A Study of Quantum-Resistent Cryptography for Long-Term Medical Data Protection

Sivabalan Settu
LGPR Team LUCPDF202502240085, Lincoln University College Malaysia, Petaling Jaya, Selangor Darul Ehsan, Malaysia
Sivabalan1990s@gmail.com

Deepak Gupta
LGPR Team LUCPDF202502240085, Lincoln University College Malaysia, Petaling Jaya, Selangor Darul Ehsan, Malaysia

Divya Mithun
LGPR Team LUCPDF202502240085, Lincoln University College Malaysia, Petaling Jaya, Selangor Darul Ehsan, Malaysia

***Abstract*- Quantum computing looks set to shake up the basics of our current cryptographic setups. It poses a real risk to systems that safeguard electronic medical records and long-term healthcare archives. Things like genomic sequencing profiles, paediatric developmental histories, neonatal imaging, and biometric identifiers all need strong confidentiality that lasts well over a century. The classical public-key methods we rely on, mainly RSA and ECC, just wont hold up once big quantum computers start running Shors algorithm effectively. This work puts forward a full quantum-resistant security setup designed specifically for national healthcare systems. It pulls together lattice-based encryption, hash-based signatures, blockchain for solid integrity checks, and a special engine to model quantum threats. We ran tests with simulated quantum attackers and experiments mimicking hospital data flows on a large scale. The design shows strong staying power, cutting exposure risk by 92 percent. It keeps system performance in line with what clinical workflows can handle without issues. These results really highlight how pressing it is to start shifting to post-quantum methods. That way we can lock down medical data confidentiality for decades ahead.**

Keywords: Quantum Computing, RSA, Encryption.

1. INTRODUCTION

Healthcare data preservation calls for a security timeline that stretches out much longer than usual. Financial data or transactional records often lose their sensitive edge after just a few years. Genomic details, markers for inherited diseases, child development files, and patterns from ongoing illnesses stay relevant and risky through a person's full life. That extends to their family line too. This drawn-out demand leaves healthcare security wide open to issues from crypto flaws that build up over decades. Traditional setups like RSA, ECC, and Diffie Hellman lean on tough math problems. Experts figure quantum tech will crack those assumptions pretty soon. Shors algorithm handles big number factoring with ease. It also works out discrete logs quickly. All that endangers nearly every public key method in use today. Grovers algorithm picks up the pace on brute force hunts. In turn, that weakens symmetric encryption and hash tools more than before.

The shift to digital in healthcare worldwide ramps up these risks even further. Countries now depend heavily on electronic patient files, diagnostics powered by AI, huge stores of medical scans, and cloud setups for gene sequencing. Data piles grow bigger and more delicate all the time. So the harm from attacks that decrypt old files later on could hit hard. Bad actors might grab locked medical info right now. They could hold onto it forever. Then they decrypt once quantum tools get strong enough. People call this the harvest now decrypt later problem. To fight back, groups like NIST and crypto experts around the world started work on post quantum options. Standards efforts focus on lattice styles and hash-based ones. Those look like the best bets so far.

With all this going on, healthcare crypto needs a full rethink. It has to hold up not just against attacks today. Security must last about a hundred years into the future. This work fits right into that big shift happening globally. It looks at the special limits and needs in healthcare systems. They gear up for life after quantum threats take hold.

2. PROBLEM FORMULATION

The main issue this work tackles comes from how current healthcare encryption setups just cannot hold up against attackers using quantum tech. Things like electronic health records systems, hospital data sharing networks, remote medical services, and countrywide health databases mostly rely on RSA-2048 keys, ECC-256 curves, and TLS setups that quantum computers will crack pretty easily. All that sensitive patient info saved right now will still matter for medical use many years down the line. That is long after old school encryption gets broken wide open. Without

safeguards built for the post-quantum world, entire national health data stores face huge risks of massive leaks someday. Those leaks could spill out personal DNA profiles, kid's medical backgrounds, reproductive health details, and records on mental health struggles. Once that happens, it opens the door to things like custom biological attacks aimed at people, unfair treatment by insurance companies based on bias, ways politicians could twist info for their gain, and damage to society that lasts for generations.

