primarily systematic or narrative reviews, survey papers, and secondary analyses of empirical research conducted within the healthcare, finance, and quantum physics domains. At this stage, we were left with n=3094 academic works.

D. Eligibility

During the eligibility assessment phase, a total of n=2974 empirical studies were excluded because they focused on PQC adoption and implementation on non-healthcare domains such as finance and manufacturing sectors, or on classical and Blockchain only cryptography without minimal quantum reliant support. At this stage, a total of n=119 eligible papers remained for a full text review.

E. Included

A total of 119 studies qualified for full text review. After a detailed assessment, n=99 studies were excluded. The primary reasons for exclusion were that the studies presented a conceptual structure and review without presenting an applicable PQC method and the proposed PQC solution was not applied or tested within a specific healthcare data setting. Another reason was that the studies were focused on secondary security areas such as pure Quantum Key Distribution (QKD) and authentication which strictly require fully functional quantum computers at a large scale. Subsequently, n=20 studies were included for the final qualitative synthesis in this systematic literature review. The flow diagram for this study review using PRISMA is depicted in Figure 1.

F. Data Extraction and Synthesis

Having completed the eligibility screening process, all of the included studies were imported into Mendeley Desktop . We standardised the academic papers using an Excel extraction sheet that was developed by T.N. to record key details for each study, including title, authors, year, study type, research focus, PQC scheme, healthcare application, and research question addressed. TN completed the extraction and BN verified all entries for accuracy. The two authors (T.N. and B.N.) interdependently screened the full text articles to eliminate irrelevant articles based on the inclusion exclusion criteria. Any differences between the researchers were settle through a collaborative discussion.

G. Composite Metrics for Algorithm Efficiency and Performance Synthesis

Algorithm Efficiency Index (AEI) and Algorithm Performance Index (API) are two composite indices that were developed when studies reported heterogeneous algorithm metrics. The 20 included studies reported performance in a variety of formats; many reported incomplete metrics, some used qualitative descriptors ("low latency," "high efficiency"), and others provided quantitative benchmarks (milliseconds, MB/s, bytes). Because the various reporting formats prevented direct quantitative comparison of raw performance values, composite indices were required to allow valid cross-study comparison while maintaining methodological rigor. Thresholds from NIST Round 3 PQC benchmarking standards (NIST IR 8413) and healthcare IT latency requirements were used to convert metrics to band scores. Midpoint of band values for (Excellent=95, Good=82, Acceptable=65, Poor=42, Very Poor=14) were used to represent the arithmetic mean of each band's upper and lower bounds. For studies with no metric to report, a conservative median score of 50 was assigned.

H. Quality Assessment of Studies

The quality of the selected studies was evaluated using the Critical Appraisal Skills Programme (CASP) framework [26]. The CASP appraisal tool has been adapted for use in this review to suit the technological, simulation-based, and experimental nature of studies reviewed, especially in those assessing post-quantum cryptography, cloud infrastructure, as well as those relating to healthcare data security. The adapted appraisal tool evaluates results across three main areas, namely validity in the study, methodological rigour, and applications of study results [27]. Each question was scored 1 point for fully met criteria, 0.75 for mostly met, 0.5 for partially met, or 0 for not met at all, yielding total scores of 0 12 points throughout the checklist. 12 studies were noted as high quality, 7 were noted as medium and 1 study was marked as low quality. Two reviewers (T.N. and B.N.) independently assessed each study using the adapted tool. Inter rater reliability was excellent, with disagreements resolved through discussion. The complete adapted CASP checklist with scoring criteria. Quality scores were not used as exclusion criteria but inform evidence strength ratings and sensitivity analyses. Despite the relatively small number of studies included in this systematic review, it must be acknowledged that it represents the current state of development of applied PQC studies in healthcare and that it has been conducted with strict criteria for inclusion in order to be relevant to healthcare systems in general.

III. RESULTS AND DISCUSSION

The delimitation process is shown in the following PRISMA flowchart by[25] in Figure 1:

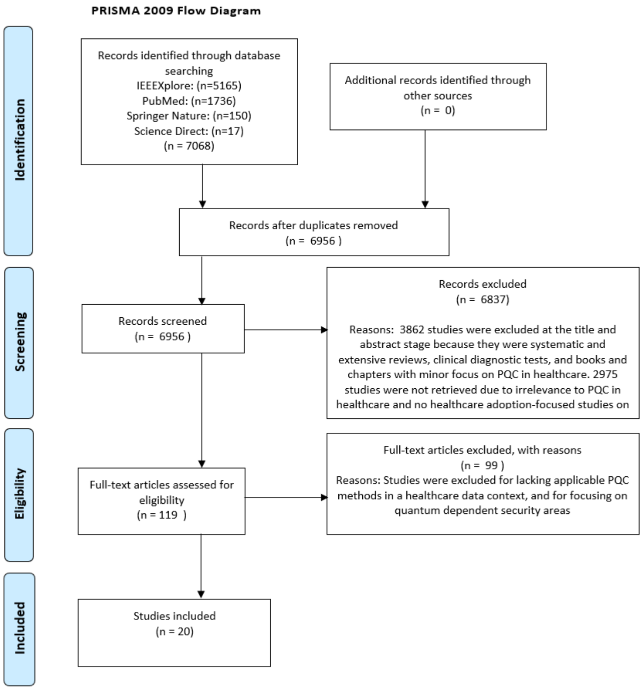
PRISMA 2009 Flow Diagram
Identification
Screening
Eligibility
Included
Records identified through database searching IEEEXplore: (n=5165) PubMed: (n=1736) Springer Nature: (n=150) Science Direct: (n=17) (n = 7068)
Additional records identified through other sources (n = 0)
Records after duplicates removed (n = 6956)
Records screened (n = 6956)
Records excluded (n = 6837)
Reasons: 3862 studies were excluded at the title and abstract stage because they were systematic and extensive reviews, clinical diagnostic tests, and books and chapters with minor focus on PQC in healthcare. 2975 studies were not retrieved due to irrelevance to PQC in healthcare and no healthcare adoption-focused studies on
Full-text articles assessed for eligibility (n = 119)
Full-text articles excluded, with reasons (n = 99)
Reasons: Studies were excluded for lacking applicable PQC methods in a healthcare data context, and for focusing on quantum dependent security areas
Studies included (n = 20)

