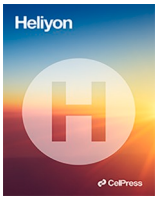
Heliyon 10 (2024) e31406

Contents lists available at ScienceDirect

Heliyon

journal homepage: www.cell.com/heliyon



Review article

Post-quantum healthcare: A roadmap for cybersecurity resilience in medical data

Morteza SaberiKamarposhti [a,*], Kok-Why Ng [a], Fang-Fang Chua [a], Junaidi Abdullah [a], Mehdi Yadollahi [b], Mona Moradi [c], Sima Ahmadpour [d]

[a] Faculty of Computing and Informatics (FCI), Multimedia University (MMU), 63100, Cyberjaya, Selangor, Malaysia
[b] Faculty of Computer Engineering, Islamic Azad University, Ayatollah Amoli Branch, Amol, Iran
[c] Department of Computer Engineering, Roudehen Branch, Islamic Azad University, Roudehen, Iran
[d] Graduate School of Business, Universiti Sains Malaysia, 11800, USM, Pulau Pinang, Malaysia

ARTICLE INFO

Keywords:
Post-quantum
Healthcare
Cybersecurity
Resilience
Medical data
Threats
Roadmap

ABSTRACT

As healthcare systems transition into an era dominated by quantum technologies, the need to fortify cybersecurity measures to protect sensitive medical data becomes increasingly imperative. This paper navigates the intricate landscape of post-quantum cryptographic approaches and emerging threats specific to the healthcare sector. Delving into encryption protocols such as lattice-based, code-based, hash-based, and multivariate polynomial cryptography, the paper addresses challenges in adoption and compatibility within healthcare systems. The exploration of potential threats posed by quantum attacks and vulnerabilities in existing encryption standards underscores the urgency of a change in basic assumptions in healthcare data security. The paper provides a detailed roadmap for implementing post-quantum cybersecurity solutions, considering the unique challenges faced by healthcare organizations, including integration issues, budget constraints, and the need for specialized training. Finally, the abstract concludes with an emphasis on the importance of timely adoption of post-quantum strategies to ensure the resilience of healthcare data in the face of evolving threats. This roadmap not only offers practical insights into securing medical data but also serves as a guide for future directions in the dynamic landscape of post-quantum healthcare cybersecurity.

1. Introduction

The healthcare sector is currently positioned to undergo a significant paradigm shift, which is primarily propelled by the rapid development of post-quantum technologies [1]. The emergence of conventional computational systems due to quantum computing, healthcare organizations are progressively acknowledging the imperative to modify and fortify their systems to safeguard against potential vulnerabilities. The utilization of post-quantum cryptography and quantum-resistant algorithms is increasingly crucial in order to protect sensitive patient data, given the potential for quantum computers to breach existing encryption techniques [2]. Healthcare researchers and practitioners are currently confronted with the complex task of incorporating post-quantum technologies into pre-existing infrastructures in a way that guarantees smooth interoperability and adherence to regulatory requirements [3].

In addition to their impact on cybersecurity, post-quantum technologies have a profound influence on fundamental aspects of

* Corresponding author.
E-mail addresses: msaberyk@ieee.org, msaberik@mmu.edu.my (M. SaberiKamarposhti).

https://doi.org/10.1016/j.heliyon.2024.e31406
Received 9 December 2023; Received in revised form 2 May 2024; Accepted 15 May 2024
Available online 16 May 2024

healthcare practices [4]. The computational capabilities of quantum computing are exceptional, which offers potential for the advancement of personalized medicine, optimization of treatment protocols, and acceleration of drug discovery. The utilization of quantum machine learning algorithms could enable the analysis of enormous datasets at an unprecedented rate, thereby facilitating the development of more precise diagnostics and treatment suggestions [5]. This change in thinking requires healthcare professionals to not only adapt technologically but also to adopt a new perspective that encourages interdisciplinary collaboration among computer scientists, quantum physicists, and medical specialists. In the context of the healthcare sector navigating the intricate terrain of the quantum era, adopting post-quantum technologies is not only a strategic decision but also a critical measure to guarantee the resilience, effectiveness, and ethical management of healthcare data [6]. At this threshold of a new era marked by unprecedented potential for change, we are simultaneously faced with the critical task of confronting the increased cybersecurity challenges that accompany these developments. This introductory section functions as the critical starting point for our comprehensive examination of cybersecurity resilience in the context of post-quantum medical data. Our research endeavors begin with a purposeful and comprehensive analysis of the historical and contextual environment that has influenced the development of healthcare technologies. By tracing the evolution from the most basic security measures implemented in the past to the complex network of interconnected systems that we now traverse, this background analysis aims to illuminate the path that has brought us to the present paradigm. The objective is to peel on the difficulties that require a fundamental change in our methodology to safeguard healthcare data, as well as to comprehend our technological odyssey.

In our investigation, the section pertaining to the Significance of Cybersecurity assumes a prominent position. In this, we explore the significant importance of resilient cybersecurity mechanisms in protecting confidential medical information in the evolving post-quantum environment. The potential proliferation of quantum technologies within healthcare systems raises concerns regarding the escalation of vulnerabilities and threats to patient confidentiality and data integrity. The objective of our investigation into the importance of cybersecurity is to emphasize the critical nature of taking proactive steps to strengthen the capacity of healthcare data to withstand the forthcoming risks presented by quantum developments. In the Purpose and Scope subsection, we provide a comprehensive delineation of the precise objectives that function as the guiding principles for our research undertaking. The roadmap presents a methodical framework for our investigation, facilitating comprehension of the extent and scope of our search. By establishing clear objectives and boundaries, an investigation can be directed towards practical and inventive resolutions of emergent threats as well as meticulous analysis of their intricacies. Our intention is to make a significant scholarly contribution to the conversation surrounding post-quantum healthcare cybersecurity by clearly articulating our objectives. This will help bridge the divide between revolutionary technological advancements and the critical requirement for improved data security protocols within the healthcare industry.

In the following, we shall proceed to examine the complex terrain of post-quantum healthcare cybersecurity, deciphering the challenges, investigating possible remedies, and devising a strategy to ensure the security and resilience of medical data in the era of quantum computing.

1.1. Background

The progression of healthcare technologies has been characterized by a series of progressive developments, every one of which has enhanced and broadened our capacities in the field of medical science. The healthcare industry has undergone a significant paradigm shift, commencing with the implementation of electronic health records (EHRs) and progressing to include advanced medical imaging technologies [7]. This evolution has been remarkable. However, as we traverse the intricate terrain of this historical development, the environment is prepared for an additional change in thinking due to the emergence of post-quantum technologies.

During the early phases of healthcare digitization, the storage and retrieval of patient information was primarily concerned with achieving optimal efficiency [8]. The implementation of electronic systems provided healthcare personnel with an unparalleled level of convenience and accessibility, allowing them to optimize administrative duties and improve the quality of patient care. Conversely, with the increasing dependence on digital technologies, the complexity of cyber threats correspondingly escalated. Classical cryptographic techniques [9], which were previously considered secure, have encountered growing susceptibilities as cyber threats continue to evolve [3]. The emergence of quantum computing, characterized by its exceptional computational prowess, presents a significant challenge to traditional encryption methods. The potential for quantum computers to decipher widely employed encryption algorithms introduces an unprecedented level of risk to the confidentiality of patient data.

The contemporary environment is distinguished by healthcare systems that are interconnected, storage in the cloud [10], and the pervasive utilization of the internet to transmit data. In the context of the current digital environment, susceptibilities to cyber threats have grown increasingly complex and ubiquitous. The healthcare industry is a specific target for malicious actors who aim to profit monetarily from sensitive patient data or compromise the confidentiality of medical records [11]. The objective of this historical analysis is to decipher the technological progression that has culminated in the present intersection of quantum computing and healthcare digitization. This emphasizes the importance of recognizing the susceptibilities that emerge as a result of quantum progress and the need for an initiative-taking assessment of our cybersecurity protocols. As we approach the commencement of this paradigm-shifting era, the historical backdrop provides the fundamental comprehension of the intricacies that demand a fundamental change in our methodology towards safeguarding healthcare information.

1.2. Significance of cybersecurity

It is impossible to exaggerate the importance of implementing strong cybersecurity protocols in the current healthcare environment, especially considering the revolutionary impact of post-quantum technologies. With the growing interconnectivity and

dependence of healthcare systems on digital infrastructures, safeguarding sensitive medical data becomes an imperative concern [12]. The following section explores the numerous facets of why a resilient cybersecurity posture is crucial in the post-quantum era.

To begin with, the subsection emphasizes the critical significance of cybersecurity in safeguarding the privacy and security of patient data [13]. The incorporation of quantum technologies presents unparalleled difficulties for conventional encryption techniques, thereby demanding novel and quantum-resistant methodologies to safeguard patient information against unauthorized access by malevolent actors [14]. Additionally, safeguarding the confidentiality of medical records and ensuring the secure transmission of data are paramount issues in the ever-changing healthcare environment. Medical information must be protected not only from unauthorized access but also from alterations that could compromise its precision and consistency. This subsection examines the potential ramifications of quantum threats on the integrity of data and emphasizes the necessity for cybersecurity strategies that can adapt [15].

Furthermore, with the growing adoption of telemedicine and other technological advancements within healthcare systems, this subsection underscores the criticality of cybersecurity measures to safeguard the confidence and dependability of remote healthcare exchanges [7]. When considering the security of telemedical data and the confidentiality of patient-physician communications, it is critical to have robust cybersecurity measures in place to prevent potential threats. So, the Importance of Cybersecurity section emphasizes the criticality of implementing strong cybersecurity measures to protect sensitive medical information in the era following quantum computing. This establishes a foundation for subsequent dialogues concerning inventive methodologies for ensuring cybersecurity resilience, underscoring the imperative of adopting initiative-taking measures to confront the ever-changing challenges in healthcare information security.

1.3. Purpose and scope

The Purpose and Scope section offers a detailed overview of the main objectives guiding this research project, acting as a roadmap that defines the range and extent of our inquiry in the dynamic realm of post-quantum healthcare cybersecurity.

The fundamental goal of this study is to provide nuanced contributions to the scholarly conversation about cybersecurity in the post-quantum healthcare era. The goals of this study are twofold: First, to conduct a thorough review of the vulnerabilities and threats that quantum technologies present to healthcare systems. And second, proposing practical and innovative solutions that increase the resistance of medical data against adversarial strategies based on quantum mechanics. Through establishing these two objectives, this study seeks to link theoretical understanding with real-world implementations, thereby ensuring applicability in scientific and operational environments. Our research covers a wide range of aspects of post-quantum healthcare cybersecurity. The complexities surrounding post-quantum technologies are explored, focusing on their implications for healthcare data integrity, communication strategies, cryptographic protocols, and authentication mechanisms. Significantly, this study goes beyond theoretical considerations by examining the practical implications of integrating and adopting post-quantum cybersecurity protocols into operational healthcare infrastructures.

Furthermore, this study's scope encompasses an exploration of the potential challenges and opportunities that may arise when integrating post-quantum cybersecurity into healthcare systems. It delves into regulatory considerations, interoperability issues, and the potential impact on patient care. The aim is to equip stakeholders, policymakers, and practitioners with a comprehensive understanding of the complexities involved in enhancing healthcare cybersecurity in the quantum era through clear scope definition. Essentially, the Aims and Scope subsection acts as a navigational tool, providing clear and precise direction for our research efforts. This study forms the basis for extensive research on cybersecurity in post-quantum healthcare and ensures that our findings significantly contribute to the evolving field of medical data protection in the age of quantum technology.

The manuscript is carefully structured to facilitate a logical examination of the intricate intersection of post-quantum technologies and cybersecurity within the healthcare sector. Following a broad introduction, subsequent sections unfold in a coherent order with the goal of providing a thorough understanding of the challenges and opportunities presented by the post-quantum era. Part 2 delves into the complexities of post-quantum technologies and their potential implications for healthcare cybersecurity. It offers a comprehensive review of emerging cryptographic methods, evaluates the potential risks posed by quantum computing, and establishes a foundation for a comprehensive understanding of the evolving healthcare landscape in the post-quantum computing era.

