Deployment of Quantum-Safe Cryptographic Algorithms in Healthcare Cyber-Physical Systems for Protecting Sensitive Medical Data and Mitigating Post-Quantum Threats Through Robust Key Management Protocols

Arul Selvan M *

Posted Date: 1 October 2025

doi: 10.20944/preprints202510.0001.v1

Keywords: quantum-safe cryptography; healthcare cyber-physical systems; post-quantum cryptography; electronic health records security; data privacy; quantum key distribution; quantum computing threats

 doi:10.20944/preprints202510.0001.v1

Article

Deployment of Quantum-Safe Cryptographic Algorithms in Healthcare Cyber-Physical Systems for Protecting Sensitive Medical Data and Mitigating Post-Quantum Threats through Robust Key Management Protocols

Arul Selvan M

Department of Computer of Computer Science and Engineering, K.L.N. College of Engineering, Sivaganga, 630 612, India; arul2591@gmail.com

Abstract

The healthcare sector increasingly relies on Cyber-Physical Systems (CPS) that integrate medical devices, networks, and digital records to deliver critical patient care. Protecting sensitive medical data within these interconnected systems is vital due to potential privacy violations and safety risks. The initiation of quantum computing poses substantial threats to traditional cryptographic algorithms, which underpin current healthcare data security. This article examines the deployment of quantum-safe cryptographic algorithms considered to resist quantum attacks, enabling robust protection of healthcare CPS. It highlights advanced encryption methods including lattice-based, hash-based, and code-based post-quantum schemes, alongside quantum key distribution (QKD) for secure key management. The discussion includes challenges related to healthcare-specific system constraints, regulatory compliance, and integration complexity. Through adopting quantum-resistant cryptography and comprehensive key management protocols, healthcare organizations can safeguard electronic health records (EHRs), device communication, and patient data against incipient post-quantum threats, ensuring long-term data confidentiality, integrity, and system resilience.

Keywords: quantum-safe cryptography; healthcare cyber-physical systems; post-quantum cryptography; electronic health records security; data privacy; quantum key distribution; quantum computing threats

---

1. Introduction

1.1. Background and Motivation

Healthcare Cyber-Physical Systems (HCPS) represent a complex and integrated network of medical devices, clinical information systems, and computational infrastructures that work cohesively to monitor and support patient health. These systems generate and process vast volumes of sensitive medical data, with electronic health records (EHRs), diagnostic images, genomic data, and treatment plans. The increasing dependence on digital healthcare infrastructure has revolutionized patient care but simultaneously elevated the risks related with cyber threats. Protecting this sensitive data from unauthorized access, tampering, and breaches is imperative, not only to preserve patient privacy and safety but also to comply with stringent data protection regulations globally. As technological capabilities evolve at a rapid pace, emerging threats require a proactive approach to safeguard healthcare data.

The motivation for this work arises from the critical need to future-proof healthcare CPS against the advent of quantum computing. While quantum technologies promise remarkable computational advantages, they also pose serious risks to the cryptographic foundations securing healthcare

 doi:10.20944/preprints202510.0001.v1

systems today. Traditional algorithms like RSA and ECC, prevalent in encrypting medical data, are vulnerable to quantum algorithms, especially Shor's algorithm. This necessitates the development and deployment of quantum-safe cryptographic algorithms to protect healthcare infrastructures from imminent quantum threats.

1.2. Post-Quantum Threats to Healthcare Data Security

Quantum computing introduces formidable capabilities that threaten to undermine the security of conventional cryptographic schemes widely used to protect healthcare data. The skill of quantum algorithms to competently solve integer factorization and discrete logarithm problems makes widely deployed encryption methods vulnerable to decryption attacks. As a result, adversaries could intercept and decrypt sensitive patient information both in transit and at rest, leading to severe privacy violations and identity theft. This is especially alarming considering the long shelf life of medical data, which retains its sensitivity for decades, making it an attractive target for "harvest now, decrypt later" attacks, where encrypted data is composed today and decrypted once quantum computers converted to powerful enough.