Figure 1: PRISMA screening results

TABLE II
OVERVIEW OF INCLUDED ARTICLES

Author	Title	Country	Data Type	Core System	PQC Algorithm Efficiency	Quantum Resistance	Key Findings
[28]	A lattice-based group signature with backward unlinkability for medical blockchain systems	China	Medical Imaging Data	• Blockchain • IPFS	Lattice based group signature using Short Integer Solution (SIS) problem with bimodal Gaussian distribution for optimized sampling efficiency	• Efficient signature verification. • Scalable revocation management.	Efficient blockchain group management with backward unlinkability.
[29]	A Programmable Crypto Processor for NIST Post Quantum Cryptography Standardization Based on the RISC V Architecture	South Korea	Crypto Keys on EHR Data	• Programmable Crypto Processor • RISC V Architecture	RISC V instruction set extension for NIST PQC algorithms with up to 79% code size reduction, 92% instruction reduction, and 87% execution cycle reduction	• High speed decryption for a wide range of PQC algorithms.	Generality trades off against peak hardware performance.
[30]	A quantum resilient lattice-based security framework for internet of medical things in healthcare systems	Saudi Arabia	EHR Patient Data	• Internet of Medical Things (IoMT)	Lattice based cryptography using LWE, Ring LWE, and SIS with 50 75% smaller ciphertext sizes, 50% reduction in communication overhead, and 60% less computational cost	• High decryption efficiency. • Lightweight design for resource constrained IoMT devices.	Scalability challenges for resource-constrained IoMT devices.
[31]	An enhanced and verifiable lightweight authentication protocol for securing the Internet of Medical Things (IoMT)	Morocco	IoMT Data	• Internet of Medical Things (IoMT) • Telemedicine Information System	CP ABE with elliptic curves and U Quark hash function 95 98% efficiency improvement over other protocols	• Highly efficient for authentication on embedded medical devices.	Lightweight but not quantum-resistant; near-term solution only.
[32]	An optimized hybrid encryption framework for smart home healthcare	UK	EHR Data	• Smart Healthcare IoT	ECC 256r1 with AES 128 in EAX mode 25.6% improvement in processing speed	• High decryption speed enabling real time data streams.	Transitional scheme; ECC-256 limits long-term quantum resistance.
[33]	CRYSTALS Dilithium post quantum cyber secure SoC for wired communications in critical systems	Spain	EHR Data	• System on Chip (SoC) • RISC V CPU • TSN/MACsec Networks (IIoT)	Lattice based (CRYSTALS Dilithium). Hardware optimized for low power consumption and high performance in SoC. Provides quantum resistant digital signatures for MACsec.	• High performance hardware implementation. • Efficient signature verification for real time systems.	Meets strict power/resource constraints for critical IIoT systems.
[34]	EHRVault: A Secure, Patient Centric, Privacy Preserving and Blockchain Based Platform	Tunisia	EHR Data	• Hyperledger Fabric Blockchain • IPFS • Cloud Storage	Lattice based (CRYSTALS Kyber for key exchange). Integrated into a scalable blockchain platform. Provides quantum resistant key exchange for	• Efficient key decapsulation by authorized parties.	PHI compliance challenges; blockchain-PQC performance trade-offs.

	for EHR Management				EHR confidentiality and integrity.		
[35]	Intelligent two-phase dual authentication framework for Internet of Medical Things	Saudi Arabia	Medical sensor data	• Internet of Medical Things (IoMT)	Combines ECDH and AES GCM (Transitional, not pure PQC). Reduces encryption/decryption time by >45%, computational cost by 45.38%. Resilient to man in the middle, replay, and brute force attacks.	• Low latency ensuring real time communication. • High decryption efficiency.	Transitional; ECDH dependency limits quantum resistance.
[36]	Lattice based ring signcryption scheme for smart healthcare management	India	EHR Data	• Smart Healthcare Management Systems	Lattice based ring signcryption (LRS SHM) with regenerated keys for every signature, more efficient than existing schemes	• Efficient combined signature and encryption (signcryption).	Threshold key reconstruction without compromising privacy.
[37]	LDVAS: Lattice Based Designated Verifier Auditing Scheme for Electronic Medical Data in Cloud Assisted WBANs	China	EHR Data	• Cloud assisted Wireless Body Area Networks (WBANs)	Lattice based designated verifier auditing scheme (LDVAS) with high efficiency and feasibility. Security: Formally proven security based on lattice problems for data integrity auditing.	• Efficient for the designated verifier to audit data integrity without full decryption.	Secure patient-delegated auditing for resource-constrained WBANs.
[38]	Lightweight Two Factor Based User Authentication Protocol for IoT Enabled Healthcare Ecosystem in Quantum Computing	Saudi Arabia	User Authentication for Medical Data	• IoT enabled Healthcare Ecosystem	Post quantum fuzzy commitment scheme (PQFC) more efficient than existing protocols. Security: Proven secure in the random oracle model; resists biometric tampering and stolen device attacks.	• Efficient for lightweight authentication on IoT devices.	Balances security with IoT computational constraints.
[39]	Post Quantum Cryptography Security with CSPM for Secure Data Transmission in Cloud Environments	India	EHR Data	• Cloud Infrastructure	Code based (Variant of McEliece cryptosystem). Proposed as a robust alternative for cloud encryption. Provides resistance against potential quantum attacks.	• Efficient for securing data in transit and at rest in the cloud.	CSPM integration; code-based algorithms incur performance overhead.
[40]	Post quantum secure health records: a blockchain based lattice threshold signcryption scheme	India	EHR Data	• Blockchain	Lattice threshold signcryption based on SIS and LWE problems with threshold cryptography to minimize computational costs	• Efficient decentralized verification on the blockchain.	Threshold cryptography reduces blockchain costs and congestion.
[41]	PPLBB: a novel privacy preserving lattice based blockchain platform in IoMT	Turkey	Medical sensor data	• Blockchain • IoMT • Constrained Application Protocol (CoAP)	Dilithium lattice based signature scheme outperforms Falcon and ECDSA	• Efficient signature verification for real time IoMT communications.	Event-based smart contracts reduce IoMT-blockchain overhead.
[42]	Public Blockchain Envisioned	India	Medical sensor data	• Public Blockchain	Lattice based aggregate signature scheme based on Ring LWE problem with	• Efficient batch verification of	Lattice cryptography adapted for

	Security Scheme Using Post Quantum Lattice Based Aggregate Signature for Internet of Drones Applications			• Internet of Drones (IoD)	superior security and quantum attack resistance	aggregate signatures.	high-mobility drone environments.
[43]	Quantum safe blockchain assisted data encryption protocol for internet of things networks	India	IoT Data	• Blockchain • Internet of Health Things (IoHT)	Lattice based encryption with blockchain minimized encryption and decryption costs	• Very high decryption efficiency. • Suitable for IoT data exchange.	Decentralised key management ensures IoT scalability.
[44]	Quantum safe mutual authentication scheme for IoHT using blockchain	Malaysia	EHR Data	• Blockchain • IoT Networks	Module lattice based blockchain architecture with 62% increase in computation throughput and 36% improvement in transaction processing efficiency	• Low latency authentication. • High data throughput.	Low-latency, high-throughput blockchain authentication.
[45]	Smart healthcare system using integrated and lightweight ECC with private blockchain for multimedia medical data processing	India	Medical Imaging Data	• Blockchain • Cloud Storage • Fog Computing • IoT (Healthcare 4.0)	Uses Elliptic Curve Cryptography (ECC), not PQC. Higher computational efficiency and good PSNR/MSE for images. Provides security for biomedical images but is vulnerable to quantum attacks.	• Vulnerable to quantum attacks.	Not quantum-resistant; ECC vulnerable to quantum attacks.
[46]	Towards attribute based conjunctive encrypted search over lattice for internet of medical things	China	EHR Data	• Internet of Medical Things (IoMT)	Lattice based ACES scheme computational overhead only 82.86% for encryption compared to other schemes. Security: IND CKA and IND CPA secure; enables secure, conjunctive keyword search.	• Exceptionally high decryption efficiency. • Enables practical searches on encrypted data.	Complex key management; search functionality at scale.
[47]	Ultra secure quantum protection for e healthcare images: Hybrid chaotic one time pad with cipher chaining encryption framework	India	Medical Imaging Data	• IBM Quantum Processor (ibm_sherbrooke) • Quantum Computing	Mixed Logistic Ikeda Henon chaotic map with quantum CNOT operations 12.7% improvement in logic gate efficiency. Security: Resilient to Grover's algorithm and quantum chosen plaintext attacks.	• Resilient to Grover's algorithm and quantum chosen plaintext attacks. • High throughput on quantum hardware.	Requires specialised NISQ hardware; limited practical deployment.

A. Geographical Distribution of Research

Figure 2 illustrates the annual number and rate of publications on quantum-resistant security for healthcare data from the year 2020 to 2025.