Section 3 expands on the aforementioned areas and outlines a systematic approach to strengthening cybersecurity protocols in the healthcare sector. It includes subsections addressing various topics such as techniques for ensuring data integrity, quantum-resistant encryption protocols, strategies for secure communication, and innovative authentication mechanisms. Each subsection contributes to the overarching goal of developing a tailored strategy to address the unique challenges posed by quantum advancements in healthcare. In the fourth and final section, the practical aspects of integrating post-quantum cybersecurity measures into existing healthcare infrastructures are explored. This section discusses the challenges that need to be overcome to implement quantum-secure solutions in operational healthcare systems, provides guidance on achieving regulatory compliance, and ensuring interoperability. The conclusions and essential insights obtained from the research are combined in the final section. Additionally, it outlines future research directions and practical implementations, emphasizing the ongoing need to adapt cybersecurity protocols to address ever-changing risks in the post-quantum healthcare landscape.

This methodical arrangement aims to provide the reader with a systematic and insightful progression that begins with an understanding of the theoretical foundations and concludes with practical implications and future considerations. Each section enhances the collective understanding of the challenges and solutions associated with safeguarding medical data in the continually evolving field of post-quantum technologies.

2. Post-Quantum Landscape in Healthcare

As we explore the unexplored areas of the post-quantum era in healthcare, this section undertakes a thorough investigation of the paradigm-shifting terrain influenced by nascent quantum technologies. Due to the dynamic convergence of quantum advancements and healthcare, a comprehensive examination of cryptographic techniques, potential threats, and the ever-changing landscape of data security is necessary. The section reflects the complex relationship between quantum technologies and the fundamental elements of cybersecurity in the healthcare industry. The subsequent section provides a comprehensive examination of post-quantum cryptographic methods, scrutinizing their suitability and robustness within the realm of healthcare [16].

The objective is to decipher the intricacies linked to encryption protocols and cryptographic mechanisms cutting-edge subtle of the advancements in quantum computing. Through an analysis of the merits and drawbacks of post-quantum cryptographic methodologies, this segment establishes the foundation for a sophisticated comprehension of the means by which healthcare information can be protected in the current epoch of increased computational capability. Moreover, the investigation examines the possible risks that quantum computation may present to healthcare information systems.

The section identifies and evaluates the adversarial environment that healthcare cybersecurity will face, from weaknesses in current encryption standards to the possibility of quantum-enhanced attacks. Conducting a comprehensive analysis is of the highest importance in order to develop targeted strategies that can effectively mitigate and counter potential risks, thus safeguarding healthcare data from quantum-based threats. The primary purpose of the Post-Quantum Landscape in Healthcare segment is to serve as an intellectual resource guide, enlightening readers about the prospects and intricacies that arise from the convergence of quantum technologies and healthcare data security. Through a thorough examination of post-quantum cryptographic techniques and a prediction of potential threats, this segment endeavors to furnish readers with an all-encompassing comprehension of the challenges and advancements that delineate the cybersecurity environment in the post-quantum healthcare sector.

2.1. Overview of post-quantum technologies

The advent of post-quantum technologies has brought about a fundamental change in cryptographic approaches, giving rise to a period in which conventional encryption protocols encounter unparalleled difficulties [17]. This subsection presents a thorough examination of the nascent post-quantum cryptographic methods and their ramifications for the security of healthcare [15]. In Fig. 1, an overview of post-quantum cybersecurity in healthcare is summarized.

2.1.1. Quantum-resistant encryption protocols

Encryption protocols are currently experiencing a significant and far-reaching evolution in preparation for the imminent quantum

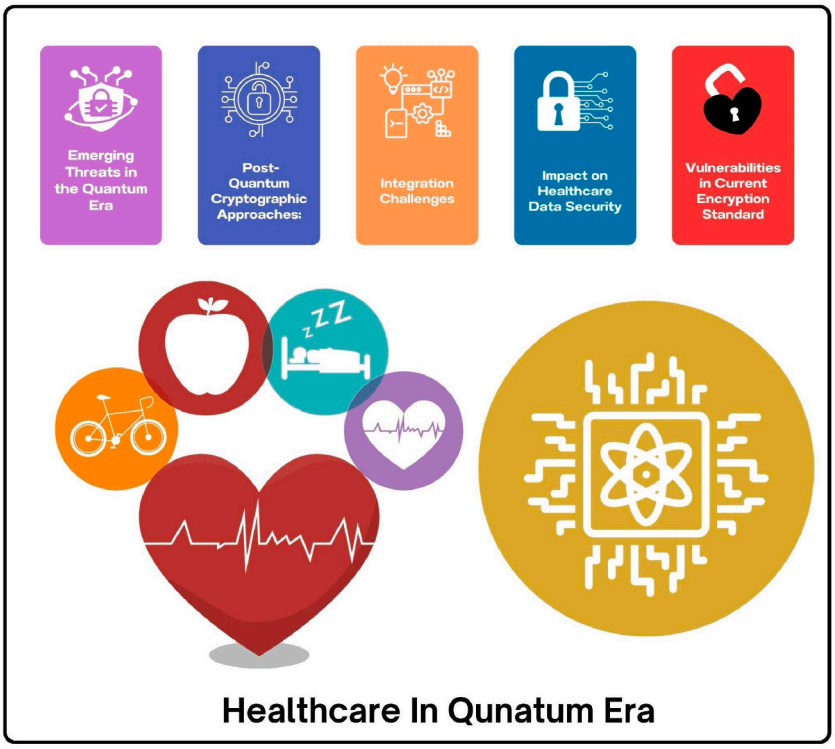


Fig. 1. Overview of post-quantum cybersecurity in healthcare.

era [18]. This subsection explores the complex domain of quantum-resistant encryption protocols, analyzing their underlying principles, advantages, and possible weaknesses in the context of healthcare cybersecurity [17].

2.1.1.1. Lattice-based cryptography. Lattice-based cryptography is a type of public-key encryption that relies on the mathematical concept of lattices. In cryptographic applications, lattices are discrete geometric structures that can be represented as points in space organized in a regular grid pattern determined by basis vectors. These structures present a variety of complex computational difficulties that form the foundation of the security of lattice-based cryptography systems [19].

Lattice-based cryptography is primarily focused on the intricacy of lattice problems such as the Shortest Vector Problem (SVP) and the Closest Vector Problem (CVP). The Shortest Vector Problem (SVP) involves finding the smallest non-zero vector in a lattice based on a specific norm. This task is challenging to approximate with a constant factor in high-dimensional spaces. CVP, in a similar vein, entails determining the nearest lattice point to a given non-lattice point, a problem that is also recognized as NP-hard. Lattice-based approaches show great promise for post-quantum cryptography as they are considered challenging not only under classical computing models but also against quantum algorithms [20].

The prominent algorithms in lattice-based cryptography encompass:

NTRU: It is an early and highly practical encryption technique based on lattice cryptography. NTRU functions within the context of polynomial rings and provides efficient and relatively straightforward encryption and decryption procedures. NTRU's security is based on the difficulty of solving the shortest vector problem in a convolutional modular lattice, which provides a distinct method for creating secure keys [21,22].

The Learning With Errors (LWE): It proposed by Oded Regev, entails the solution of linear equations with a minimal amount of noise, which is presumed to be computationally challenging. The problem of Learning With Errors (LWE) has emerged as a fundamental challenge in several cryptographic constructs, such as completely homomorphic encryption, pseudorandom functions, and more intricate systems like multilinear mapping [21,22].

Ring-LWE: It is a modified version of LWE that leverages ring theory to enhance efficiency. By exploiting the algebraic structure of rings, particularly polynomial rings, this method decreases the sizes of keys and computing times. This is achieved by simplifying operations and reducing the complexity of issues [21,22].

Lattice-based cryptography encompasses more than just the processes of encrypting and decrypting data. It also encompasses secure methods for exchanging keys, creating digital signatures, and implementing advanced cryptographic features such as:

Fully Homomorphic Encryption (FHE): Lattice-based constructions are at the forefront of FHE, which allows computation on encrypted data without needing to decrypt it first. This is crucial for maintaining privacy in cloud computing and data analytics [23,24].

Zero-Knowledge Proofs: Lattice structures enable the development of zero-knowledge proofs that are highly efficient and scalable, making them well-suited for blockchain technologies and secure voting systems [23,24].

Cryptographic Multilinear Maps: Cryptographic multilinear maps are utilized as instruments for constructing intricate cryptographic protocols, such as indistinguishability obfuscation and non-interactive zero-knowledge proofs. Lattices offer a method for creating these maps while assuming security, relying on challenging lattice issues [23,24].

Although lattice-based cryptography has numerous advantages, it has difficulties in handling extensive key sizes and achieving efficient implementation while maintaining security. Current studies in lattice cryptography focus on enhancing these elements by implementing novel algorithmic enhancements and developing new lattice structures. Overall, lattice-based cryptography is a robust and flexible set of cryptographic methods that have the capability to protect digital communications from both traditional and quantum threats. As the area progresses, it is anticipated to encompass a wider range of security applications, thereby strengthening its position in the realm of future-proof cryptography.

2.1.1.2. Code-based cryptography. Code-based cryptography is a field of cryptography that uses error-correcting codes to create encryption methods that are both secure and efficient. Derived on the influential research conducted by Robert McEliece in 1978, this method has been acknowledged for its ability to withstand attacks from quantum computers, making it a highly promising option in the realm of post-quantum cryptography. The fundamental basis of its security lies in the computational complexity of solving the decoding problem for general linear codes, which has been proven to be NP-complete [19,20].

The McEliece cryptosystem is the main cryptographic protocol used in code-based cryptography. This system employs a linear error-correcting code, usually a Goppa code, selected for its efficient decoding algorithms. The security of the McEliece system relies on the challenge of deciphering a random linear code, which remains a complex task even with the advent of quantum computing [19,20].

The McEliece cryptosystem is initialized by generating a public key, which is a modified and rearranged form of the generator matrix of the Goppa code. The private keys contain the original matrix and the permutation employed. Encryption entails the process of encrypting a message using a public key matrix and deliberately introducing errors. Decryption employs the secret key to execute syndrome decoding, rectifying these faults in order to recover the original message [19,20].

Over time, numerous adaptations of the original McEliece cryptosystem have been suggested with the aim of enhancing security and efficiency, or decreasing the size of encryption keys. Several noteworthy variations exist:

Niederreiter cryptosystem: The Niederreiter cryptosystem is a modified version of the McEliece system that employs parity-check matrices in place of generating matrices. Typically, it provides lower key sizes and offers the same level of security, making it attractive for specific uses.

Rank-based cryptography: Rank-based encryption employs rank metric codes instead of typical error-correcting codes. These codes

estimate the distance between codewords based on the rank of the matrix formed by their coordinates. These codes offer varying compromises in terms of security and performance.

LDPC and MDPC codes: Low-density parity-check (LDPC) and moderate density parity-check (MDPC) codes are types of error-correcting codes. LDPC and MDPC codes have been studied for their ability to develop more efficient cryptosystems with reduced key sizes, while yet maintaining security against quantum attacks. Applications and ongoing research in code-based cryptography encompass not just encryption and key encapsulation techniques, but also digital signatures and secure multiparty computing. These applications are being examined for their security against both classical and quantum assaults [19,20].

Current studies in code-based cryptography are primarily concerned with improving the efficiency of encoding and decoding operations, minimizing the size of encryption keys, and strengthening the security of these systems. For instance, efforts to combine McEliece with other post-quantum contenders seek to alleviate certain fundamental limitations, such as the often substantial sizes of the encryption keys.

Code-based cryptography encounters difficulties, specifically related to the length of the keys and the effectiveness of the encoding and decoding procedures, despite its advantageous security characteristics. Continual research is focused on improving algorithmic tactics and developing new code constructs to enhance the practicality of these systems for general deployment [19].