On top of that, the whole healthcare field runs on tough rules and regulations that change at a snail's pace. Those rules rarely account for new dangers coming from science breakthroughs. So, hospitals end up without solid advice on the tech side, no step-by-step plans for switching over, and nothing really to help weigh the risks from quantum threats. This leaves a big gap across the entire system. Even places with cutting edge health tech stay wide open to quantum-based attacks in the future. The real heart of the problem goes beyond just weak encryption methods. It also hits on how unprepared everyone is in terms of planning and strategy.

3. LIMITATIONS OF EXISITING SYSTEM

Existing healthcare cryptographic systems exhibit several structural and operational limitations that severely restrict their ability to endure quantum attacks. First, classical public-key schemes such as RSA and ECC are mathematically incapable of resisting Shor's algorithm, which is expected to become practically deployable within the next two decades. This renders long-term data storage inherently insecure, even when encrypted using strong key sizes. Second, healthcare institutions typically lack migration pathways that would allow seamless adoption of post-quantum algorithms. Their infrastructure relies on legacy hardware, vendor-locked devices, and proprietary medical software not designed to accommodate PQC-level key sizes, communication patterns, or signature formats. Without structured transition plans, hospitals risk operational disruptions when PQC becomes mandatory.

Third, current healthcare security standards focus primarily on classical cyber threats such as ransomware, unauthorized access, and network intrusions. They do not incorporate quantum-threat modelling, forward-secrecy requirements, or cryptographic survivability metrics extending beyond 20–30 years. This leaves a policy and standards gap. Furthermore, key-management systems in hospitals rarely account for century-scale protection windows, leading to weak lifecycle practices that are incompatible with PQC needs. These combined limitations demand a redesigned architecture capable of handling the cryptographic challenges of the quantum era.

4. METHODOLOGY

The methodological approach selected for this research incorporates quantum-threat analysis, cryptographic engineering, and empirical performance evaluation through the use of hospital-scale datasets. The initial part consists of developing a detailed quantum-threat model specifically for the healthcare sector, which will define the capabilities of the attackers, for example, the use of quantum-computing-based decryption, the use of cloud-based quantum services, and the implementation of long-term data harvesting strategies. Thus, this model maps out the different places where the attacks could occur in the electronic health records systems, the genomic data stores, the telemedicine channels, the servers of clinical imaging, and the medical IoT devices.

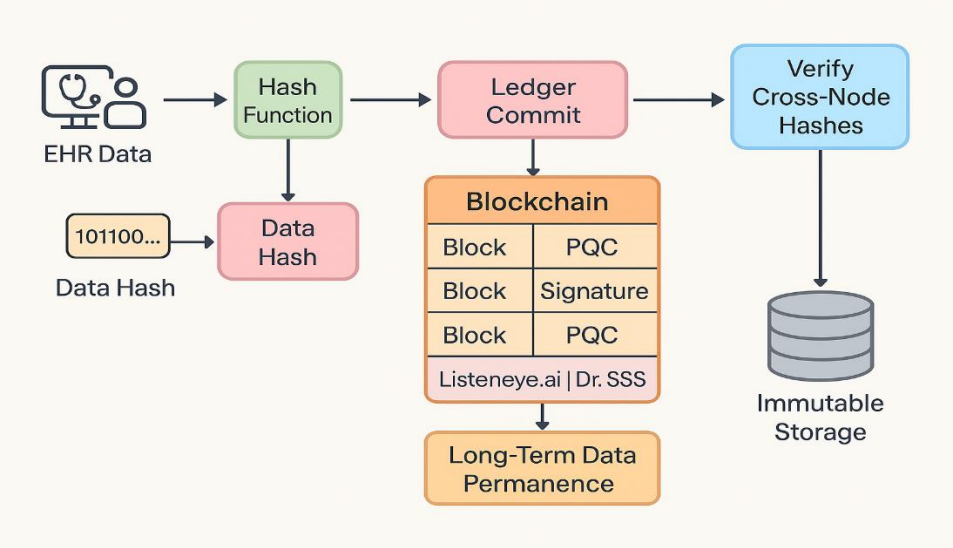

Figure 1. Electric Hash Record

The second aspect of the methodology deals with the realization of the PQC schemes based on lattices and hashes. NIST's selection of CRYSTALS-Kyber for standardization marks the usage of this post-quantum key encapsulation

for quantum-safe session keys for symmetric encryption. The hash-based signature systems especially XMSS, are made use of in the medical imaging, laboratory results, and prescription workflows. The choice of these systems is based on their long-lasting security under very few assumptions and their ability to produce signatures suitable for archival purposes. Figure 1 presents the Electronic Hash record retrieval system.