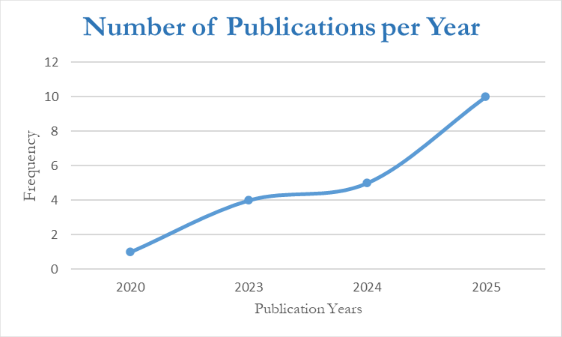

Figure 2: Number of Publications

The exponential growth experienced in research related to the matter can be noted, from six publications between 2020-2023, to fifteen publications in 2024 and 2025. This demonstrates an increased recognition by the research community of the vulnerability of healthcare data to the potential threats exerted by quantum computing.

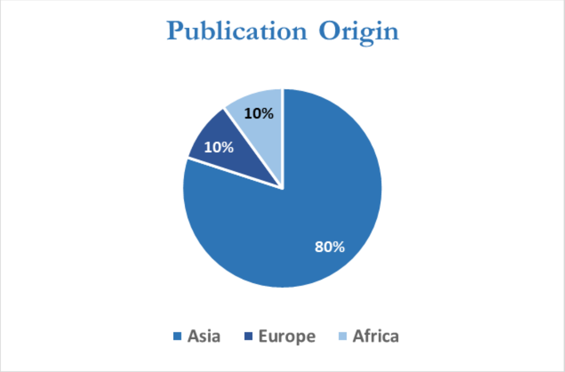

Figure 3: Publication Origin by Continent

Figure 3 shows the geographic representation of PQC healthcare studies on all continents from which the studies were published, revealing the regional concentration of scholarly activity in this emerging field. The dominance of Asian publications at 80% suggests that there is a significant presence of PQC healthcare research in the Asian region, which could likely be influenced by the development of quantum computers and subsequent QC policies. The total lack of North American studies is notable, especially when considering their highly developed healthcare policies, and could indicate differing research priorities or perhaps slower, non-urgent awareness of the quantum threat to healthcare across the West. The uneven geographic representation here suggests that policies for the implementation of PQC in healthcare could be lacking diversity.

B. PQC Adoption Across Healthcare Data Types and Core Infrastructures

Figure 4 presents a cross clustered analysis showing the distribution of the 20 included studies across different healthcare data types and the core infrastructures they aim to secure.

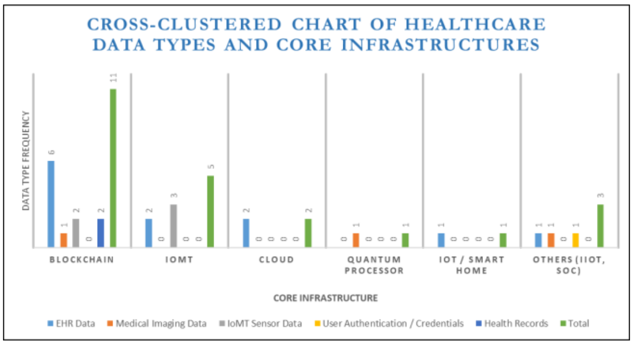

Figure 4: PQC Adoption on Core Infrastructure and Healthcare Datatype

With 55% (n = 11) of the total focus on blockchain-related work, the evident imbalance between research interests and actual healthcare systems is significantly alarming. As appealing as blockchain design is to PQC research efforts, cloud PACS systems are severely underrepresented with merely 2 publications. This strongly implies that PQC research work is currently more interested in exploring and studying new forms of decentralized communication rather than actual healthcare systems protection, as they are already at risk of quantum attacks and adverse effects. The underrepresentation of work related to cloud and PACS systems hinders effective comparisons of algorithms in environments that are already in actual need of PQC applications.

C. Comparative Efficiency of Post Quantum Cryptographic Families

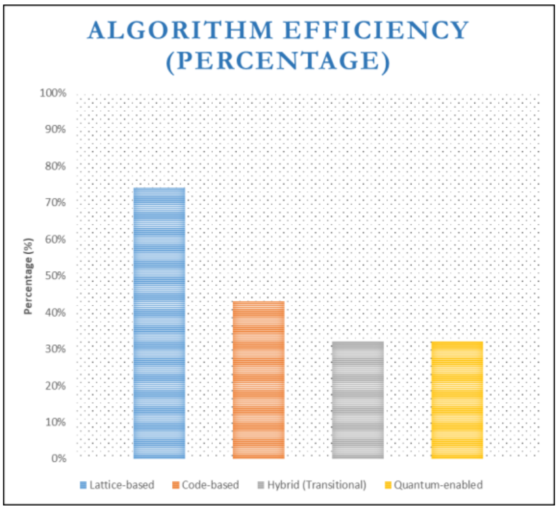

Figure 5: Algorithm Efficiency Index Scoring (Percentage)

Figure 5 illustrates the overall algorithmic efficiency of the primary PQC families identified in this review, and provides a detailed breakdown of their performance scores and core applications in healthcare

The observed efficiency difference for lattice-based cryptographic approaches (73.9%, n = 12) seems to represent the current state of research and optimizations rather than an intrinsic superiority over other approaches. Conversely, the non-optimal efficiency for code-based and quantum-enabled options (both 32%, n = 1) most probably indicates overlooked potential instead of the current absence of suitability. These results suggest an efficiency order influenced by the so-called publication bias for lattice-based methods instead of an overall evaluation for post-quantum cryptography approaches in the healthcare domain. Despite the majority of lattice-based cryptosystems in the literature reviewed, their popularity is more of a function of active research and alignment with standardization efforts than any absolute appropriateness in general healthcare settings. Hash-based signatures are highly secure but also quite challenging in practical implementation terms for key management and signature size considerations. Code-based cryptosystems are secure but typically inordinately expensive in terms of computational complexity for healthcare implementations that are subject to real-time constraints. Multivariate cryptosystems are still represented inadequately in healthcare literature partly because of concerns over cryptanalytic maturity levels.

D. Performance Metrics of Individual PQC Algorithms

Table 3 provides a detailed comparison of the performance characteristics for specific PQC algorithms identified in the review to summarizes their overall qualitative performance by family.

TABLE III
ALGORITHM PERFORMANCE PARAMETERS

Algorithm	PQC Family	Encryption Cost	Decryption Cost	Throughput	Ciphertext Size	Supporting Author
Kyber	Lattice based	Low	Very Low	High	Small	[34] [43]
Dilithium	Lattice based	Medium	Medium	High	Small	[33] [41]
Ring LWE	Lattice based	Low	Low	Medium	Small	[42] [30]
LWE/SIS	Lattice based	Low	Very Low	High	Very Small	[30] [46] [28]
McEliece	Code based	High	High	Low	Very Large	[39]
Module Lattice	Lattice based	Low	Low	High	Not Specified	[44]

Table III reveals that performance disparities between PQC families reflect evaluation context rather than inherent algorithmic limitations. While the lattice-based schemes were tested in latency-optimized setups like IoMT and Blockchain, their performance metrics are superior, and code-based approaches are poor because of their evaluation in the context of limited bandwidth, focusing more on long-term security than efficiency. Direct comparisons across families for determining if code-based approaches were capable of comparable lattice-based performance in the same setting are affected by this experimental difference. Any direct comparison of Post-Quantum Cryptography (PQC) solutions and traditional cryptography solutions is hampered by inconsistent methods of comparison used in different research works. In cases where comparisons are made, it is seen that PQC solutions have much larger key sizes and computation overheads than RSA or ECC solutions, which may be problematic in healthcare applications requiring low latency. These results again highlight the quantum resistance versus efficiency trade-off. Although PQC solutions are conceptually supportive of decentralized healthcare systems, empirical research in PQC solutions in resource-constrained IoMT devices is limited to simulated or theoretical performances.

