Chapter 3
Securing Healthcare Data With Quantum-Safe Encryption

Titiksha Tulsidas Bhagat
http://orcid.org/0009-0009-1454-6948
Ramdeobaba University, Nagpur, India

Shweta Bondre
Ramdeobaba University, Nagpur, India

Vipin Bondre
Yeshwantrao Chavan College of Engineering, Nagpur, India

Uma Yadav
http://orcid.org/0000-0003-2781-9756
Ramdeobaba University, Nagpur, India

Priya Dasarwar
Symbiosis Institute of Technology, Symbiosis International (Deemed to be) University, Pune, India

ABSTRACT

With the swift development of healthcare digitization we have access to an exponentially growing amount of extremely sensitive patient data that requires advanced security. However, now with the advent of quantum computing we are faced with a very real risk of exposing medical data in ways we never thought possible through traditional encryption. In this chapter, we will discuss the critical need for quantum-safe encryption to protect against quantum-based attacks on electronic health records, telemedicine communications, and IoT-enabled medical devices. We will

DOI: 10.4018/979-8-3373-7426-0.ch003

review existing cryptography standards (i.e. RSA, ECC) in a post-quantum world, and consider new quantum-resistant algorithms like lattice-based, hash-based, and multivariate algorithms outlined in NIST's Post-Quantum Cryptography (PQC) standardization program. We will also highlight how quantum secure encryption will revolutionize the security of healthcare data in terms of data integrity, privacy protection, and secure communications.

1. INTRODUCTION

An unprecedented amount of extremely sensitive patient data has been unleashed during the healthcare industry's rapid digital evolution, from genomic records to medical imaging to streaming telemetry data from IoT devices (ElSayed et al., 2025). Despite this data revolution being a game-changer for precision medicine and also creating huge vulnerability vectors for cybercriminals, the intricate interlink between cybersecurity and digital transformation in the healthcare space comes with several challenges and implications. In a way, they have been developed and improved cyber-technologies because of the sudden adoption and integration of cyber-technologies. But with such improvements, greater risks have equally emerged. A growing trend in cybersecurity crime such as data breach and cyberattack more than ever calls for a desperate need for adequate defense.

1.1 Significance of Cryptography in Healthcare

Cryptography definitely plays a vital role in securing and maintaining the privacy of health data, especially as medical records gradually go digital (Ankunda, n.d.). With electronic health records (EHRs) and connected medical gadgets being popularly cloud-based, strongly secured cryptography stands as the first barrier preventing unauthorized access and data breaches. Patient data can be safeguarded through encryption techniques such as symmetric and asymmetric cryptography pertaining to encoding data such that only the authorized party can decode it (Balogun, n.d.). These encryption features also maintain patients' privacy and ensure that rules and regulations pertinent to healthcare, such as the Health Insurance Portability and Accountability Act (HIPAA) or the General Data Protection Regulation (GDPR), are adhered to. Homomorphic encryption (HE), one of the most advanced encryption mechanisms, has become a potential technology to provide privacy to medical information and yet be able to perform computations on encrypted data (Chukwunweike et al., 2024). The art of protecting communication via the principles of quantum mechanics is referred to as quantum cryptography (Imran et al., 2024). Quantum cryptography uses the very properties of quantum mechanics to