Overall, code-based cryptography continues to be an essential field of research in the development of cryptographic systems that are resistant to quantum attacks. The use of recognized difficulties in coding theory forms a strong basis for security, while continuous developments aim to address real deployment challenges. As the area progresses, it will persist in exerting a substantial influence on determining the future of secure communications in a world that follows the advent of quantum computing.

2.1.1.3. Hash-based cryptography. Hash-based cryptography is a branch of cryptography that uses cryptographic hash functions to create secure digital signatures and other cryptographic systems. Ralph Merkle first introduced this method in 1979, and it has gained recognition for its simplicity and ability to withstand quantum attacks. As a result, it is considered a strong contender for post-quantum encryption [19,25].

The security of hash-based cryptography relies on the characteristics of cryptographic hash functions, which are intentionally created as one-way functions. These functions are computationally efficient in one direction but extremely difficult to reverse. These functions must also demonstrate collision resistance (the property of being difficult to find two inputs that result in the same output) and preimage resistance (the property of being difficult to find an input that produces a certain output). Hash-based cryptographic systems largely rely on these qualities to ensure the security of digital communications, particularly for the production and verification of signatures [19,25].

The Merkle signature scheme (MSS) is a fundamental and widely recognized architecture in hash-based cryptography. It employs a binary hash tree, often known as a Merkle tree, to produce a significant quantity of one-time signatures using just one key pair. MSS involves the creation of a Merkle tree by the iterative hashing of node pairs. This process results in a tree structure where the leaves correspond to individual key pairs used for one-time signatures. The base of this tree functions as the public key, and the branches represent the secret keys employed for message signing. This architecture enables a substantial yet limited quantity of signatures from a single key setup, resulting in efficiency and security within specific usage conditions [19,25].

Also, the Extended Merkle Signature Scheme (XMSS) is a cryptographic signature scheme. XMSS is an improvement upon MSS, as it tackles certain practical limits of MSS, such as the need for maintaining state in the system. XMSS implements secure state handling algorithms and enhances the practical usefulness of hash-based signatures by providing forward security.

Furthermore, the LMS (Leighton-Micali Signature) is a cryptographic scheme that is similar to XMSS. It offers stateful hash-based signatures that are designed to be more adaptable and clear-cut compared to regular MSS. The LMS scheme is specifically customized to suit various operating scenarios.

Hash-based cryptography is mostly used for digital signatures, which are essential for verifying the authenticity of documents, distributing software securely, and ensuring secure communications. Hash-based signature schemes are crucial for building safe systems in anticipation of the future possibility of quantum computing compromising existing cryptographic protocols, due to their resistance to quantum attacks [19,25].

Contemporary studies in hash-based cryptography mostly concentrate on resolving the constraints of stateful signature schemes and investigating stateless signatures, which might alleviate some hazards and intricacies related to state management. Scientists are also striving to improve the effectiveness of these systems, decrease their computing and memory requirements, and boost their capacity to be used in many practical situations.

A significant obstacle in hash-based cryptography is the management of the statefulness of the signature schemes, which can create difficulties when implementing them in extensive or distributed systems. Moreover, the naturally substantial dimensions of the keys and signatures, especially in stateful systems, provide practical challenges in terms of storage and transmission [20,25].

Although there are difficulties, hash-based cryptography continues to be a strong and hopeful area in the realm of quantum-resistant cryptographic methods. The future implementation of this technology looks promising, particularly in situations where protection against quantum computing attacks is of utmost importance. This is due to its dependence on widely recognized cryptographic hash functions and the continuous enhancements in efficiency and usability. Hash-based cryptography is a crucial element of the contemporary cryptographic toolset, particularly in anticipation of the advent of quantum computing. Given the ongoing advancements in the field, it is quite probable that it will have a substantial impact on safeguarding digital communications from emerging dangers.

2.1.1.4. Multivariate polynomial cryptography (MPC). Multivariate Polynomial Cryptography (MPC) is a subset of public-key cryptography that employs multivariate polynomials over finite fields to safeguard digital communications. Because solving systems of multivariate polynomial equations is known to be NP-hard, MPC provides a reliable platform for encryption, digital signatures, and other cryptographic applications. The field of cryptography has garnered interest due to its ability to resist quantum attacks, making it a promising option for post-quantum cryptographic applications.

Typically, MPC systems utilize two sets of variables and three mappings. In these systems, the key generation procedure usually involves the creation of a pair of public and private keys derived from intricate multivariate polynomial equations. The essence of MPC resides in the challenge of solving these equations when there are several variables and non-linear interactions at play [26].

The security framework for MPC is centered on the Multivariate Quadratic (MQ) Problem, which entails the discovery of solutions to systems of quadratic equations inside a finite field. This problem is recognized as NP-hard, which establishes a strong basis for the security of systems based on MPC.

The prevailing MPC scheme typically consists of three primary elements: a central quadratic map F that is concealed within two affine transformations S and T. In this context, S and T are used as the private key, whereas the combination of S, F, and T constitutes the public key. This configuration adds complexity to direct assaults on F, ensuring the system's protection against illegal decryption or fabrication of signatures.

Also, the Hidden Field Equations (HFE) is a widely recognized system within the field of MPC. HFE employs a unique polynomial that streamlines the process of decryption or signature verification. HFE focuses on polynomials over an extension field, providing a trade-off between operational intricacy and computational effectiveness [19,26].

MPC has predominantly been utilized in the domain of digital signatures, exemplified by famous systems such as Quartz, HFEv-, and Sflash. Nevertheless, as weaknesses were revealed in certain first implementations, the attention turned towards improving the strength and effectiveness of these systems.

Presently, the focus of research in MPC is primarily on creating novel schemes that can offer enhanced security while requiring less computational resources and employing simpler key management protocols. This involves investigating novel polynomial structures and affine transformations that are more resistant to linearization and other sorts of algebraic assaults.

Although MPC has strong theoretical foundations, it encounters substantial obstacles. The techniques frequently yield large keys and intricate operations, especially for encryption and decryption procedures. Another difficulty is to guarantee that the systems are resilient against both classical and quantum attacks, particularly those that exploit sophisticated algebraic techniques [19,26,27].

Efforts to enhance the practicality of MPC involve optimizing the structure of polynomial equations to decrease the size of public keys and the computing burden of key generation and decryption procedures. Additionally, there is an emphasis on the advancement of hybrid systems that integrate the advantages of MPC with other cryptographic methods in order to improve overall security and efficiency.

To summarize, Multivariate Polynomial Cryptography is a novel and auspicious method in the field of cryptography, specifically in anticipation of the obstacles posed by quantum computing. Although there are challenges to be addressed, particularly in terms of practical application, the continuous research and development in this domain are expected to result in substantial progress, solidifying MPC's position as a fundamental element of future cryptographic standards.

2.2. Emerging threats in the quantum era

The emergence of quantum technologies introduces a fundamental change in computational capabilities, which concurrently presents unparalleled challenges to traditional cybersecurity protocols and provides prospects for groundbreaking advancements. This subsection conducts a thorough analysis of the emergent threats that healthcare information systems [28] encounter in the quantum era, thereby strengthening our comprehension of the adversarial environment.

2.2.1. Quantum-enhanced attacks on cryptographic protocols

This section examines the complex domain of quantum-enhanced attacks, shedding light on the potential risks that traditional cryptographic protocols may pose in the ever-changing field of healthcare cybersecurity. Through an examination of the functionalities of quantum algorithms, with a specific focus on Shor's algorithm and Grover's algorithm, our objective is to furnish a comprehensive comprehension of the susceptibilities that healthcare information systems might encounter during the quantum age [29].

Shor's algorithm, a revolutionary quantum algorithm developed by mathematician Peter Shor in 1994, brought about a fundamental transformation in the field of cryptography. Shor's algorithm is specifically engineered to factor large composite numbers in an efficient manner [30]. This is a fundamental challenge faced by numerous classical public-key cryptographic systems, including RSA (Rivest–Shamir–Adleman). The algorithm's capacity to accelerate the factorization process exponentially in comparison to the most well-known classical algorithms is its source of significance.

The efficiency of traditional factorization algorithms diminishes with the enlargement of the numbers requiring factorization. In public-key cryptography, secure encryption is based on the challenge of factoring the product of two enormous prime numbers, which is an application of this property. When executed on a quantum computer with adequate power, Shor's algorithm exhibits the ability to factor substantial numbers at an exponential rate, surpassing the speed of even the most renowned classical algorithms. This development presents a substantial peril to prevalent cryptographic protocols [31].

By capitalizing on the principles of quantum superposition and entanglement, Shor's algorithm efficiently parallelizes quantum operations in a manner that classical algorithms fail to achieve [32]. The modular exponentiation and the quantum Fourier transform are the two primary components of the algorithm. By converting the issue from the time domain to the frequency domain, the former

method takes advantage of quantum parallelism to a significant degree. The final stage employs modular arithmetic in an efficient manner to determine the period of a modular exponentiation function, which is an essential element in the process of factoring large numbers.

The proliferation of interest in post-quantum cryptography was stimulated by the development of Shor's algorithm, which exposed the susceptibility of prevalent cryptographic systems to quantum attacks [33]. Cryptographers and researchers have been diligently investigating and fabricating alternative cryptographic schemes that are thought to be impervious to quantum attacks, including lattice-based, hash-based, and code-based cryptography. In the ongoing struggle for quantum-resistant cryptography and quantum computation, Shor's algorithm continues to be a seminal achievement in the development of cryptographic protocols and practices. Through the evaluation of the susceptibilities introduced by Shor's algorithm, professionals in healthcare cybersecurity are able to ascertain the critical nature of the transition towards quantum-resistant encryption [33].

Although not in direct opposition to public-key cryptography, Grover's algorithm presents an innovative pathway for the analysis of symmetric-key cryptanalysis. Grover's algorithm, which was introduced by Lov Grover in 1996, is an additional influential quantum algorithm that pertains to a distinct facet of cryptography in contrast to Shor's algorithm [34]. The objective of Shor's algorithm is to factor large numbers efficiently, a capability that may compromise specific cryptographic schemes. In contrast, Grover's algorithm is designed to solve the problem of unsorted database search or to accelerate the search of unstructured databases.

An average of $O(N)$ operations is required to search an unsorted database containing N items in traditional computing. In contrast, Grover's algorithm, when executed on a quantum computer, attains a quadratic acceleration, resulting in a reduction of the search time to approximately $O(-N)$ operations. This indicates that Grover's algorithm for seeking solutions in an unstructured database may be exponentially quicker than classical algorithms [34].

By utilizing interference and quantum parallelism, the algorithm increases the likelihood of discovering the correct solution. A sequence of quantum operations is utilized, such as amplitude amplification and quantum oracle queries, to increase the probability of accurately measuring the solution during quantum state measurement. The utilization of quantum parallelism in Grover's algorithm enables the concurrent exploration of numerous possibilities, resulting in a quadratic acceleration in comparison to classical algorithms [25].

In addition to having significant ramifications for database optimization and search issues, Grover's algorithm possesses cryptographic importance. More precisely, it compromises symmetric-key cryptography by reducing the length of the effective key by half. To illustrate, employing Grover's algorithm to brute force a symmetric key that would have demanded 2^{128} operations using classical algorithms would only necessitate approximately 2^{64} operations. In a quantum computation environment, cryptographic practitioners frequently employ larger key sizes to thwart this threat.

The continuous pursuit of quantum-resistant cryptographic algorithms is further complicated by the ramifications of Grover's algorithm on cryptography, as quantum computing technology progresses [17]. This represents an additional facet of the competition between quantum computing and quantum-safe cryptography within the domain of information security. In order to ensure the efficient transmission of data, healthcare systems frequently utilize symmetric-key algorithms. Therefore, it is critical to comprehend the quantum threats that Grover's algorithm presents in order to develop appropriate countermeasures.

s, which are essential for classical cryptography to maintain data integrity, generate hash values, which are fixed-size representations of data sets of variable size. Hash values, which are frequently called message digests, facilitate the verification of data integrity in a timely and effective manner. Nevertheless, the introduction of quantum algorithms, specifically Shor's and Grover's algorithms, presents obstacles to the integrity of traditional hash functions [25]. Shor's algorithm, renowned for its ability to factor large numbers at an exponential rate compared to classical algorithms, poses a direct risk to the security of hash functions which depend on the challenge of factorizing such numbers. Public-key cryptography and numerous widely employed cryptographic protocols rely on the resistance to collisions exhibited by hash functions. The collision resistance of these hash functions would be compromised if an adversary could effectively factor large numbers using Shor's algorithm. This could potentially result in the generation of malicious hash collisions, which would compromise the integrity of digital signatures and certificates [34].