E. Encryption and Decryption Efficiency of PQC Algorithms

Figure 6 provides a detailed comparison of AEI and API scores for the primary PQC algorithms evaluated in the included studies across different cryptographic implementations.

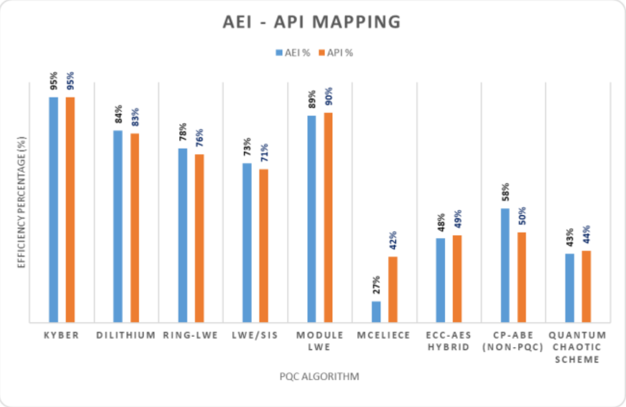

Figure 6: AEI to API Mapping for Individual Algorithms

The research prioritization of lattice-based optimization for healthcare contexts is revealed by Kyber's remarkable scores (95%/95%), which show more than just superior performance. While Kyber gains from multi-study refinement across healthcare scenarios, McEliece's low performance (27%/42%) might not be due to intrinsic unsuitability but rather to insufficient healthcare-specific optimization. Therefore, rather than providing conclusive algorithmic comparisons, current efficiency rankings show differences in research investment, questioning whether code-based schemes could achieve comparable performance under equivalent optimization efforts.

F. Challenges

Table 4 shows the challenges that have been encountered by the research community when it comes to the evaluation and implementation of PQC methods in the healthcare industry on core systems such as Blockchain, IoMT and Cloud infrastructure, and Figure 7 shows the impact scoring for the identified challenges.

TABLE IV
CHALLENGES IDENTIFIED IN LITERATURE

Challenge	Description	Impact	Authors
Scalability and Integration Overhead	Integrating lattice based and blockchain supported PQC frameworks within large scale healthcare and IoMT systems often introduces substantial computational and communication overheads. These challenges hinder performance, increase latency, and reduce real time responsiveness.	High computational load limits the scalability of PQC in real world healthcare deployments, especially where continuous data exchange and rapid processing are required.	[28], [30], [36], [41], [43]
Hardware and Quantum Processor Dependency	Quantum enabled and hardware based PQC implementations rely heavily on specialized hardware such as quantum processors and RISC V SoCs, which are not yet widely available in clinical or cloud environments.	Restricts practical adoption due to cost, hardware availability, and technical expertise required to maintain and deploy such specialized systems.	[29], [32], [33], [47]
Cloud Implementation Gap	Despite widespread cloud use in healthcare, very few studies have evaluated PQC algorithms under real world cloud workloads or virtualized environments.	Creates a critical evidence gap for secure cloud based EHR and imaging storage, limiting confidence in PQC's readiness for scalable healthcare data hosting.	[32], [34], [39], [46]
Complex Key and Credential Management	Many lattice based and attribute based encryption models require intricate key generation, distribution, and revocation processes, which are difficult to automate at scale.	Adds significant operational burden and increases the risk of configuration errors or credential mismanagement that can compromise security integrity.	[28], [31], [36], [38], [46]
Interoperability with Legacy Systems	Existing hospital systems (e.g., PACS, EHR servers, HL7/FHIR interfaces) are not designed for quantum safe cryptography, creating integration incompatibilities.	Restricts the backward compatibility and seamless data exchange between legacy systems and new PQC secured frameworks.	[32], [34], [39]
Energy Consumption and Cost	PQC algorithms generally demand higher computational resources and power, leading to increased operational costs in both on premise and cloud deployments.	Raises sustainability and energy efficiency concerns, particularly for continuous IoMT or imaging applications in resource limited healthcare facilities.	[30], [32], [33], [45]
Regulatory and Compliance Alignment	There is limited discussion on aligning PQC implementations with healthcare data protection laws such as HIPAA, GDPR, and PHI compliance requirements.	Without legal and regulatory integration, PQC adoption may fail to meet compliance standards, delaying or preventing institutional implementation.	[32], [34], [39]

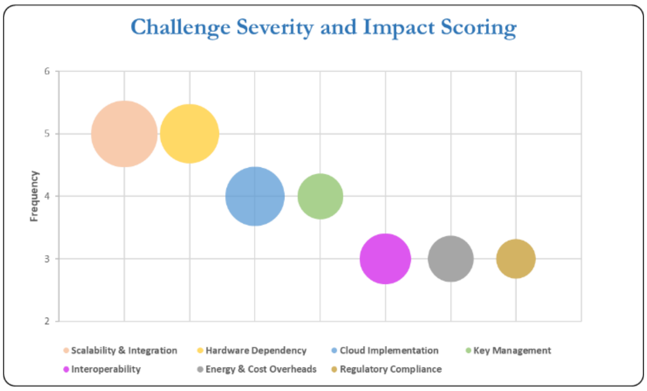

Figure 7: Challenge Severity and Impact Scoring Analysis

Figure 7 and Table 4 illustrate the main trade-offs between the security requirements of PQC and the operations of healthcare. More importantly, the methodological bias in the Cloud Implementation Gap reveals the preference for IoMT, experimental blockchain, over cloud-based PACS in storing healthcare data. This means the research on PQC at the moment leans towards innovation rather than the mitigation of quantum risk in the healthcare sector.

G. Discussions

This discussion addresses the four research questions formulated in Section I.

RQ1: Challenges in Integrating Medical Imaging Data with Metadata into healthcare data servers

The following exploration into the challenges informed by collective evidence of this set of studies, provides clarity for what must be remedied in order for healthcare data to be safe in this quantum age.

1) *Scalability and integration overhead*: Scalability and integration overhead refers to the computational complexity introduced by PQC schemes, which can impede processing speed within medical services data servers. Lattice-based cryptography is secure but computationally issues in large data for healthcare [30], [43]. Regarding medical image processing, this means that delays are substantial when encrypting large files for DICOM, potentially impacting radiological workflows [36]. [33] show that hardware-optimized implementations, like System-on-Chip technologies, For CRYSTALS-Dilithium, SoC designs may also reduce this problem indicates that hardware accelerators are needed together with PACS to function as clinical servers.

2) *Hardware and Quantum Processor Dependency*: This challenge is the reliance on specialised hardware, such as quantum processors and RISC V SoCs, which are absent from standard clinical IT infrastructure. The study by [47] for encrypting e healthcare images is a prime example, as it requires an IBM quantum processor. Similarly, the programmable crypto processor by [29] and the Dilithium based SoC by [33] are tied to specific hardware platforms. The consequence for integrating with a PACS is a practical impossibility; hospitals cannot replace their entire imaging infrastructure with experimental, costly hardware. This dependency confines such solutions to research labs, as acknowledged in the hybrid framework by [32]. Overcoming this problem requires a paradigm shift. This is achieved through a software-based system based on standardized quantum-resistant cryptography algorithms, such as CRYSTALS Kyber and Dilithium, which operate optimally in common servers used in hospitals, such as PACS or a cloud-based infrastructure.