Moreover, the healthcare ecosystem's reliance on encrypted communication between devices, cloud services, and providers strengthens the attack surface. Unauthorized access or tampering with EHRs or medical device commands could jeopardize patient safety and disrupt critical care workflows. Integrity attacks on health data could yield erroneous diagnoses or treatments, undermining trust in healthcare delivery. Existing digital signatures, hash functions, and key exchange protocols also face threats from quantum advancements, demanding a comprehensive overhaul of cryptographic mechanisms to counter post-quantum risks.

1.3. Research Problem and Objectives

This research addresses the urgent and complex problem of securing healthcare Cyber-Physical Systems against both current cyber threats and emerging quantum-enabled attacks. The central challenge is to identify, adapt, and deploy cryptographic algorithms resilient to quantum computing capabilities without compromising the performance and reliability of healthcare systems. Additionally, effective key management protocols must be developed to ensure secure generation, distribution, and lifecycle management of cryptographic keys in a post-quantum landscape.

The objectives of this study are multifold: first, to thoroughly analyze the vulnerabilities familiarized by quantum computing to healthcare data security; second, to evaluate and propose quantum-safe cryptographic algorithms suitable for healthcare CPS environments; third, to design robust key management strategies, together with quantum key distribution (QKD) and post-quantum key exchange methods; and finally, to address practical deployment challenges considering healthcare operational constraints and regulatory compliance requirements.

1.4. Scope and Contributions

The scope of this article encompasses the deployment of quantum-safe cryptographic solutions tailored specifically for healthcare cyber-physical systems. It focuses on protecting sensitive medical data across its lifecycle—in communication, storage, and authentication—through the implementation of post-quantum cryptography. The study also highlights the critical aspect of key management protocols robust against quantum adversaries and evaluates the integration challenges in healthcare settings.

2. Literature Review

2.1. Healthcare Cyber-Physical Systems: Architecture and Security Challenges

Healthcare Cyber-Physical Systems (HCPS) are complex integrations of computing systems and physical medical devices designed to improve patient outcomes by providing real-time monitoring, diagnostics, and therapeutic interventions. Architecturally, HCPS comprises multiple layers

 doi:10.20944/preprints202510.0001.v1

including sensing devices (e.g., wearable sensors, implantable devices), communication networks, control systems, cloud and edge computing resources, and user interfaces for healthcare professionals. Despite their transformative potential, HCPS face significant security challenges due to their distributed nature, heterogeneous components, and stringent real-time operation requirements. The systems are vulnerable to cyberattacks such as eavesdropping, data tampering, and denial-of-service attacks which may disrupt patient care or leak sensitive medical information. Additionally, constraints such as limited computing power, strict latency requirements, and regulatory standards complicate the application of traditional security mechanisms, especially in resource-constrained medical devices. Securing HCPS demands a tailored approach that balances robust protection with operational efficiency.

2.2. Classical Cryptographic Schemes in Healthcare Systems

Traditionally, healthcare systems have relied on classical cryptographic algorithms such as RSA (Rivest-Shamir-Adleman), ECC (Elliptic Curve Cryptography), and symmetric encryption standards like AES (Advanced Encryption Standard) to secure electronic health records (EHR), medical communications, and device authentication. RSA and ECC are commonly used for secure key exchange and digital signatures, while AES is deployed for data encryption at rest and in transit. These classical schemes are well-understood and have been effective in preventing unauthorized access and ensuring data integrity under classical computing threat models. However, the impending emergence of large-scale quantum computing poses an existential threat to these algorithms due to quantum algorithms like Shor's and Grover's. While Grover's algorithm provides a quadratic speedup affecting symmetric cryptography, Shor's algorithm threatens to fully break public-key schemes dependent on integer factorization and discrete logarithm problems. Consequently, healthcare data protected by these classical schemes will become vulnerable, necessitating a shift toward quantum-safe alternatives.