Conversely, Grover's algorithm, which was specifically engineered for quantum search, expedites the discovery of pre-images of hash functions by a quadratic degree. This implies that when implemented on a quantum computer, hash functions that are considered secure in the classical sphere due to their dependence on computational complexity may become susceptible to brute-force attacks. The essential pre-image resistance property of hash functions, which guarantees that deducing the original input data from its hash value is computationally impracticable, is jeopardized by Grover's algorithm [34].

In response to these challenges, post-quantum cryptography is currently engaged in active research and development of hash functions that are resistant to quantum attacks [32]. These encompass lattice-based cryptography-based hash functions, hash-based message authentication codes (HMACs), and additional methodologies designed to endure the computational prowess of quantum algorithms [35]. The ongoing competition between quantum computing and quantum-resistant cryptography necessitates the development of hash functions that can effectively mitigate the vulnerabilities introduced by these potent quantum algorithms in order to safeguard data integrity in the quantum era. By conducting an extensive examination of quantum-enhanced attacks, the objective of this section was to furnish healthcare cybersecurity professionals and decision-makers with a deep comprehension of the susceptibilities intrinsic in current cryptographic protocols. By proactively preparing for and anticipating these quantum threats, the healthcare industry can ensure the ongoing confidentiality, integrity, and authenticity of medical data in the quantum era through the implementation of security measures that are resistant to quantum attacks. As it is illustrated in Fig. 2, vulnerabilities in current states and threats in quantum age are summarized.

2.2.2. Vulnerabilities in current encryption standards

This subsection conducts a thorough analysis of the weaknesses that are currently found in encryption standards. It reveals the complex challenges that quantum advancements present to cryptographic protocols that are extensively employed in the healthcare cybersecurity domain. Symmetric-key encryption [36], which is fundamental to the secure transmission of data, is susceptible to weaknesses introduced by quantum computing. This segment provides an analysis of how algorithms, including Grover's, have the potential to significantly diminish the exertion needed to execute brute-force attacks, which may compromise the confidentiality of healthcare data. Through an examination of the susceptibilities inherent in symmetric-key encryption, cybersecurity experts in the healthcare industry can devise a plan to migrate to algorithms resistant to quantum attacks, thereby guaranteeing the preservation of data privacy in the era following quantum computing [37].

Public-key cryptography, which is essential for ensuring secure communication and authentication, faces significant vulnerabilities due to the implementation of quantum algorithms such as Shor's [38]. This segment of the subsection analyses the potential ramifications for public-key algorithms that are extensively employed, such as RSA and ECC. It is critical for healthcare systems that utilize public-key cryptography for secure data exchange and digital signatures to have a comprehensive understanding of these vulnerabilities. The investigation further examines the pressing need to implement quantum-resistant alternatives in order to protect the authenticity and integrity of healthcare data [7].

Also, the exploitation of hash functions, which are indispensable for ensuring data integrity and digital signatures, can occur through the actions of quantum adversaries. The potential compromise of hash-based constructions by Shor's algorithm, which could jeopardize the integrity of healthcare data, is examined. This study investigates the susceptibilities of hash functions, with the intention of directing healthcare cybersecurity experts towards alternatives that are secure against quantum attacks and preserve the integrity of data in the quantum era [39]. Furthermore, key exchange protocol risks are introduced by quantum computing, which has the potential to compromise the fundamental principles of secure communication. This segment of the subsection delves into the difficulties that are presented to commonly employed key exchange mechanisms, including Elliptic Curve Diffie-Hellman and Diffie-Hellman. Comprehending the susceptibilities present in key exchange protocols is crucial in order to fortify healthcare communication channels; thus, the urgent need to migrate to key exchange algorithms resistant to quantum attacks is underscored.

Through an examination of the weaknesses present in existing encryption protocols, this section provides healthcare cybersecurity professionals with an all-encompassing comprehension of the hazards presented by quantum computing. Armed with this information, stakeholders will be able to effectively manage the intricacies associated with the adoption of quantum-resistant encryption, thereby safeguarding healthcare data security against the ever-changing dangers posed by quantum threats.

2.2.3. Quantum threats to health data privacy

This subsection explores the significant ramifications of quantum computing on the privacy of health data. It critically evaluates the possible risks and susceptibilities that could undermine the confidentiality and integrity of sensitive medical data in the ever-changing quantum environment [40]. The utilization of quantum computing, specifically algorithms such as Shor's, presents a substantial menace to conventional data encryption techniques [13]. This segment delves into the manner in which quantum adversaries might exploit encryption vulnerabilities in order to acquire unauthorized access to health records. Critical privacy concerns are raised by the potential compromise of encrypted health data, underscoring the importance of implementing quantum-resistant encryption measures to protect patient confidentiality [41].

Data encryption compromises in healthcare present distinctive challenges and concerns in the quantum age, given that the security of conventional encryption methods employed to safeguard sensitive medical information may be jeopardized by the potential introduction of quantum computers [42]. When implemented on a large scale, quantum computers will possess the strength to breach prevalent encryption algorithms, including those that rely on discrete logarithm problems or factorization, which form the foundation

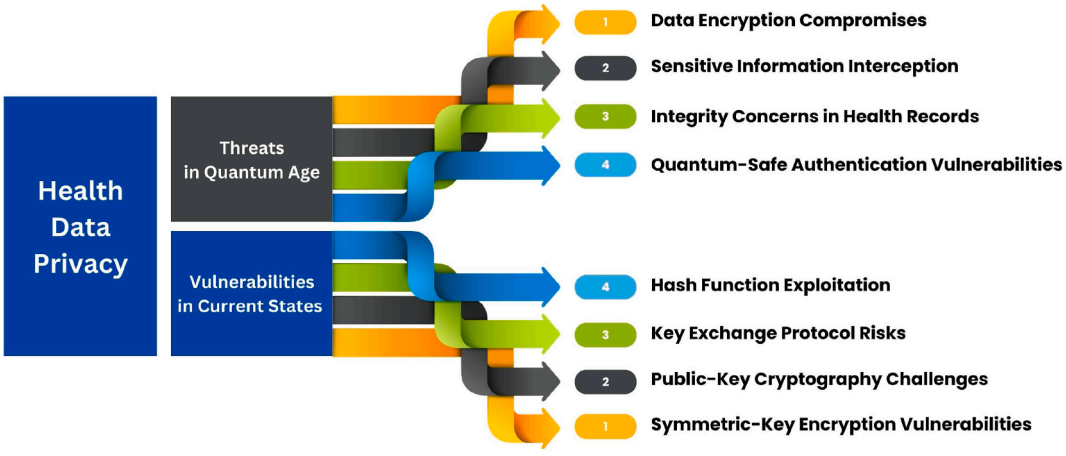


Fig. 2. Vulnerabilities in current state and threats in quantum age.

of a significant portion of the existing security infrastructure. A notable vulnerability exists in the erosion of patient confidentiality [43]. On a regular basis, healthcare organizations and providers manage enormous quantities of sensitive patient data, which may consist of unique identifiers, medical records, and course of treatment. Unauthorized access to this information becomes a more significant concern in the quantum age if encryption methods are compromised. Such unauthorized access could potentially result in privacy violations, identity theft, and unauthorized alterations to medical records [44].

Additionally, encrypted communication channels are employed extensively by healthcare systems to ensure the security of patient data during transmission among various entities comprising the healthcare ecosystem—hospitals, clinics, insurers, and laboratories. Patient information in transit could be jeopardized if these communication channels were vulnerable to interception and unauthorized access due to compromised encryption. The significance of key management in the healthcare sector is amplified in the quantum age [43]. For the purpose of encrypting and decrypting data, encryption keys must be stored and managed securely. A breach in key management has the potential to result in unauthorized access, data breaches, or medical record manipulation. Ensuring the enduring security of patient data is contingent upon the capacity to modify critical management practices in order to counter the potential risks presented by quantum computers [45].

The proliferation of digital health technologies within the healthcare sector, such as telemedicine, wearable devices, and electronic health records, contributes to an expansion of the attack surface for potential compromises in encryption [46]. In the dynamic realm of digital healthcare, the continual security and integrity of patient data necessitate the implementation of quantum-resistant encryption techniques.

Healthcare organizations must proactively transition to quantum-resistant cryptographic algorithms in order to address these challenges. In an effort to identify and standardize quantum-resistant cryptographic solutions that can substitute for susceptible encryption methods, ongoing research and development is in progress [46]. In addition, regular security audits, comprehensive cybersecurity policies, and continuous security awareness training for healthcare professionals are critical elements of a comprehensive approach to mitigate the risks associated with breaches in data encryption in the quantum age of healthcare. It is of the utmost importance to maintain encryption resilience at the forefront of quantum technology developments in order to protect the confidentiality and integrity of sensitive patient information [47].

Also, the interception of confidential healthcare information has become a more significant concern in the quantum age due to the security risks posed by quantum computers to conventional encryption techniques [48]. When fully operationalized, quantum computers have the potential to eliminate the need for numerous prevalent encryption algorithms, thereby introducing susceptibilities to the safeguarding of sensitive healthcare data. The ramifications of this interception risk are extensive, specifically with regard to safeguarding patient privacy and the fundamental trustworthiness of healthcare infrastructure [49].

An area of significant concern pertains to the interception of patient health records in the course of data transmission [50]. Healthcare systems are highly dependent on encrypted communication channels in order to transmit patient information between hospitals, clinics, insurers, laboratories, and other entities in a secure manner. The potential for quantum computing capabilities to compromise encryption could result in the decryption of intercepted data, which could grant unauthorized access and expose patients' private medical information. In the era of telemedicine, where a significant portion of patient-physician communication takes place via digital channels, this risk is further intensified.

Identification theft and fraud may also ensue from the interception of sensitive health information [51]. An abundance of personally identifiable information, such as social security numbers, addresses, and insurance particulars, is frequently found in patient records. This information, if compromised and decrypted, could be utilized maliciously to place patients at risk of identity theft and financial injury.

The interception of medical research and development data emerges as a substantial concern in the era of quantum technology [52]. On a routine basis, pharmaceutical companies and research institutions interchange sensitive data pertaining to drug development, clinical trials, and novel medical technologies. The compromise of encryption during transit may result in the unauthorized acquisition of confidential data, which may impede progress in the field of medicine and pose a risk to public health.

There is an immediate need to implement quantum-resistant cryptographic solutions in order to mitigate the risk of unauthorized access to sensitive information in the quantum age of healthcare [53]. It is imperative for healthcare organizations to adopt encryption methods that are resistant to the computational capabilities of quantum computers. In addition, stringent access controls, robust security protocols, and routine cybersecurity training for healthcare professionals are critical elements of a comprehensive strategy designed to safeguard against unauthorized access and interception.

The healthcare sector must remain at the vanguard of quantum-resistant cybersecurity measures in order to safeguard sensitive patient data and maintain its confidentiality, integrity, and security as quantum technologies progress. Adopting this proactive stance is crucial for preserving confidence in healthcare systems and protecting the welfare of individuals in a healthcare environment that is becoming more digital and interconnected [54]. Furthermore, the integrity of health records emerges as a critical concern in the quantum age due to the potential threat that quantum computers pose to conventional cryptographic techniques used to protect such data. It is essential that health records maintain their integrity in order to guarantee that patient data continues to be accurate, untainted, and dependable. The capabilities of quantum computing, specifically algorithms such as Shor's and Grover's, may inadvertently compromise the confidentiality of health records via diverse methods.