3) *Cloud Implementation Gap*: The cloud implementation gap is the critical absence of PQC research in real world cloud environments, which are increasingly used for hosting medical imaging archives and even full PACS solutions. This is evidenced by the scarcity of cloud native studies, where only the work of [39] on McEliece for cloud environments and [37] on cloud assisted WBANs directly address this setting. This is a critical omission because, as seen in studies such as EHRVault by [34] which utilizes cloud storage in systems research, performance is not measured in the usual environments for cloud PACS infrastructure. As observed, this raises questions about the performance capabilities of PQC in essentially the same infrastructure in which most of tomorrow's healthcare data, including pictures, will be processed and stored. This is a critical area that needs to be filled by actual applications of algorithms such as Kyber and Dilithium to virtualized, cloud-based healthcare systems to prove actual integration into healthcare systems. The integration of post-quantum cryptography (PQC) in the processes of the Picture Archiving and Communication System (PACS) is justified at three instances: during the secure exchange of keys during the transmission of images, during the storage of encrypted DICOM images in cloud storage, and during the authentication process of clinician access requests. There is little, if any, empirical study in existing literature about the performance of PQC integration at these instances. In the context of the PACS process, it appears most likely that the integration of PQC takes place at the stages involving key management, authentication, and secure archival, but not limited to image transmission.

4) *Complex key and credential management*: Complex key and credential management emerges as a result of complex processes of key generation, distribution, and revocation in an advanced PQC system, which cannot be easily automated in a large healthcare organization. Key management challenges in lattice-based group signatures are discussed by [28] [36] [46]. In medical archives where patient data can amount to thousands of entries, improper key management leads to medical data confidentiality breaches [38] and medical data unavailability for diagnoses and medical services due to lost or improperly managed cryptographic keys, causing inaccessible DICOM files. This can be managed by using cloud security services-integrated

Key Management Systems (KMS), for example, HashiCorp Vault or AWS-KMS.

5) *Interoperability with Legacy Systems*: Challenges in interoperability are encountered when securing PQC-secured environments with legacy environments in the healthcare industry that are using classical cryptographic approaches. This issue is recognized by [34] and [39] remains unsolved. This is because existing environments in the healthcare industry, including environments for image review using PACS, are difficult to replace within present economic limitations and create a problem where legacy environments are vulnerable to quantum attacks but must work together with quantum-secured environments. A practical way to operate would be to implement hybrid migration. Thus, classical cryptography such as RSA and ECC are deployed concurrently with PQC algorithms until the transition phase is completed. This allows gradual system migration and backward compatibility to the legacy PACS and EHR systems.

6) *Energy Consumption and Cost*: PQC algorithms consume more computational resources, thereby increasing operating costs. This challenge has been tackled by [33] for Dilithium SoC implementation to optimize for hardware capabilities. It is also implicitly recognized by [32] and [30] for their respective hybrid and IoMT approaches. Despite this disadvantage, using clouds can lower cost for using PQC than maintaining classical encryption protocols exposed to attacks.

7) *Regulatory and Compliance Alignment*: Although very limited research work has been accomplished to align PQC implementation with healthcare regulations like HIPAA and GDPR, [34] and other studies by authors such as [39] did partially address the issue. The use of strong cryptographic measures in the protection of patient data is required by GDPR under Article 32 and HIPAA guidelines in the provision 45 CFR 164.312(a)(2)(iv) on encryption. To protect against quantum threats long term, PQC must meet this provision. There is no guideline on how quantum algorithms resistant to quantum computers can be certified in terms of adhering to existing guidelines on compliance. This can create hurdles for its usage within institutions due to uncertainty related to healthcare regulation adherence. Active research work needs to be accomplished to align PQC with NIST norms and healthcare regulations. Recent studies on responsible data stewardship for institutional use have claimed that institutional frameworks of governance need to incorporate privacy by design [48], and this could facilitate effective cryptography.

RQ2: Comparative Efficiency and Security of Lattice Based and Code Based Cryptography

This discussion outlines the operational characteristics of the different Quantum Cryptographic approaches, as well as their fundamental implications in securing data in the cloud for healthcare applications.

1) *Lattice Based Cryptography*: The lattice-based cryptographic approach relies on computational difficulties with lattice problems, Learning With Errors, or Short Integer Solutions. This category encompasses most studies on PQC for healthcare. This encompasses blockchain-based healthcare applications [28] [36], IoMT frameworks [30] [31], and SoC lattice-based optimizations for healthcare [33]. Lattice-based cryptographic algorithms are ideal for healthcare operations, with around 74% combined efficiency for cloud-based medical image processing within a PACS, which entails fast encryption operations.

2) *Critical Assessment of PQC Family Trade-Offs*: Although lattice-based methods are efficient (73.9%, n = 12), they present substantial real-world challenges that are not adequately treated in current research. The operational migration towards PQC in the healthcare system is also expected to require hybrid cryptographic implementations that combine classical and post-quantum cryptography algorithms to support backward compatibility. But the available literature provides very minimal information regarding the migration process and the mitigation of system downtime.

The works by [28] [36] refer to heavyweight integration costs in large-scale healthcare networks, while [30] indicates complex key management as an obstacle to implementation. The prevalence of lattice-based methods in research might already be the effect of optimization maturity instead of objective superiority. By contrast, code-based methods' simplified representation (n = 1) and absence of suitable methods with either hash functions or multivariable problems reveal latent potential instead of obvious failure. The low efficiency (32%) of McEliece might originate from insufficient healthcare-specific optimization, implying that perhaps other post-quantum cryptography families can be similarly efficient with comparable research investment.

3) *Code Based Cryptography*: Code based cryptography, as illustrated in the McEliece cryptosystem, is grounded in the hardness of decoding random linear codes, which is presumed safe even against quantum computers. This single study adopting code based cryptography as proposed by [39] would find it useful for cloud storage, appreciative of the strong established foundation in security that it has. Nonetheless, in terms of algorithmic efficiency at only 43%, it is clear that it has a basically inherent property of high computational complexity. As a solution for cloud storage, most especially for large data entities such as medical images, this would result in much slower uploading and downloading speed, as well as higher computational requirements for processing encrypted files, for which large sizes of ciphertext as in code based cryptography systems would obviously result in higher costs for storage in the cloud as well.

4) *Hybrid and Quantum Based Approaches*: Hybrid approaches integrate classical cryptographic techniques (ECC, AES) with PQC concepts on a transition basis [45] [32] [35], and quantum-enabled approaches leverage quantum hardware for encryption purposes [47]. Both types achieve a score of about 32% composite efficiency. Hybrid approaches are short on quantum resistive capabilities as they are based on classical cryptography that is quantum-vulnerable. Quantum-enabled approaches, though promising on paper, are not feasible with present-day healthcare facilities.

5) *Comparative Analysis:* Lattice cryptography appears to be the leading category in PQC for healthcare applications, counting for 12 out of 20 studies with 73.9% efficiency. Another method, code-based cryptography, only counted for one study with 32% efficiency. While lattice schemes are currently the most prevalent in post-quantum cryptography related to healthcare, it is the maturity level of the related research and not the superiority of the algorithms that explains this dominance. Code-based cryptography, as presented by the McEliece scheme, provides strong underlying assumptions about security and immunity to side-channel attacks, while hash-based cryptography provides low implementation overhead and strong guarantees for forward security. Multivariate cryptography, while less mature, offers some benefits for resource-limited authentication applications.

RQ3: Core Digital Health Infrastructure Technologies Integrable with Quantum Resilient Cryptography

This discussion delves into the operation, application, and PQC integration of these dominant infrastructures to ascertain their role in a future proof healthcare ecosystem. It should be mentioned that the majority of PQC implementations based on blockchain and IoMT that have been reviewed are still in the experimental stage and have not received much large-scale validation on real medical devices with limited resources in operational healthcare settings.