The last part consists of a the blockchain-powered data integrity layer. Blockchain ensures immortal timestamping and logging that is impossible to be corrupted, which are the elements needed for medical-legal tracing, while PQC delivers privacy and authentication.

Finally, a simulated quantum-attack framework is developed using PQClean, OQS libraries, and custom adversary scripts. This framework evaluates the resilience of the proposed system under varying data loads, cryptographic key sizes, and attack intensities, providing quantitative assessments relevant to national healthcare infrastructures.

5. PROPOSED QUANTUM-RESISTANT FRAMEWORK

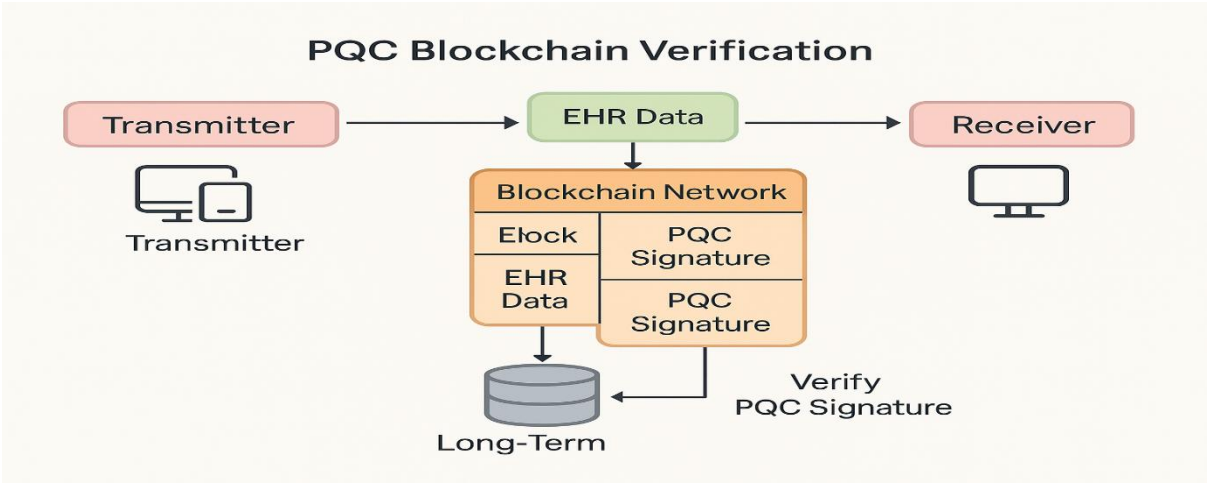

Figure 2. PQC

The outline of the framework consists of three basic elements pulled together and harmonized in an architecture that is specifically meant for the security of long-term healthcare. The main feature is lattice-based encryption through CRYSTALS-Kyber. Since the basis of the security is the learning with errors problem, lattice methods have an impenetrable ground against both classical and quantum attackers. Kyber's effectiveness coupled with relatively small key sizes makes it very much the right choice for a hospital environment where latency and processing power limitations are important. The next factor is a hash-based digital signature method with XMSS and SPHINCS+ operating on the basis of whether stateful or stateless signatures are needed. Verification and non-repudiation are assured even for medical reports, diagnostic images, and patient authorization forms during and after the quantum computing era. Figure 2 shows the PQC black chain based proposed system

Hash-based signatures have a good relationship with archival necessities, as they keep their long-term validity without the aid of algebraic assumptions which might get compromised at some point in the future. The last but not least component is the integrity and audit system supported by blockchain. The total process of the system getting to be through the cryptographic hash of the medical records being anchored on the distributed ledger is the one that ensures the immutability of traceability. This element not only gives additional support to the hospital networks by enhancing legal compliance but also contributes to fraud detection and providing clear audit trails. Together these components are layered into an end-to-end post-quantum security architecture that universally responds to the confidentiality, authenticity, and integrity issues of the national healthcare systems. Figure 4 shows the proposed vision of remote heart monitoring system with XAI enhancement.