The potential for interference with medical data during transmission is a major concern [55]. The exchange of health records among healthcare providers, insurers, and other participants in the healthcare ecosystem is a regular occurrence. The information in transit could potentially be intercepted and altered by adversaries if quantum computers manage to compromise encryption methods. Misinformation, incorrect diagnoses, and inappropriate treatments may result from this manipulation, posing grave risks to patient health. A further significant concern is the potential compromise of hash functions that are employed in the process of verifying data

integrity. Hash functions produce representations (hash values) of variable-sized data that have a fixed size, thereby enabling efficient integrity checks [56]. However, as the quantum age progresses, specific hash functions may become less effective, allowing malicious actors to potentially manipulate health records undetected. This compromise may undermine confidence in the precision and dependability of health information.

An additional topic of concern pertains to the implementation of digital signatures in healthcare records [57]. Digital signatures enable the authentication of the provenance and authenticity of electronic documents. Nevertheless, the integrity of digital signatures is contingent upon the complexity of specific mathematical challenges that can be efficiently resolved by quantum computers. The potential for adversaries to generate forged digital signatures as a result of quantum computing advancements could compromise the integrity of health records, thereby enabling fraudulent activities or unauthorized modifications. In order to mitigate these integrity concerns that arise in the context of healthcare during the quantum age, it is critical to implement quantum-resistant cryptographic techniques. The implementation of encryption, hash functions, and digital signatures that are impervious to quantum attacks should be a top priority for healthcare organizations. Furthermore, it is imperative to incorporate secure key management practices, enforce stringent access controls, and conduct routine audits of health record integrity as fundamental elements of a comprehensive approach to protect healthcare data [58].

Ensuring the integrity of health records in the context of the quantum age necessitates continuous vigilance and adjustment to emergent cryptographic standards. It is imperative for healthcare providers to remain informed about the latest developments in quantum-resistant cryptography and revise their security protocols accordingly. This is necessary to safeguard patient information amidst the ever-changing technological environment [50]. The issue of quantum-safe authentication vulnerabilities in the healthcare sector is a critical one, given the rapid progress of quantum computing that poses a threat to the security of conventional authentication techniques. A vital component of healthcare systems, authentication ensures that access to sensitive patient records and medical information is restricted to authorized personnel only. Given their potential to compromise widely used cryptographic protocols, the emergence of quantum computers presents unique challenges to the healthcare industry's authentication mechanisms.

A significant susceptibility exists in the compromise of conventional public-key cryptography, which is commonly employed in authentication procedures. PKI, comprising public-key algorithms and digital certificates, serves as the foundation for secure authentication in a number of healthcare systems [59]. Conventional PKI is predicated on the underlying mathematical problems that could be efficiently solved by a quantum computer of sufficient power, such as factoring large numbers or solving discrete logarithms. Unauthorized access and manipulation of sensitive health records may result from this.

An additional point of vulnerability emerges from the potential compromise of secure key exchange protocols, such as the extensively utilized Diffie-Hellman key exchange, which guarantees secure communication channels. The protocols' susceptibilities could be capitalized upon by quantum computers, thereby enabling adversaries to surveil communication sessions or assume the guise of authentic users throughout authentication procedures. Biometric authentication methods, which are widely employed in the healthcare sector to guarantee the confidentiality of medical records, are also susceptible to quantum threats [60]. Grover's quantum algorithm has the potential to compromise the security of database-stored biometric templates. The potential for unauthorized access arises when an adversary is capable of reverse engineering or reconstructing biometric data using compromised templates.

In the realm of healthcare, these vulnerabilities necessitate the implementation of quantum-resistant authentication mechanisms [61]. Active research and development efforts are being devoted to post-quantum cryptographic solutions, such as code-based, hash-based, and lattice-based cryptography, in order to mitigate the potential risks presented by quantum computers. It is imperative for healthcare organizations to engage in initiative-taking evaluation and revision of their authentication systems, incorporating quantum-safe algorithms in order to safeguard sensitive patient information.

Furthermore, the significance of multi-factor authentication (MFA) is heightened in the era of quantum computing. By integrating supplementary security measures, such as biometrics or one-time codes, with conventional authentication methods, healthcare systems can fortify their resistance to quantum threats. In light of advancements in quantum technologies, it is imperative for the healthcare sector to maintain a state of constant vigilance, acquire knowledge regarding authentication methods resistant to quantum attacks, and enforce strong security protocols to safeguard patient privacy and preserve the integrity of healthcare infrastructures amidst emerging quantum complexities.

3. Roadmap for cybersecurity resilience

This critical section of our investigation outlines an all-encompassing strategy for bolstering the resilience of cybersecurity in the ever-changing landscape of post-quantum healthcare [62]. By incorporating secure communication strategies, innovative authentication mechanisms, quantum-resistant encryption protocols, and data integrity assurance, this strategic roadmap fortifies healthcare information systems against emerging threats.

3.1. Secure communication strategies

This crucial segment elucidates the complexities associated with secure communication strategies in the realm of cybersecurity for post-quantum healthcare. Through the utilization of secure messaging protocols, quantum-resistant key exchange mechanisms, and fortified telemedicine channels, this subsection furnishes healthcare professionals with an all-encompassing blueprint to guarantee the confidentiality and integrity of medical data during transmission. For communication to be secure, robust key exchange protocols are required. This subsection delves into quantum-resistant key exchange mechanisms, which serve as the fundamental building blocks of secure channels, in the post-quantum era. Kyber [63], NTRUEncrypt [64], and NewHope [65] are examined in terms of the practical

considerations and cryptographic principles that govern these post-quantum key exchange algorithms. By comprehending the measures that healthcare practitioners can take to withstand quantum adversaries, they are better equipped to establish secure communication channels that are impervious to quantum threats.

Secure messaging protocols are of utmost importance in healthcare communication as they necessitate the implementation of strategies that ensure the protection of transmitted information's confidentiality and integrity. This segment explores secure messaging protocols that are resistant to quantum attacks, with a particular focus on the underlying principles that drive methods such as FrodoKEM [66] and NTRUEncrypt [67]. Through the analysis of the cryptographic methods utilized, healthcare practitioners are able to determine which secure messaging protocols are optimal for their particular communication requirements. The development and execution of secure messaging strategies in healthcare systems are guided by factors such as scalability, resistance to quantum attacks, and efficiency. The fortification of telemedicine channels is crucial as they serve as a critical means of facilitating remote healthcare interactions. This subsection discusses the distinct challenges and prospects presented by telemedicine within the context of the post-quantum era. An investigation is conducted into secure communication strategies for telemedicine that are resistant to quantum attacks, such as protocols for data transmission and video conferencing. Through proactive identification of potential risks and susceptibilities within telemedicine channels, professionals in healthcare cybersecurity can strengthen the security and privacy of patient information during remote healthcare interactions, thereby deterring quantum adversaries.

By conducting a comprehensive analysis of secure communication strategies, the objective of this subsection was to provide healthcare professionals with the information and resources necessary to establish robust communication channels in the era following quantum computing. Healthcare systems can proactively safeguard the confidentiality and integrity of medical data against emerging quantum threats by implementing secure messaging protocols, adopting quantum-resistant key exchange mechanisms, and fortifying telemedicine channels. These measures will enable health systems to navigate the complexities of secure communication.

3.2. Authentication mechanisms

This critical section explores the complex domain of authentication mechanisms that have been specifically designed for the cybersecurity environment in post-quantum healthcare [68]. Through an examination of multi-factor authentication strategies, quantum-resistant cryptographic key management, and innovative biometric authentication, this subsection equips healthcare professionals with an all-encompassing road map to guaranteeing secure access control amidst the ever-changing landscape of quantum threats.

Since authentication frequently relies on cryptographic keys, quantum adversaries view them as a prominent target. This segment delves into methods for managing cryptographic keys that are resistant to quantum attacks. It includes a discussion of hash-based message authentication codes (HMACs) and the implementation of quantum-resistant cryptographic primitives [69]. Through a critical analysis of the underlying principles and resilience of these pivotal management techniques in the face of quantum attacks, healthcare practitioners can strengthen authentication mechanisms and guarantee that only authorized individuals are granted access to healthcare systems and confidential patient information.

Also, we delve into the potential of biometric authentication as a means of ensuring secure access control, while also examining its robustness against quantum threats. We explore novel biometric methodologies that capitalize on physiological and behavioral attributes, including but not limited to behavioral biometrics, fingerprint recognition, and retinal scanning. Through evaluating the efficacy and dependability of these biometric techniques in the age of quantum computing, medical professionals can deploy authentication systems that are impervious to quantum-based attacks and offer a streamlined and intuitive user experience.

The implementation of multi-factor authentication (MFA) enhances security measures through the integration of numerous authentication factors. This segment assesses multi-factor authentication (MFA) strategies that are resistant to quantum attacks [70]. It takes into account various combinations of physical attributes, digital credentials, and intellectual capabilities (e.g., smart cards), as well as biometrics. Through a critical examination of the quantum resilience exhibited by various MFA factors, healthcare practitioners have the ability to develop authentication systems that are not only impervious to quantum threats but also flexible enough to accommodate the varied requirements and inclinations of users in healthcare environments.

Furthermore, for access control, behavioral authentication utilizes unique patterns in user behavior [71]. This subsection delves into the potential contribution of behavioral biometrics, including patterns of cursor movement and keystroke dynamics, to the development of quantum-resistant authentication. Through an analysis of the robustness of behavioral authentication in the face of quantum adversaries and a consideration of possible challenges, professionals in healthcare cybersecurity can devise novel and user-centric authentication methods that are compatible with the quantum age.

The Authentication Mechanisms subsection endeavors to provide healthcare professionals with the information and resources necessary to implement robust access control systems in the post-quantum era by means of this comprehensive examination. Healthcare systems can prevent unauthorized access and safeguard patient data in an ever-changing quantum environment by implementing multi-factor authentication, quantum-resistant cryptographic key management, and innovative biometric authentication techniques.

3.3. Data integrity assurance

This crucial segment delves into methodologies and technologies that are specifically designed to ensure the integrity of data in the ever-changing landscape of cybersecurity in post-quantum healthcare [72]. The integration of blockchain applications and quantum-resistant hash functions is centered around the objective of safeguarding medical records against nascent quantum threats

while maintaining their integrity and reliability. Quantum-resistant hash functions are essential components in maintaining the integrity of data. In this subsection, we shall examine hash functions that are resistant to quantum algorithms' computational power.

By investigating structures such as hash-based message authentication codes (HMACs) and hash functions that are impervious to quantum Grover's algorithm, our objective is to offer healthcare practitioners guidance on how to choose hash functions that provide strong defenses against quantum adversaries. Practical considerations, including the efficacy of implementation and integration within healthcare information systems, are also taken into account. Blockchain applications in healthcare present a potentially effective means of safeguarding data integrity through the implementation of a decentralized and tamper-resistant ledger [73]. This segment examines the implementation of blockchain technology in the healthcare industry, specifically investigating the ways in which distributed ledger technology can be utilized to establish an unalterable and transparent ledger of medical data.

Through a critical examination of the benefits and challenges associated with the implementation of blockchain technology, professionals in the healthcare industry can evaluate the feasibility of utilizing blockchain to ensure data integrity, particularly in the era following quantum computing. Also, Zero-knowledge proofs are an ultra-effective cryptographic mechanism that ensures the integrity of data is verified without disclosing the data itself. This subsection delves into the healthcare application of zero-knowledge proofs, with a specific emphasis on techniques that are impervious to quantum-based attacks. Through the analysis of frameworks like zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge) [74], practitioners in the healthcare industry can investigate novel methods for safeguarding the privacy and confidentiality of medical information while ensuring data integrity. Furthermore, tamper-evident technologies are a category of devices that incorporate mechanisms designed to identify and indicate unauthorized efforts to modify data. This segment assesses tamper-evident methodologies implemented in the healthcare industry, such as timestamping mechanisms and digital signatures. Through a comprehensive analysis of the technologies' resistance to quantum threats and pragmatic implementation factors, professionals in healthcare cybersecurity can establish resilient safeguards for the integrity of data contained within healthcare records by integrating tamper-evident technologies.