Despite the alignment of the concepts of PQC and the vision of a decentralized healthcare system, there is a lack of empirical evidence for resource-constrained IoMT devices. This is the case for energy consumption, latency, as well as memory overhead in real-world use cases. Normative claims about post-quantum cryptography's appropriateness in blockchain-related and Internet of Medical Things settings are often inferred from experimental trials rather than their operational deployments in a health care scenario. Results of promising work in terms of theoretical efficiency [30], [31], [38], [41], [42] have not been verified regarding their practical efficiency in health care-related IoMT devices in a more constrained clinical scenario. Along the same lines, the merits of blockchain technology in health care [28], [34], [40], [43], [44] have been untested in the more stressing health care-related transactions.

1) *Blockchain*: The application of blockchain technology in the health sector has been shown to improve data security, interoperability, and patient-focused access control mechanisms [49] and thus sets the stage for the implementation of quantum-resistant cryptographic methods. The integration between blockchain and PQC mainly uses lattice-based cryptography, where key exchange is implemented using CRYSTALS-Kyber by [34], while threshold signcryption is applied by [40]. This approach mainly provides assurance for non-repudiation and data integrity. The main issue seems to be handling the computational complexity, resulting from combining lattice-based algorithms' computational complexity, as well as combining blockchain methodologies for data exchange throughput.

2) *Internet of Medical Things (IoMT)*: As far as devices operating on limited resources are concerned in IoMT, minimized cryptographic protocols are required. This has emphasized lattice-based cryptography. Here, most literature relies on lattice-based cryptography. For instance, [30] minimized cryptographic sizes using LWE and ring LWE in 2025. Another scheme using CP-ABE on elliptic curves was adopted by [31], but this is not quantum resistant, which does not guarantee near-term performance and long-term quantum security.

3) *Cloud Infrastructure*: Cloud platforms are identified as the most prominent research gap. To design for cloud platform security, [39] suggested using the McEliece scheme in 2024. However, its large size does not support efficiency. Additionally, lattice-based audit for cloud-assisted WBANs for more promising outcomes was demonstrated by [37]. This indicates that lattice-based solutions are more adapted to cloud-based healthcare but are not well-explored. In the typical PACS workflow, there must be cryptographic security at three levels: (i) at image capture and modal transmission (DICOM C-STORE), (ii) at archival and retrieval, and (iii) at remote viewing and teleradiology. The addition of PQC, therefore, must include quantum-resistant key exchange in modal and PACS negotiation, classical and PQC hybrid archival storage, and PQC transport security at clinician access. None of the reviewed studies currently evaluate these end-to-end workflows.

RQ4: Most Efficient Quantum Resistant Algorithm for Decrypting Healthcare Data

Lattice-based cryptography algorithms, particularly CRYSTALS-Kyber and Dilithium, are identified to be most efficient quantum-resistant methods in the healthcare domain. Although their effectiveness has been established only in blockchain and IoMT settings, it has not been thoroughly examined in cloud-based healthcare environments.

1) *Kyber (CRYSTALS Kyber)*: Kyber is a key encapsulation mechanism (KEM) that helps people set up secure symmetric keys between them. In healthcare, this is the

basic way to safely share a key to encrypt and decrypt patient records, whether they are stored in a cloud database or sent over a network. Kyber's low decryption cost and compact ciphertext size qualify it for optimal usage in accessing high-frequency data in the healthcare industry. This was quantified in terms of its decryption costs to about 0.010 by [43], and its integration into the EHRVault blockchain platform was demonstrated to be feasible by [34].

2) *Dilithium (CRYSTALS Dilithium)*: Dilithium is a digital signature algorithm used for authentication and ensuring data integrity. Dilithium offers efficient digital signatures for healthcare authentications and data integrity verification. This has been shown to achieve viable real-time execution via hardware-optimized SoC design by [33]. Composite efficiency of 84% makes Dilithium applicable for digital signatures for prescriptions, laboratory reports, and medical image access logs where non-repudiation is required.

3) *McEliece*: The McEliece cryptosystem, a code-based algorithm, is employed for direct public key encryption. The main targeted use of McEliece in the literature is for encrypting data in a cloud system [39]. McEliece is somewhat less popular as a solution when compared to lattice-based methods. McEliece is marked by High decryption & encryption complexity and Large ciphertext size [39]. The work by [39] recognized that this solution carries a possible performance implication in decryption. This impacts methods for decrypting patient data, including large imaging files, resulting in slow access times for faster data processing pathways in a dynamic healthcare environment.

H. Implications of the Study

1) *Practical Implications*: The research finds that lattice cryptography (CRYSTALS-Kyber and Dilithium) is the most efficient method of secure medical data protection. Kyber supports low latency and compact ciphertexts, which are suitable for efficient key exchange, while Dilithium supports authentication. These are applicable on current cloud infrastructure (AWS, Azure) with non-quantum chips. For software programmers, lattice cryptography primitives allow efficient encryption/decryption in high-data-rate apps. For medical institutions, implementing Kyber and Dilithium will facilitate HIPAA and GDPR regulations while consuming less bandwidth and storage. For policymakers, implementing PQC in medical security on a large scale should include cooperation between medical organizations and standardization organizations (like NIST) to establish guidelines on EHR/PACS systems.

2) *Theoretical Implications*: This work solidifies lattice cryptography as the most adaptable and scalable PQC solution for blockchain, IoMT, and cloud-native healthcare environments. Kyber for key exchange and Dilithium for verification are also sufficient for providing full protection against attacks on confidentiality, integrity, and authenticity using quantum computers. This assessment also reveals a critical need for more empirical research on PQC for secure cloud-based medical image processing environments, specifically for those on PACS.

I. Limitations of the Study

This review has various limitations. Due to the limited number of empirical studies eligible for analysis, the results of the review are considered indicative of the trend, rather than conclusive proof of the readiness of PQC for widespread adoption within the healthcare systems. First, the performance metrics were constructed using reported benchmarks to create the efficiency metrics. This can pose risks to the construct validity given the inconsistent testing conditions across the sources. Second, the paper only sampled the performance of the four academic databases. There can be papers within other databases that can be overlooked. Third, the paper focused on English literature alone. There can be studies on quantum cryptography or medical care conducted in other languages. Finally, the actual access to the quantum hardware may be limited to compare the performance metrics of the PQC algorithms.

J. Future Works

Priority areas where research needs to be done include the validation of PQC in the cloud-native medical setting where sensitive images are involved. The goals include the development of quantum-resistant architectures in the cloud in the context of medical images using Kyber (Key Encapsulation) and Dilithium protocols in the authentication phase. Additionally, the development of deployment best practices to support HIPAA and GDPR requirements should be accomplished.

IV. CONCLUSION

This SLR examined post-quantum cryptography for healthcare data security across 20 peer-reviewed publications, evaluating algorithms, infrastructure, implementation challenges, and efficiency metrics. Lattice-based cryptography, specifically CRYSTALS-Kyber and Dilithium, emerged as the most efficient solution for encrypting, decrypting, and authenticating healthcare data in blockchain and IoMT environments. However, until there are empirical studies in cloud environments and PACS systems, quantum-secure solutions remain theoretical for mainstream healthcare deployment. Future work must focus on proof-of-concept implementations integrating Kyber and Dilithium into cloud-based PACS, alongside regulatory alignment, to enable practical quantum-resilient healthcare infrastructure globally. Overall, it appears from the existing evidence that the current state of post-quantum cryptography in healthcare is still largely theoretical. While there are promising developments in the area of lattice-based cryptographic algorithms, it would seem that the maturity of PQC in healthcare deployment readiness remains highly context-dependent. Instead, PQC could be seen more as a strategic area requiring continued research efforts.