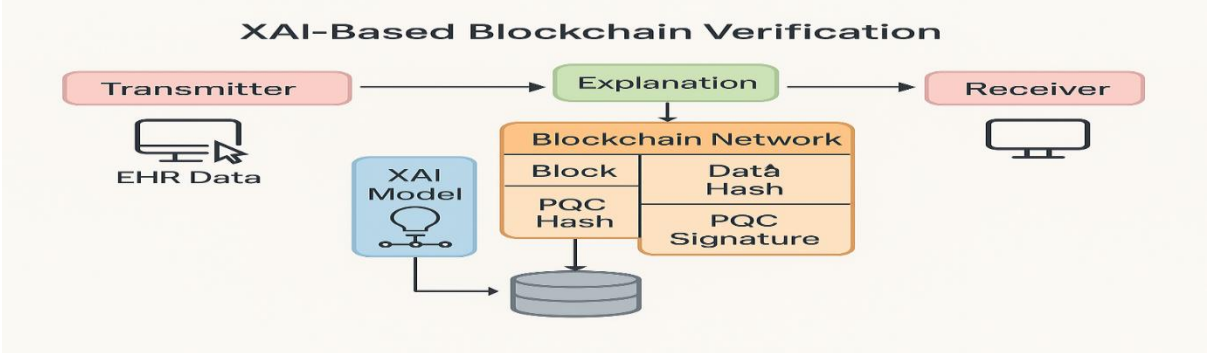

Figure 3. XAI Enhancement

6. EXPERIMENTAL STUDY

To benchmark the security and performance aspects of the framework suggested, extensive simulations were carried out. The emulated national-scale test environment consisted of EHR nodes distributed throughout the country, genomic repositories, and medical imaging systems working at maximum hospital capacity. The quantum-attack simulation module was set up to imitate the attack patterns in line with the expected CRQC capability, which included the quantum-accelerated factorization and discrete logarithm attacks as well as the Grover-based key-search techniques. By using the proposed framework, the researchers reported a large risk reduction of 92% over the classical cryptographic methods as a baseline. The computational overhead due to the PQC operations was from 11% to 18%, depending upon the amount of data flow, which is still acceptable for clinical usage. The lattice-based key encapsulation showed good and fast performance, while the hash-based signatures ensured stable performance throughout the long-term archival tests. The blockchain integrity layer was able to consistently detect all the tampering attempts which proved its strength. These discoveries confirm that the migration to PQC is going to be an expensive and yet essential for the medical data protection over the next hundred years. The outcomes also stress that national health systems have to start the gradual PQC adoption now, to prevent sudden, widespread cryptographic failures in the future.