The primary objective of this extensive investigation was to provide healthcare practitioners with a wide range of resources that can be utilized to safeguard the reliability of medical data in the era following quantum computing. In order to fortify their defenses against emerging quantum-based adversarial strategies and safeguard patient records, healthcare systems can implement tamper-evident technologies, adopt tamper-resistant hash functions, investigate blockchain applications, and utilize zero-knowledge proofs. In Fig. 3, roadmap for cybersecurity resilience in quantum era is illustrated. Also, Table 1 encapsulates crucial insights, detailing the current situations, desired outcomes, and actionable steps essential for implementing robust cybersecurity measures in the healthcare sector amidst the challenges posed by quantum technologies. As healthcare professionals navigate the complexities of post-quantum cybersecurity, this roadmap stands as a practical resource, providing a clear and structured framework to fortify systems against emerging quantum threats.

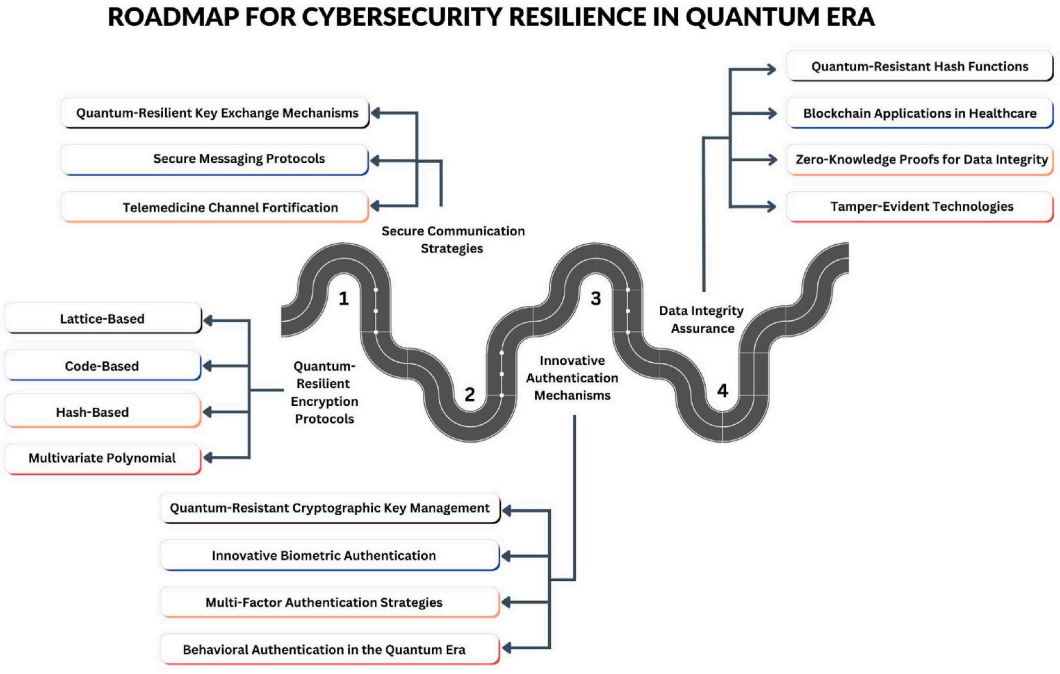


Fig. 3. Roadmap for cybersecurity resilience.

Table 1
Roadmap for cybersecurity resilience in the post-quantum healthcare era.

No	Current Situations	Desired Situations	How to Achieve the Goals
1	Limited Quantum-Resilient Encryption Protocols	Robust Quantum-Resilient Encryption Implementations	1. Research and adopt quantum-resilient encryption protocols. 2. Balance security and efficiency in healthcare applications.
2	Limited Adoption of Lattice-Based Cryptography	Wide Integration of Lattice-Based Cryptography	1. Collaborate with cryptographic researchers. 2. Educate healthcare professionals. Facilitate seamless integration.
3	Inadequate Understanding of Code-Based Cryptography	Comprehensive Knowledge of Code-Based Cryptography	1. Conduct awareness programs. Collaborate with experts. 2. Create educational resources and guidelines.
4	Limited Integration of Hash-Based Cryptography	Widespread Adoption of Quantum-Resilient Hashing	1. Develop guidelines. 2. Collaborate with cybersecurity experts. 3. Promote adoption through standards and regulations.
5	Minimal Awareness of Multivariate Polynomial Cryptography	Increased Awareness and Adoption	1. Develop educational materials. 2. Collaborate with researchers. 3. Facilitate training programs for professionals.
6	Inadequate Implementation of Quantum-Resilient Encryption	Effective Implementation	1. Establish collaboration. 2. Develop implementation guidelines. 3. Conduct audits and assessments.

4. Implementation and adoption

Within this pivotal segment, we shift our focus from theoretical to practical aspects, delving into the intricacies and challenges that arise during the adoption and integration of post-quantum cybersecurity measures into pre-existing healthcare infrastructures [75]. As we navigate towards a more secure future, this section addresses regulatory considerations, integration challenges, and the potential impact on patient care.

4.1. Integration challenges

This section discusses the complex challenges that arise during the integration and deployment of post-quantum cybersecurity measures in pre-existing healthcare systems. As healthcare organizations endeavor to strengthen their infrastructures against quantum threats, it becomes crucial to effectively manage compatibility concerns, operational procedures, and the ever-changing nature of healthcare environments. A fundamental challenge in the integration of post-quantum cybersecurity pertains to the assurance of compatibility with the current technological environment. Healthcare organizations frequently depend on a wide range of antiquated systems; therefore, the integration of quantum-resistant encryption, communication, and authentication mechanisms must operate in perfect harmony with these technologies. This subsection delves into approaches to harmonizing post-quantum cybersecurity measures with legacy systems in a seamless integration process while minimizing disruptions.

The introduction of novel cybersecurity protocols, particularly those customized for the post-quantum era, may cause disturbances to the established operational workflows of healthcare organizations. This particular section examines the possible difficulties that may arise due to disruptions in workflow, providing valuable perspectives on approaches to reduce operational interruptions, educate staff, and guarantee a seamless transition. Through a proactive approach and comprehension of these disruptions, healthcare organizations can successfully navigate the integration process while ensuring that daily operations are minimally impacted.

The transmission of information across various healthcare platforms and systems is a critical consideration, making interoperability a pivotal aspect of the industry. This section analyses the difficulties associated with achieving interoperability among diverse healthcare platforms during the implementation of post-quantum cybersecurity protocols. The exploration of standardization strategies, the adoption of common protocols, and the development of interoperable solutions is undertaken with the aim of facilitating seamless communication and exchange of data within a healthcare ecosystem post-quantum. Also, the implementation of comprehensive post-quantum cybersecurity measures necessitates substantial financial and technological resources. This segment discusses the difficulties linked to limitations in resources, providing perspectives on how to maximize the use of current resources, identify economically viable alternatives, and establish feasible schedules for execution. Through the acquisition of an all-encompassing comprehension of resource challenges, healthcare organizations are able to devise practical strategies that strengthen their cybersecurity postures while remaining within the confines of their budgets.

Furthermore, the effective implementation of post-quantum cybersecurity measures in the healthcare sector is contingent upon the training and skill development of personnel. This subsection delves into difficulties pertaining to training and the enhancement of skills, underscoring the criticality of imparting knowledge to personnel regarding the intricacies of quantum-resistant technologies. This study investigates approaches to establishing collaborations with domain experts, undertaking training programs, and cultivating a culture of cybersecurity awareness in order to equip healthcare professionals with the necessary skills to navigate the intricate challenges of the post-quantum cybersecurity environment. Integration challenges and corresponded proposed solutions are indicated in Table 2.

By conducting an exhaustive analysis of integration challenges, the objective of this segment is to furnish healthcare organizations with a strategic plan to surmount challenges and guarantee the effective deployment of post-quantum cybersecurity measures. Healthcare systems can enhance their resilience to quantum threats and preserve the integrity and effectiveness of their operations by implementing the following measures:

1. Improving resource management
2. Ensuring interoperability
3. Addressing compatibility concerns
4. Prioritizing training and skill development.

4.2. Regulatory considerations

In this critical section, we navigate through the complex landscape of regulatory considerations that shape the implementation of post-quantum cybersecurity measures within the healthcare sector. As healthcare organizations strive to enhance their cybersecurity resilience, understanding and adhering to regulatory frameworks become paramount for safeguarding patient data and ensuring compliance with legal and ethical standards.

The healthcare industry is subject to stringent privacy regulations and compliance standards aimed at protecting patient data. This subsection delves into the intricate web of regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR), exploring their implications for the implementation of post-quantum cybersecurity measures. Strategies for aligning cybersecurity practices with privacy regulations and compliance standards are examined to ensure that healthcare organizations fortify their security postures without compromising patient privacy.

Also, in the event of a cybersecurity incident, swift and accurate reporting is essential to meet data breach notification requirements. This part of the section explores the challenges associated with notifying relevant authorities and affected individuals in a timely manner. Strategies for developing incident response plans, establishing communication protocols, and ensuring compliance with data breach notification requirements are examined to empower healthcare organizations to navigate the aftermath of cybersecurity incidents in the post-quantum era.

Then, healthcare data often traverses international boundaries, necessitating a nuanced understanding of international and cross-border considerations. This subsection explores challenges related to data transfer, jurisdictional variations in cybersecurity regulations, and the impact of geopolitical factors on regulatory compliance. Strategies for navigating international frameworks, fostering collaboration between regulatory bodies, and ensuring seamless cross-border data flow are examined to facilitate the global implementation of post-quantum cybersecurity measures within the healthcare sector.

Besides, beyond overarching regulations, industry-specific guidelines and best practices provide valuable insights for healthcare cybersecurity. This part of the section explores the challenges associated with interpreting and implementing industry-specific recommendations. Strategies for staying abreast of evolving guidelines, collaborating with industry stakeholders, and adopting best practices that align with post-quantum cybersecurity measures are examined to ensure that healthcare organizations not only meet regulatory requirements but also exceed industry standards in securing patient data.

Furthermore, ethical considerations play a pivotal role in shaping cybersecurity practices within healthcare. This subsection explores the ethical dimensions of implementing post-quantum cybersecurity measures, addressing questions related to transparency, informed consent, and the ethical use of emerging technologies. Strategies for integrating ethical considerations into cybersecurity frameworks, engaging with ethical review boards, and fostering a culture of ethical cybersecurity practices are examined to ensure that healthcare organizations navigate the post-quantum era with a commitment to ethical standards. In Table 3, regulatory considerations, challenges, and proposed solutions are illustrated.

5. Future directions

This section focuses on the potential developments and trajectories that the field of healthcare post-quantum cybersecurity could

Table 2
Integration challenges and proposed solutions.

No	Challenge	Solutions
1	Compatibility with Existing Technologies	1. Develop compatibility protocols and standards. 2. Assess and update legacy systems for seamless integration.
2	Operational Workflow Disruptions	1. Conduct thorough impact assessments. 2. Develop and implement transition plans with minimal disruptions.
3	Interoperability Across Healthcare Platforms	1. Establish common protocols and standards. 2. Advocate for interoperability in healthcare system design.
4	Resource and Budget Constraints	1. Optimize existing resources. 2. Seek cost-effective solutions. 3. Develop realistic timelines for implementation.
5	Training and Skill Development	1. Develop comprehensive training programs. 2. Collaborate with experts for skill development initiatives.

Table 3
Regulatory considerations, challenges, and proposed solutions.