REFERENCES

[1] S. Saif, P. Das, S. Biswas, S. Khan, M. A. Haq, and V. Kovtun, “A secure data transmission framework for IoT enabled healthcare,” *Heliyon*, vol. 10, no. 16, p. e36269, Aug. 2024, doi: 10.1016/J.HELIYON.2024.E36269.

[2] A. P. Varghese, S. Naik, S. Asrar Up Haq Andrabi, A. Luharia, and S. Tivaskar, “Enhancing Radiological Diagnosis: A Comprehensive Review of Image Quality Assessment and Optimization Strategies,” *Cureus*, vol. 2024, no. 6, pp. 1–10, 2024, doi: 10.7759/cureus.63016.

[3] I. U. Haq, M. Mhamed, M. Al-Harbi, H. Osman, Z. Y. Hamd, and Z. Liu, “Advancements in Medical Radiology Through Multimodal Machine Learning: A Comprehensive Overview,” *Bioengineering*, vol. 12, no. 5, pp. 1–38, 2025, doi: 10.3390/bioengineering12050477.

[4] M. Rempe, L. Heine, C. Seibold, F. Hörst, and J. Kleesiek, “De-identification of medical imaging data: a comprehensive tool for ensuring patient privacy,” *Eur. Radiol.*, 2025, doi: 10.1007/s00330-025-11695-x.

[5] H. Pereira, L. Romero, and P. Miguel Faria, “Web-Based DICOM Viewers: A Survey and a Performance Classification,” *J. Imaging Informatics Med.*, vol. 38, no. 3, pp. 1304–1322, 2025, doi: 10.1007/s10278-024-01216-5.

[6] M. SaberiKamarposhti *et al.*, “Post-quantum healthcare: A roadmap for cybersecurity resilience in medical data,” *Heliyon*, vol. 10, no. 10, p. e31406, May 2024, doi: 10.1016/j.heliyon.2024.e31406.

[7] A. Karakaya and A. Ulu, “A survey on post-quantum based approaches for edge computing security,” *Wiley Interdiscip. Rev. Comput. Stat.*, vol. 16, no. 1, 2024, doi: 10.1002/wics.1644.

[8] V. A. Muderere, B. Ndlovu, and K. Maguraushe, “Blockchain Adoption in Healthcare: Enhancing Interoperability, Security and Data Exchange,” *J. Inf. Syst. Informatics*, vol. 7, no. 3, pp. 2939–2977, 2025, doi: 10.51519/journalisi.v7i3.1267.

[9] C. M. Prakaashana *et al.*, “Measuring the potential risk of re-identification of imaging research participants from open-source automated face recognition software,” *Neuroimage*, vol. 320, p. 121476, Oct. 2025, doi: 10.1016/J.NEUROIMAGE.2025.121476.

[10] B. Dharangan *et al.*, “Secure Cloud-based E-Health System using Advanced Encryption Standard,” in *2022 3rd International Conference on Electronics and Sustainable Communication Systems (ICESC)*, Institute of Electrical and Electronics Engineers Inc., 2022, pp. 642–646. doi: 10.1109/ICESC54411.2022.9885501.

[11] W. Hurst, B. Tekinerdogan, T. Alskaif, A. Boddy, and N. Shone, “Securing electronic health records against insider-threats: A supervised machine learning approach,” *Smart Heal.*, vol. 26, p. 100354, Dec. 2022, doi: 10.1016/J.SMHL.2022.100354.

[12] L. J. R. Lopez, D. Millan Mayorga, L. H. Martinez Poveda, A. F. C. Amaya, and W. Rojas Reales, “Hybrid Architectures Used in the Protection of Large Healthcare Records Based on Cloud and Blockchain Integration: A Review,” *Computers*, vol. 13, no. 6, Jun. 2024, doi: 10.3390/computers13060152.

[13] A. Ahmad and S. Jagatheswari, “Quantum Safe Multi-Factor User Authentication Protocol for Cloud-Assisted Medical IoT,” *IEEE Access*, vol. 13, no. December 2024, pp. 3532–3545, 2025, doi: 10.1109/ACCESS.2024.3523530.

[14] M. A. Naranjo and L. A. Fletscher, “Review Quantum Circuit Synthesis for Grover’s Algorithm Oracle,” *Algorithms*, vol. 17, no. 9, 2024, doi: 10.3390/a17090382.

[15] F. Opiłka, M. Niemiec, M. Gagliardi, and M. A. Kourtis, “Performance Analysis of Post-Quantum Cryptography Algorithms for Digital Signature,” *Appl. Sci.*, vol. 14, no. 12, 2024, doi: 10.3390/app14124994.

[16] P. Vareta, H. Muzenda, T. Nyamupaguma, B. Ndlovu, and Y. Dube, “The Rise of Quantum Computing and its Impact on Cybersecurity,” vol. 14, no. 6, pp. 10072–10102, 2025, doi: https://doi.org/10.33022/ijcs.v14i6.5040.

[17] J. Martin, M. Cheng, J. Martin, and A. Johnson, “Encryption in Transit in Healthcare SaaS: The Role of Mutual TLS,” *SSRN Electron. J.*, Feb. 2025, doi: 10.2139/ssrn.5131928.

[18] E. Fathalla and M. Azab, “Beyond Classical Cryptography: A Systematic Review of Post-Quantum Hash-Based Signature Schemes, Security, and Optimizations,” *IEEE Access*, vol. 12, pp. 175969–175987, 2024, doi: 10.1109/ACCESS.2024.3485602.

[19] D. Gyasi-Nyarko, E. Freeman, M. M. Ujakpa, W. Amponsah, and S. O. Amoako, “A Systematic Review of Public Key Cryptography: Implementation, Challenges and Future Opportunities,” in *2025 IST-Africa Conference (IST-Africa)*, 2025, pp. 1–15. doi: 10.23919/IST-Africa67297.2025.11060567.

[20] P. Maitireni, V. Ncube, B. Ndlovu, and T. Sibanda, “Quantum Computing Cryptography : A Systematic Review of Innovations , Applications , Challenges , and Algorithms,” *J. Inf. Syst. Informatics*, vol. 7, no. 4, pp. 3668–3710, 2025, doi: 10.51519/journalisi.v7i4.1331.

[21] N. Sharma and P. G. Shambharkar, “A Systematic Literature Review of the Emerging Technologies used in Securing Healthcare Data,” in *2024 12th International Conference on Internet of Everything, Microwave, Embedded, Communication and Networks (IEMECON)*, 2024, pp. 1–12. doi: 10.1109/IEMECON62401.2024.10846068.

[22] M. Akkal, S. Cherbal, B. Annane, H. Lakhlef, and K. Kharoubi, “Quantum, post-quantum, and blockchain approaches for securing the internet of medical things: a systematic review,” *Cluster Comput.*, vol. 28, no. 10, p. 655, Oct. 2025, doi: 10.1007/s10586-025-05481-z.

[23] S. Cherbal, A. Zier, S. Hebal, L. Louail, and B. Annane, “Security in internet of things: a review on approaches based on blockchain, machine learning, cryptography, and quantum computing,” *J. Supercomput.*, vol. 80, no. 3, pp. 3738–3816, Feb. 2024, doi: 10.1007/s11227-023-05616-2.