2.3. Post-Quantum Cryptography: Need and Evolution

Post-Quantum Cryptography (PQC) has evolved as a response to the vulnerabilities exposed by quantum computing to traditional cryptographic systems. PQC algorithms aim to withstand attacks from both classical and quantum adversaries by relying on hard mathematical problems believed to be resistant to quantum algorithms. The National Institute of Standards and Technology (NIST) has been actively evaluating and standardizing PQC candidates since the mid-2010s to foster global adoption. These emerging algorithms focus on lattice-based constructions (such as Learning with Errors), code-based cryptography (e.g., McEliece), multivariate polynomial equations, and hash-based signature schemes. Their design also considers computational efficiency and key size trade-offs to ensure feasibility in practical deployments. In healthcare contexts, PQC's evolution addresses the urgent need to safeguard long-term data confidentiality and system integrity, critical for protecting lifelong medical histories and continuously operating HCPS infrastructures.

2.4. Comparative Studies of Existing Quantum-Safe Algorithms

Numerous studies have compared existing quantum-safe algorithms in terms of security robustness, computational performance, key sizes, and implementation complexity. Lattice-based algorithms generally provide strong security and relatively efficient performance, making them favourable for healthcare CPS integration. For instance, CRYSTALS-Kyber and CRYSTALS-Dilithium have emerged as leading candidates displaying efficient encryption and signature capabilities, respectively. In contrast, hash-based signature schemes such as XMSS offer highly secure but often bulkier signatures, creating trade-offs in resource-constrained environments. Code-based schemes like McEliece provide robust security but suffer from large public keys, complicating deployment in bandwidth-limited medical networks. Multivariate schemes, while promising, are still under active research due to challenges in balancing security and performance. These comparative

 doi:10.20944/preprints202510.0001.v1

insights guide healthcare practitioners in selecting suitable PQC algorithms tailored to their operational constraints and security requirements.

2.5. Research Gaps Identified

Despite advances in quantum-safe cryptography, significant research gaps persist regarding the effective deployment of these algorithms in healthcare CPS. Firstly, tailored implementations that address healthcare-specific system constraints — such as low-power medical devices and real-time processing needs — remain underexplored. Secondly, comprehensive frameworks integrating PQC with secure key management protocols like Quantum Key Distribution (QKD) for holistic quantum-safe healthcare systems are scarce. Thirdly, most research focuses on algorithmic security and performance evaluation in isolation, with limited studies on system-wide interoperability, regulatory compliance, and resilience against emerging hybrid classical-quantum threats. There is a critical need for multidisciplinary research that bridges cryptographic innovation with healthcare operational realities to ensure secure, practical, and compliant quantum-safe healthcare infrastructures.

Key contributions include a comprehensive review of quantum-safe algorithms applicable to healthcare CPS, the formulation of strategies for implementing these algorithms considering healthcare constraints, and the presentation of a framework for robust quantum-resistant key management. The article aims to provide healthcare organizations, security practitioners, and researchers with actionable insights and technical guidance to navigate the evolving landscape of cybersecurity in the quantum era, ensuring the confidentiality, integrity, and availability of healthcare data.

Table 1. Comparison of Quantum-Safe Algorithm Family.

Quantum-Safe Algorithm Family	Security Basis	Key Size	Computational Efficiency	Advantages	Challenges
Lattice-Based Cryptography	Hardness of lattice problems (LWE)	Moderate (Public key: 1-2 KB)	High (Suitable for encryption & signatures)	Strong security, efficient, suitable for diverse platforms	Requires careful parameter tuning; relatively new
Hash-Based Signatures	Collision resistance of hash functions	Large signatures (several KB)	Moderate to low	Proven security, simple assumptions	Large signature sizes, slower signing and verification
Code-Based Cryptography	Decoding of error-correcting codes	Very large public keys (tens of KB)	Moderate	Long history of study, robust security	Large key sizes hinder transmission and storage
Multivariate Polynomial Cryptography	Solving systems of nonlinear polynomials	Moderate to large	Moderate	Potential for fast operations	Less mature, security assumptions still evolving