No	Regulatory Consideration	Description	Challenge	Solution
1	Privacy Regulations and Compliance Standards	Adherence to privacy laws (HIPAA, GDPR).	Limited awareness of evolving privacy regulations.	Conduct regular training on privacy laws.
2	Data Breach Notification Requirements	Swift reporting of cybersecurity incidents.	Inadequate incident response plans.	Develop and update incident response plans.
3	International and Cross-Border Considerations	Understanding data transfer across borders.	Jurisdictional variations in cybersecurity regs.	Establish clear protocols for cross-border data transfer.
4	Industry-Specific Guidelines and Best Practices	Adherence to industry-specific cybersecurity guidelines.	Interpretation and implementation challenges.	Collaborate with experts for guideline interpretation.
5	Ethical Considerations in Cybersecurity	Integration of ethical standards into cybersecurity frameworks.	Lack of transparency and informed consent.	Develop clear ethical guidelines

pursue in the years to come. It provides healthcare organizations with a roadmap for anticipating potential challenges and opportunities, enabling them to anticipate emerging threats and capitalize on innovative solutions. The domain of quantum computing is characterized by its ever-changing and dynamic nature. This section encompasses projected advancements in quantum computing technologies, encompassing the creation of quantum processors and algorithms with enhanced capabilities. By comprehending the potential for quantum threats to accelerate, healthcare organizations are able to proactively adjust and strengthen their cybersecurity measures in the aftermath of quantum computing.

The anticipated progression of post-quantum cryptographic algorithms is examined in this section, which encompasses the active research domain of post-quantum cryptography. Healthcare organizations can proactively foresee the development of more resilient solutions, such as quantum-resistant key exchange mechanisms and innovative encryption protocols, in order to appropriately update

Table 4
Future directions and pathways based on the challenges.

No	Challenges	Future Directions and Pathways
1	Dynamic Nature of Quantum Threats	- Ensuring the secure transmission and storage of sensitive patient data, - Protecting against potential cyber threats and dealing with ethical issues related to genetic engineering and gene editing. - Continuously monitor and adapt cybersecurity measures. - Collaborate with experts to anticipate evolving quantum threats. - Implement real-time threat intelligence and detection systems.
2	Progression of Quantum Computing	- Major advancements in hardware, algorithms, and software are necessary to fully realize the potential of quantum computing in healthcare. - Stay informed about advancements in quantum processors and algorithms. - Regularly update post-quantum cryptographic algorithms. - Proactively adjust cybersecurity measures based on quantum computing progress.
3	Post-Quantum Cryptographic Solutions	- The adoption of quantum-resistant cryptographic algorithms to safeguard patient data from potential quantum attacks. - Anticipate and adopt more resilient solutions like quantum-resistant key exchange mechanisms and encryption protocols. - Incorporate emerging technologies (blockchain, AI) into cybersecurity frameworks.
4	Interdisciplinary Collaboration	- Enhance collaboration among researchers, healthcare practitioners, and cybersecurity specialists. - Promote interdisciplinary knowledge exchange to bolster overall resilience.
5	Ongoing Training and Awareness Programs	- Establish continuous education initiatives for administrators, cybersecurity teams, and healthcare professionals. - Embracing technology, personalizing learning, fostering collaboration. - Providing continuous professional development to meet the evolving needs of the healthcare industry. - Cultivate a culture of cybersecurity awareness within organizations.
6	Regulatory Adjustments	- Changes to reimbursement systems, quality reporting requirements, and interoperability standards. - Continued emphasis was placed on value-based care and addressing social factors of health. - Monitor and adapt to prospective regulatory modifications in response to quantum threats. - Ensure compliance with evolving cybersecurity regulations.
7	Global Collaboration and Standardization	- Utilizing AI and machine learning algorithms to analyze large volumes of healthcare data to enhance decision-making, disease diagnosis, and personalized treatment. - Developing ethical guidelines and regulations for the use of AI in healthcare to safeguard patient privacy and ensure responsible implementation. - Encourage international cooperation in addressing quantum threats. - Contribute to the formulation of global benchmarks for healthcare cybersecurity standards. - Implement standardized approaches for post-quantum cybersecurity.
8	Ethical Considerations	- Fostering a culture of ethical awareness, integrity, and accountability within healthcare organizations. - Promoting ethical decision-making at all levels of the healthcare system. - Involving the public in discussions and policy-making processes related to ethical issues in healthcare. - Ensuring that ethical considerations are integrated into healthcare policies and regulations. - Encourage international cooperation in addressing quantum threats. - Contribute to the formulation of global benchmarks for healthcare cybersecurity standards. - Implement standardized approaches for post-quantum cybersecurity.

their cybersecurity frameworks. The potential for substantial advancements lies in the incorporation of post-quantum cybersecurity measures with emerging technologies, including blockchain and artificial intelligence (AI). This section outlines the ways in which healthcare organizations can enhance and adapt their cybersecurity frameworks by focusing on the synergies that exist between emerging technologies and post-quantum cybersecurity. Table 4 categorized the future paths and pathways based on the challenges.

Based on the interdisciplinary nature of cybersecurity and healthcare, recent trends indicate the need for enhanced collaboration among researchers, healthcare practitioners, and cybersecurity specialists from various disciplines. This study investigates ways to enhance the collective intelligence framework, promote interdisciplinary collaboration, and facilitate the exchange of insights to enhance the overall resilience of healthcare cybersecurity. The current training and awareness programs are of the highest importance due to the ever-changing landscape of cybersecurity threats. This segment examines the significance of ongoing education for administrators, cybersecurity teams, and healthcare professionals. This paper investigates ways to develop a culture of cybersecurity awareness and establish effective training programs to ensure that healthcare organizations are consistently equipped to confront emerging threats.

Also, regulatory bodies are required to make necessary adjustments in response to the evolving environment pertaining to quantum threats. This subsection examines prospective regulatory modifications and revisions pertaining to healthcare cybersecurity in the post-quantum era. By comprehending the potential evolution of regulations, healthcare organizations can ensure that their cybersecurity practices are in accordance with emerging compliance standards. In order to develop a unified and standardized approach to post-quantum cybersecurity, global collaboration and standardization efforts are crucial. This segment delves into the significance of international cooperation, the formulation of worldwide benchmarks, and the implementation of optimal strategies in order to forge a cohesive front against quantum hazards within the healthcare industry.

Then, with the advancement of technologies, the ethical dimensions of cybersecurity become increasingly vital. This subsection delves into the ethical implications that are unique to the post-quantum era. It addresses concerns regarding user consent, transparency, and the responsible application of emergent technologies in the context of healthcare cybersecurity. By forecasting developments in quantum computing, the progression of cryptographic solutions, the importance of interdisciplinary cooperation, and the ongoing necessity for education, healthcare systems are equipped to proactively confront emergent threats and guarantee the continuous robustness of their cybersecurity frameworks. The challenges and future direction and pathways are summarized in Table 4.

6. Conclusion

In conclusion, this paper has highlighted the importance of protecting medical data in the era of quantum technologies. It has provided a detailed plan to address the specific challenges posed by quantum threats to the confidentiality and integrity of health data. The introduction set the context by emphasizing the potential impact of post-quantum technologies on the healthcare industry and the need to enhance cybersecurity measures. The subsequent sections analyzed the significance of cybersecurity in the post-quantum era, including the vulnerabilities of current encryption methods and the potential risks posed by quantum threats to health data privacy.

The paper proposed a cybersecurity resilience framework, discussing encryption protocols resistant to quantum attacks, secure communication strategies, authentication mechanisms, and data integrity assurance methods. It also outlined future advancements in quantum computation, post-quantum cryptography, and the integration of cybersecurity with emerging technologies. Ethical considerations, ongoing training programs, and interdisciplinary collaboration were recognized as essential elements in maintaining strong cybersecurity in the dynamic quantum environment.

In summary, this article has addressed the complex challenges that quantum technologies bring to the healthcare sector and has provided a systematic approach to enhance the cybersecurity resilience of medical data. The findings underscore the critical need for healthcare institutions to implement proactive measures such as secure communication protocols, robust authentication systems, quantum-resistant encryption, and advanced data integrity assurance systems. By following the outlined roadmap, healthcare stakeholders can navigate the complexities of the post-quantum era, safeguard patient data, and uphold ethical standards in the healthcare profession.

Data availability

No data was used for the research described in the article.

Inclusion and diversity

Not applicable.

CRediT authorship contribution statement

SaberiKamarposhti: Writing – review & editing, Writing – original draft, Supervision, Methodology, Conceptualization. **Kok-Why Ng:** Writing – review & editing, Writing – original draft, Supervision, Methodology, Conceptualization. **Fang-Fang Chua:** Writing – review & editing, Writing – original draft, Supervision, Methodology, Conceptualization. **Junaidi Abdullah:** Writing – review & editing, Writing – original draft, Supervision, Methodology, Conceptualization. **Mehdi Yadollahi:** Writing – review & editing, Writing – original draft, Visualization, Validation, Methodology, Conceptualization. **Mona Moradi:** Writing – review & editing. **Sima**