[24] C. Nather, D. Herzinger, S. L. Gazdag, J. P. Steghofer, S. Daum, and D. Loebenberger, “Migrating Software Systems Toward Post-Quantum Cryptography-A Systematic Literature Review,” *IEEE Access*, vol. 12, no. June, pp. 132107–132126, 2024, doi: 10.1109/ACCESS.2024.3450306.

[25] M. J. Page *et al.*, “The PRISMA 2020 statement: an updated guideline for reporting systematic reviews,” 2021, doi: 10.1136/bmj.n71.

[26] W. Link, “CASP Checklist: For Cohort Studies”.

[27] S. Santhanam, V. Ravindran, and C. Wincup, “Critical appraisal of an original research article,” *J. R. Coll. Physicians Edinb.*, Sep. 2025, doi: 10.1177/14782715251369964.

[28] Z. H. Liu, X. B. Chen, and Y. Y. Xie, “A lattice-based group signature with backward unlinkability for medical blockchain systems,” *J. Inf. Secur. Appl.*, vol. 94, Nov. 2025, doi: 10.1016/j.jisa.2025.104226.

[29] J. Lee, W. Kim, and J. H. Kim, “A Programmable Crypto-Processor for National Institute of Standards and Technology Post-Quantum Cryptography Standardization Based on the RISC-V Architecture,” *Sensors*, vol. 23, no. 23, 2023, doi: 10.3390/s23239408.

[30] Z. G. Al-Mekhlaf *et al.*, “A quantum-resilient lattice-based security framework for internet of medical things in healthcare systems,” *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 37, no. 6, Aug. 2025, doi: 10.1007/s44443-025-00140-0.

[31] J. Jebrane and S. Lazaar, “An enhanced and verifiable lightweight authentication protocol for securing the Internet of Medical Things (IoMT) based on CP-ABE encryption,” *Int. J. Inf. Secur.*, vol. 23, no. 6, pp. 3691–3710, Dec. 2024.

[32] O. Popoola, M. A. Rodrigues, J. Marchang, A. Shenfield, A. Ikpehai, and J. Popoola, “An optimized hybrid encryption framework for smart home healthcare: Ensuring data confidentiality and security,” *Internet of Things (Netherlands)*, vol. 27, Oct. 2024, doi: 10.1016/j.iot.2024.101314.

[33] A. Astarloa, J. Lázaro, and J. I. Gárate, “CRYSTALS-Dilithium post-quantum cyber-secure SoC for wired communications in critical systems,” *Internet Things (The Netherlands)*, vol. 33, no. October 2024, p. 101656, 2025, doi: 10.1016/j.iot.2025.101656.

[34] M. Chaieb, K. Bou-Chaaya, and H. Rais, “EHRVault: A Secure,

Patient-Centric, Privacy-Preserving and Blockchain-Based Platform for EHR Management," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 14529 LNCS, pp. 119–140, 2024, doi: 10.1007/978-3-031-61231-2_9.

[35] M. Asif *et al.*, "Intelligent two-phase dual authentication framework for Internet of Medical Things," *Sci. Rep.*, vol. 15, no. 1, Dec. 2025, doi: 10.1038/S41598-024-84713-5.

[36] Sourav and R. Ali, "Lattice-based ring signcryption scheme for smart healthcare management," *Cluster Comput.*, vol. 27, no. 10, pp. 14131–14148, Dec. 2024.

[37] X. Zhang, C. Huang, Y. Zhang, J. Zhang, and J. Gong, "LDVAS: Lattice-Based Designated Verifier Auditing Scheme for Electronic Medical Data in Cloud-Assisted WBANs," *IEEE Access*, vol. 8, pp. 54402–54414, 2020, doi: 10.1109/ACCESS.2020.2981503.

[38] A. A. Al-saggaf, T. Sheltami, H. Alkhzaimi, and G. Ahmed, "Lightweight Two-Factor-Based User Authentication Protocol for IoT-Enabled Healthcare Ecosystem in Quantum Computing," *Arab. J. Sci. Eng.*, vol. 48, no. 2, pp. 2347–2357, Feb. 2023.

[39] N. Rajkumar, K. K. Kumar, M. Gokul, and S. Durai, "Post-Quantum Cryptography Security with CSPM for Secure Data Transmission in Cloud Environments," in *2024 4th International Conference on Ubiquitous Computing and Intelligent Information Systems (ICUIS)*, Institute of Electrical and Electronics Engineers Inc., 2024, pp. 1456–1462. doi: 10.1109/ICUIS64676.2024.10866709.

[40] Sourav and R. Ali, "Post-quantum secure health records: a blockchain-based lattice threshold signcryption scheme," *Cluster Comput.*, vol. 28, no. 7, pp. 1–23, Sep. 2025, Accessed: Oct. 09, 2025. [Online]. Available: https://link.springer.com/article/10.1007/s10586-025-05117-2

[41] B. B. Sezer and S. Akleylek, "PPLBB: a novel privacy-preserving lattice-based blockchain platform in IoMT," *J. Supercomput.*, vol. 81, no. 1, Jan. 2025.

[42] P. Bagchi *et al.*, "Public Blockchain-Envisioned Security Scheme Using Post Quantum Lattice-Based Aggregate Signature for Internet of Drones Applications," *IEEE Trans. Veh. Technol.*, vol. 72, no. 8, pp. 10393–10408, Aug. 2023, doi: 10.1109/TVT.2023.3260579.

[43] S. Prajapat, N. Kumar, A. K. Das, P. Kumar, and R. Ali, "Quantum-safe blockchain-assisted data encryption protocol for internet of things networks," *Cluster Comput.*, vol. 28, no. 1, pp. 1–15, Feb. 2025, Accessed: Oct. 28, 2025. [Online]. Available: https://link.springer.com/article/10.1007/s10586-024-04688-w

[44] A. Ahmad and J. Srirangan, "Quantum-safe mutual authentication scheme for IoHT using blockchain," *Results Eng.*, vol. 28, no. August, p. 106945, Dec. 2025, doi: 10.1016/j.rineng.2025.106945.

[45] H. B. Mahajan and A. A. Junnarkar, "Smart healthcare system using integrated and lightweight ECC with private blockchain for multimedia medical data processing," *Multimed. Tools Appl.*, vol. 82, no. 28, pp. 44335–44358, Nov. 2023, doi: 10.1007/S11042-023-15204-4.

[46] Y. Cao, S. Xu, X. B. Chen, G. Xu, Y. Chen, and Z. Li, "Towards attribute-based conjunctive encrypted search over lattice for internet of medical things," *Peer-to-Peer Netw. Appl.*, vol. 18, no. 5, Sep. 2025, doi: 10.1007/S12083-025-02089-3.

[47] R. I. Abdelfatah, R. M. Elsobky, and S. A. Khamis, "Ultra-secure quantum protection for e-healthcare images: Hybrid chaotic one-time pad with cipher chaining encryption framework," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 37, no. 6, pp. 1–43, Aug. 2025, doi: 10.1007/s44443-025-00155-7.

[48] B. Ndlovu and K. Maguraushe, "Balancing Ethics and Privacy in the Use of Artificial Intelligence in Institutions of Higher Learning: A Framework for Responsive AI Systems," *IJIE (Indonesian J. Informatics Educ.*, vol. 9, no. 1, p. 39, Jul. 2025, doi: 10.20961/IJIE.V9I1.100723.

[49] V. A. Muderere, B. Ndlovu, and K. Maguraushe, "Framework for Enhancing Interoperability, Data Exchange, and Security in Healthcare through Blockchain Technology," *Indones. J. Comput. Sci.*, vol. 12, no. 2, pp. 284–301, 2023, [Online]. Available: http://ijcs.stmikindonesia.ac.id/ijcs/index.php/ijcs/article/view/3135