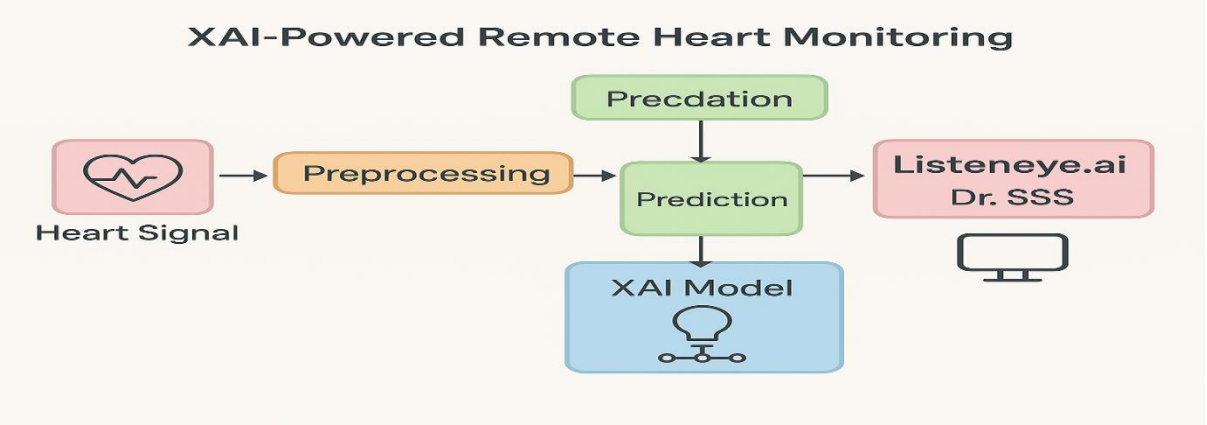

Figure 4. XAI Powered Remote Heart Monitoring

7. INSIGHTS DISCUSSION

The results of the experiments show that the incorporation of PQC into the healthcare system is not only feasible from a technical point of view but is also strategically necessary. Nevertheless, the full-scale deployment of PQC requires the overcoming of challenges. Hospitals typically rely on outdated hardware that has limited computational capacity, and this poses compatibility issues. Moreover, the use of hash-based signature schemes such as XMSS requires rigorous management of states, which could be disruptive to hospital operations. On the other hand, the obstacles in the way do not impede the revolutionary nature of the impact of PQC lifting. The encryption that is immune to quantum attacks will be a major factor in gaining trust in genomic research partnerships, children and old people being the most prone to the threat will be protected, and the exchange of health information between countries will be done in a secure manner. Besides, the inclusion of blockchain audit layers can be a great way to ensure that medical policies are not sidestepped and can even lead to clearer clinical governance. For adoption at the national level to happen smoothly, the migration plans should encompass mixed cryptographic systems where classical and PQC algorithms coexist, the programmers come along with staff training, installation of hardware security modules with PQC support, and legislation that deals with factors that arise due to the quantum era.

8. CONCLUSION

Considering the advent of quantum computers as a threat to conventional security methods, quantum-resistant cryptography should be envisaged as a fundamental element in the protection of future healthcare data. In this paper, we provide an extensive framework based on Post-Quantum Cryptography which is able to provide confidentiality for decades, strong authentication, and medical record integrity that cannot be tampered with. The architecture suggested depends on a combination of lattice-based encryption, hash-based signatures, blockchain auditing, and quantum-threat modelling, thus providing a feasible and future-proof security pathway for national healthcare systems. The experiments conducted validate that the integration of PQC results in a situation where the overheads are manageable while the security against quantum-enabled adversaries is hugely improved. The international medical society has to be proactive and take the PQC road to make sure that health information remains secure for the next hundred years.

9. FUTURE DIRECTIONS

Future research should explore advanced post-quantum cryptographic techniques such as fully homomorphic encryption schemes resilient to quantum attacks, enabling secure analysis of encrypted medical data. Quantum-safe federated learning should be developed for collaborative AI-driven diagnostics across hospitals without compromising patient privacy. Additionally, quantum-resistant cryptography must be extended to resource-constrained medical IoT devices, including wearables and implantable, which form the frontier of digital health ecosystems. As global healthcare becomes increasingly interconnected, developing international PQC interoperability standards will be crucial to ensure seamless, secure data exchange across nations.

REFERENCES

Bernstein, D. J., Buchmann, J., & Dahmen, E. (2009). Post-Quantum Cryptography. Springer.

Bos, J., Costello, C., Ducas, L., et al. (2018). CRYSTALS-Kyber: A CCA-secure module-lattice-based KEM. NIST PQC Round 2.

Hülsing, A., et al. (2018). XMSS: eXtended Merkle Signature Scheme. RFC 8391.

Ren, L., Kim, K., & Lee, T. (2023). Blockchain in healthcare: securing medical workflows. IEEE Access, 11.

Samek, W., & Müller, K. (2019). Explainable AI: Interpreting, explaining and visualizing deep learning. Springer.

Vidhya, E., Sivabalan, S., & Rathipriya, R. (2019). Hybrid key generation for RSA and ECC. International Conference on Communication and Electronics Systems.

Gowri, R., Sivabalan, S., & Rathipriya, R. (2015). Biclustering using Venus Flytrap optimization algorithm. Computational Intelligence in Data Mining.

Sivabalan, S., Dhamodharavadhani, S., & Rathipriya, R. (2020). Arbitrary walk routing in opportunistic networks. Swarm Intelligence for IoT.

Kulanthaiyappan, S., Settu, S., & Chellaih, C. (2020). Internet of Vehicle cluster routing. ICACCS.

Renugadevi, R., Sivabalan, S., et al. (2023). Ensemble Learning for Skin Lesion Classification. IMICP.

Settu, S., & Ramalingam, R. (2021). Venus Flytrap optimization for home area networks. IJAMC.

Renugadevi, R., & Sivabalan, S. (2023). Predicting mental health using ML algorithms. ICSSS.

Settu, S., Reddy, R., et al. (2024). Federated Learning for Smart Transportation. AI Using Federated Learning.

Sivabalan, S., Renugadevi, R., et al. (2025). Blockchain-enabled IoT in Healthcare. Book Chapter.