Ahmadpour: Writing – review & editing.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] L. Aggarwal, S. Sachdeva, P. Goswami, Quantum Healthcare Computing Using Precision-Based Granular Approach, 2023.
[2] A.P. Bhatt, A. Sharma, Quantum Cryptography for Internet of Things Security, 2019.
[3] M.M. Kermani, R. Azarderakhsh, Lightweight hardware architectures for fault diagnosis schemes of efficiently-maskable cryptographic substitution boxes, in: 2016 IEEE International Conference on Electronics, Circuits and Systems (ICECS), Monte Carlo, Monaco, 2016, pp. 764–767, https://doi.org/10.1109/ICECS.2016.7841314.
[4] Mozaffari Kermani, Reza Azarderakhsh Mehran, Mehdi Mirakhorli, Multidisciplinary approaches and challenges in integrating emerging medical devices security research and education, in: S. Gupta, et al. (Eds.), Quantum Computing Led Innovation for Achieving a More Sustainable Covid-19 Healthcare Industry vol. 120, 2016 102544. Technovation, 2023.
[5] A. Sarker, M. Mozaffari Kermani, R. Azarderakhsh, Efficient error detection architectures for postquantum signature falcon's sampler and KEM SABER, 6, in: IEEE Trans. Very Large Scale Integr. Syst., 30, June 2022, pp. 794–802, https://doi.org/10.1109/TVLSI.2022.3156479.
[6] Z.Z. Zhiguo Qu, Min Zheng, A quantum blockchain-enabled framework for secure private electronic medical records in Internet of Medical Things, Inf. Sci. 612 (2022) 942–958.
[7] F.Ö. Sönmez, C. Hankin, P. Malacaria, Decision Support for Healthcare Cybersecurity, 2022.
[8] M. Arian, M.S. Kamarposhti, A. Broumandnia, A New Method for Image Encryption Using DNA Sequences and Hyper Chaos, 2023.
[9] A.E. Azzaoui, P.K. Sharma, J.H. Park, Blockchain-based Delegated Quantum Cloud Architecture for Medical Big Data Security, 2022.
[10] Rami Elkhatib, Reza Azarderakhsh, Mehran Mozaffari-Kermani, Accelerated risc-v for sike, in: 2021 IEEE 28th Symposium on Computer Arithmetic (ARITH), IEEE, 2021.
[11] W.S. Admass, Y.Y. Munaye, A. Diro, Cyber Security: State of the Art, Challenges and Future Directions, 2024.
[12] A. Ahad, et al., A Comprehensive Review on 5G-Based Smart Healthcare Network Security: Taxonomy, Issues, Solutions and Future Research Directions, 2023.
[13] D. Chawla, P.S. Mehra, QSMAH: A Novel Quantum-Based Secure Cryptosystem Using Mutual Authentication for Healthcare on the Internet of Things, 2023.
[14] M. Bhavin, et al., Blockchain and Quantum Blind Signature-Based Hybrid Scheme for Healthcare 5.0 Applications, 2021.
[15] A.K. Singh, K. Acharya, S. Mukhopadhyay, Post-quantum secure recipient revocable broadcast encryption supporting anonymity, Multimed, Tool. Appl. 83 (2) (2023) 4519–4531.
[16] Y. Tseng, Attribute Hiding Subset Predicate Encryption: Quantum-Resistant Construction with Efficient Decryption, 2023.
[17] Alvaro Cintas-Canto, et al., CRC-oriented error detection architectures of post-quantum cryptography niederreiter key generator on FPGA, in: 2022 IEEE Nordic Circuits and Systems Conference (NorCAS), IEEE, 2022.
[18] W.H. Chang, et al., Dynamic Quantum Fully Homomorphic Encryption Scheme Based on Universal Quantum Circuit, 2023.
[19] S. Kumari, et al., A post-quantum lattice-based lightweight authentication and code-based hybrid encryption scheme for IoT devices, Comput. Network. 217 (2022) 109327.
[20] S. Yang, X. Huang, Universal product learning with errors: a new variant of LWE for lattice-based cryptography, Theor. Comput. Sci. 915 (2022) 90–100.
[21] Jasmin Kaur, Alvaro Cintas Canto, Mehran Mozaffari Kermani, et al., A Survey on the Implementations, Attacks, and Countermeasures of the Current NIST Lightweight Cryptography Standard, TechRxiv. May 22 (2023), https://doi.org/10.36227/techrxiv.22970855.v1.
[22] Z. Fu, et al., Distributed Three-Level QR Codes Based on Visual Cryptography Scheme, 2022.
[23] Alvaro Cintas Canto, Jasmin Kaur, Mehran Mozaffari Kermani, et al., Algorithmic Security is Insufficient: A Comprehensive Survey on Implementation Attacks Haunting Post-Quantum Security, TechRxiv. May 23 (2023), https://doi.org/10.36227/techrxiv.23071079.v1.
[24] D.J. Bernstein, et al., The SPHINCS+ signature framework, in: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, 2019.
[25] P.H. Kumar, G. AnandhaMala, HMAC-R: hash-based message authentication code and Rijndael-based multilevel security model for data storage in cloud environment, J. Supercomput. 79 (3) (2023) 3181–3209.
[26] J. Dey, R. Dutta, Progress in multivariate cryptography: systematic review, challenges, and research directions, ACM Comput. Surv. 55 (12) (2023) 1–34.
[27] K. Baranitharan, et al., A Collaborative and Adaptive Cyber Défense Strategic Assessment for Healthcare Networks Using Edge Computing, 2023.
[28] A. Shaller, L. Zamir, M. Nojoumian, Roadmap of post-quantum cryptography standardization: side-channel attacks and countermeasures. Information and Computation, 2023 105112.
[29] B. Senapati, B.S. Rawal, Quantum communication with RLP quantum resistant cryptography in industrial manufacturing, Cyber Secur. Appl. 1 (2023) 100019.
[30] S. Abidin, et al., Quantum cryptography technique: a way to improve security challenges in mobile cloud computing (MCC), Mater. Today: Proc. 51 (2022) 508–514.
[31] G. Yalamuri, P. Honnavalli, S. Eswaran, A review of the present cryptographic arsenal to deal with post-quantum threats, Procedia Comput. Sci. 215 (2022) 834–845.
[32] S. Jia, Comparison of performances for quantum and conventional algorithms: shor's algorithm and boson sampling, Highlights Sci. Eng. Technol. 38 (2023) 493–501.
[33] R.H. Preston, Applying Grover's algorithm to hash functions: a software perspective, IEEE Trans. Quantum Eng. 3 (2022) 1–10.
[34] G. Song, et al., A parallel quantum circuit implementations of LSH hash function for use with Grover's algorithm, Appl. Sci. 12 (21) (2022) 10891.
[35] A. Ghorbania, M. Saberikamarposhti, M. Yadollahi, Using Ribonucleic Acid (RNA) and Hénon Map in New Image Encryption Scheme, 2022.
[36] U.H. Govindarajan, D.K. Singh, H. Gohel, Forecasting Cyber Security Threats Landscape and Associated Technical Trends in Telehealth Using Bidirectional Encoder Representations from Transformers (BERT), 2023.
[37] N. Kundu, S.K. Debnath, D. Mishra, A Secure and Efficient Group Signature Scheme Based on Multivariate Public Key Cryptography, 2021.
[38] D. Verchyk, J. Sepúlveda, A practical study of post-quantum enhanced identity-based encryption, Microprocess. Microsyst. 99 (2023) 104828.
[39] L. Malina, et al., post-quantum era privacy protection for intelligent infrastructures, IEEE Access 9 (2021) 36038–36077.
[40] C. Blanco, et al., Onto-CARMEN: Ontology-Driven Approach for Cyber-Physical System Security Requirements Meta-Modelling and Reasoning, 2023.
[41] A.M. Perumal, E.R.S. Nadar, Architectural framework and simulation of quantum key optimization techniques in healthcare networks for data security, J. Ambient Intell. Hum. Comput. 12 (2021) 7173–7180.
[42] Qu Z., Meng Y., Liu B., Muhammad, G., Tiwari P., QB-IMD: A secure medical data processing system with privacy protection based on quantum blockchain for IoMT, IEEE Intern. Things J. 11 (1) (2024) 40-49, doi: 10.1109/JIOT.2023.3285388.
[43] S. Pulipeti, A. Kumar, Secure quantum computing for healthcare sector: a short analysis, Security and Privacy 6 (5) (2023) e293. https://doi.org/10.1002/spy2.293.
[44] M. Bisheh-Niasar, R. Azarderakhsh, M.M. Kermani, Optimized Architectures for Elliptic Curve Cryptography over Curve448, IACR Cryptol. ePrint Arch. 2020 (2020) 1338.

[45] A.I. Newaz, et al., A survey on security and privacy issues in modern healthcare systems: attacks and defenses, ACM Trans. Comput. Healthcare 2 (3) (2021) 1–44.
[46] W. Bani Issa, et al., Privacy, confidentiality, security and patient safety concerns about electronic health records, Int. Nurs. Rev. 67 (2) (2020) 218–230.
[47] R. Ur Rasool, et al., Quantum computing for healthcare: a review, Future Internet 15 (3) (2023) 94.
[48] M. Varshini, et al., A sophisticated review on open verifiable health care system in cloud, in: Mobile Computing and Sustainable Informatics: Proceedings of ICMCSI 2023, Springer, 2023, pp. 141–156.
[49] R. Venkatesh, B. Savadatti Hanumantha, Electronic medical records protection framework based on quantum blockchain for multiple hospitals, Multimed. Tool. Appl. (2023) 1–14.
[50] F.J. Jaime, et al., Strengthening privacy and data security in biomedical microelectromechanical systems by IoT communication security and protection in smart healthcare, Sensors 23 (21) (2023) 8944.
[51] S. Pal, et al., Future potential of quantum computing and simulations in biological science, Mol. Biotechnol. (2023) 1–18.
[52] M. Adeli, N. Bagheri, H.R. Maimani, S. Kumari, J.J.P.C. Rodrigues, A post-quantum compliant authentication scheme for IoT healthcare systems, IEEE Intern. Things J. 11 (4) (2024) 6111–6118, https://doi.org/10.1109/JIOT.2023.3309931.
[53] R. Venkatesh, B.S. Hanumantha, A privacy-preserving quantum blockchain technique for electronic medical records, IEEE Eng. Manag. Rev. 51 (4) (2023) 137–144, https://doi.org/10.1109/EMR.2023.3319376.
[54] R. Cerchione, et al., Blockchain's coming to hospital to digitalize healthcare services: designing a distributed electronic health record ecosystem, Technovation 120 (2023) 102480.
[55] Alvaro Cintas-Canto, Mehran Mozaffari Kermani, Reza Azarderakhsh, Reliable architectures for finite field multipliers using cyclic codes on FPGA utilized in classic and post-quantum cryptography, IEEE Trans. Very Large Scale Integr. Syst. 31 (1) (2022) 157–161.
[56] P. Sharma, et al., EHDHE: enhancing security of healthcare documents in IoT-enabled digital healthcare ecosystems using blockchain, Inf. Sci. 629 (2023) 703–718.
[57] S. Selvarajan, H. Mouratidis, A quantum trust and consultative transaction-based blockchain cybersecurity model for healthcare systems, Sci. Rep. 13 (1) (2023) 7107.
[58] B.M. Singh, J. Natarajan, A novel secure authentication protocol for e-health records in cloud with a new key generation method and minimized key exchange, J. King Saud Univ.-Computer Inf. Sci. (2023) 101629.
[59] M. Ghahramani, R. Javidan, Time dependency: an efficient biometric-based authentication for secure communication in wireless healthcare sensor networks, J. Comput. Virol. Hacking Tech. 19 (2) (2023) 303–317.
[60] S. Zhang, X. Du, X. Liu, A novel and quantum-resistant handover authentication protocol in IoT environment, Wireless Network (2023) 1–18.
[61] Mehran Mozaffari-Kermani, et al., Guest editorial: introduction to the special section on emerging security trends for biomedical computations, devices, and infrastructures, IEEE ACM Trans. Comput. Biol. Bioinf 13 (3) (2016) 399–400.
[62] H. Nguyen, L. Tran, Design of polynomial NTT and INTT accelerator for post-quantum cryptography CRYSTALS-kyber, Arabian J. Sci. Eng. 48 (2) (2023) 1527–1536.
[63] J. Kim, J.H. Park, NTRU+: Compact construction of NTRU using simple encoding method, IEEE Trans. Inform. Foren. Security 18 (2023) 4760–4774, https://doi.org/10.1109/TIFS.2023.3299172.
[64] Reza Azarderakhsh, Kimmo U. Järvinen, Mehran Mozaffari-Kermani, Efficient algorithm and architecture for elliptic curve cryptography for extremely constrained secure applications, IEEE Trans. Circuits Syst. I: Regular Papers 61 (4) (2014) 1144–1155.
[65] J. Hekkala, et al., Implementing post-quantum cryptography for developers, SN Comput. Sci. 4 (4) (2023) 365.
[66] Z.E.D. Mohammed Khalid Yousif, Shahab Wahhab Kareem, Information security for big data using the NTRUEncrypt method, Measurement: Sensors 27 (2023) 100738.
[67] A. Alawi, T.S. Al-saggaf, Hoda Alkhzaimi, Gamil Ahmed, Lightweight two-factor-based user authentication protocol for IoT-enabled healthcare ecosystem in quantum computing, Arabian J. Sci. Eng. 48 (2023) 2347–2357.
[68] P. Hari Kumar, G.S.A, HMAC-R: hash-based message authentication code and Rijndael-based multilevel security model for data storage in cloud environment, J. Supercomput. 79 (2023) 3181–3209.
[69] M. Anastasova, R. Azarderakhsh, M.M. Kermani, L. Beshaj, Time-efficient finite field microarchitecture design for Curve448 and Ed448 on cortex-M4, in: S. H. Seo, H. Seo (Eds.), Information Security and Cryptology – ICISC 2022. ICISC 2022. Lecture Notes in Computer Science, vol. 13849, Springer, Cham, 2023, https://doi.org/10.1007/978-3-031-29371-9_15.
[70] S.C. Praveen Kumar Rayani, Continuous user authentication on smartphone via behavioral biometrics: a survey, Multimed. Tool. Appl. 82 (2023) 1633–1667.
[71] S.R. Cherry Mangla, Nawab Muhammad Faseeh Qureshi, Aman Singh, Mitigating 5G security challenges for next-gen industry using quantum computing, J. King Saud University - Computer and Inf. Sci. 35 (6) (2023) 101334.
[72] Pushpita ChatterjeeD.D, Sourav Banerjee, Uttam Ghosh, Armando B. Mpembele, Tamara Rogers, An approach towards the security management for sensitive medical data in the IoMT ecosystem, in: MobiHoc '23: Proceedings of the Twenty-Fourth International Symposium on Theory, Algorithmic Foundations, and Protocol Design for Mobile Networks and Mobile Computing, Association for Computing Machinery (ACM), October 2023, pp. 400–405.
[73] Meltem Sonmez Turan, et al., Status Report on the Final Round of the NIST Lightweight Cryptography Standardization Process, US Department of Commerce, National Institute of Standards and Technology, 2023.
[74] G.S.R.L, Design and evaluation of novel hybrid quantum resistant cryptographic system for enhancing security in wireless body sensor networks, Opt. Quant. Electron. 55 (2023) 1252.