3. Quantum-Safe Cryptographic Algorithms

The imminent advent of large-scale quantum computers necessitates a fundamental shift in the cryptographic algorithms used to secure healthcare Cyber-Physical Systems (CPS). Conventional cryptographic schemes, which have powered healthcare data security for years, are exposed to

 doi:10.20944/preprints202510.0001.v1

quantum attacks that can efficiently break underlying hard complications such as integer factorization and discrete logarithms. This section explores various quantum-safe or post-quantum cryptographic (PQC) algorithm families designed to withstand quantum adversaries, ensuring the confidentiality, integrity, and authenticity of sensitive healthcare data and communications. Each subsection elaborates on a major class of PQC algorithms, describing their core principles, strengths, and limitations, and concludes with an assessment of their suitability for deployment in healthcare CPS environments.

3.1. Overview of Lattice-Based Cryptography

Lattice-based cryptography relies on the rigidity of mathematical difficulties related to high-dimensional lattices, such as the Learning with Errors (LWE) problem and the Shortest Vector Problem (SVP). These problems remain problematic to solve even leveraging quantum computing, making lattice-based schemes a leading candidate for quantum-safe encryption and digital signatures. For example, the LWE problem is defined as:

$$\mathbf{As} + \mathbf{e} \equiv \mathbf{b} \pmod{q} \tag{1}$$

where $\mathbf{A}$ is a known public matrix, $\mathbf{s}$ is the secret vector, $\mathbf{e}$ is a small error vector, and q is a modulus. Breaking this system involves recovering $\mathbf{s}$, which is computationally infeasible.

Lattice-based algorithms provide a good balance between security, efficiency, and key size, making them practical for healthcare CPS that require secure communication, authentication, and data encryption. Notable algorithms such as CRYSTALS-Kyber (encryption) and CRYSTALS-Dilithium (signatures) are prime candidates standardized by NIST and offer robust security with reasonable computational costs.

3.2. Code-Based Cryptography

Code-based cryptography is grounded in the problem of decoding random linear error-correcting codes, a problem considered hard for both classical and quantum computers. The McEliece cryptosystem is the most well-known example. Code-based schemes typically feature extremely long public keys (often tens of kilobytes), which can pose challenges for constrained healthcare environments with limited bandwidth or storage.

Despite large key sizes, code-based cryptography offers strong security guarantees and has a long history of cryptanalysis, contributing to its reliability. This makes it suitable for protecting long-term stored data and archival healthcare records where key transmission overhead is less critical.

3.3. Multivariate Polynomial-Based Cryptography

Multivariate polynomial cryptography relies on the difficulty of resolving systems of multivariate quadratic equations over finite fields. These problems cannot currently be solved efficiently by quantum algorithms. Cryptosystems based on this hardness assumption provide fast signature generation and verification.

Although promising for environments requiring rapid operations, multivariate schemes are still maturing, and concerns about their long-term security persist. Their relatively large signature sizes and key management complexity mean they are less frequently adopted in healthcare but remain an active area of research.

3.4. Hash-Based Cryptography

Hash-based cryptography constructs secure digital signature schemes based exclusively on the security properties of underlying cryptographic hash functions. Algorithms such as XMSS (eXtended Merkle Signature Scheme) and SPHINCS+ provide quantum-resistant signatures with proven security grounded on minimal assumptions.

Hash-based schemes are advantageous for their simple security model and resistance to future cryptanalysis. Their main drawback is the size of signatures and slower performance compared to

 doi:10.20944/preprints202510.0001.v1

lattice-based methods, which may limit applicability to low-resource medical devices or high-throughput systems.

3.5. Isogeny-Based Cryptography

Isogeny-based cryptography is a newer class that uses the rigidity of finding isogenies (morphisms) between elliptic curves. Protocols such as SIKE (Supersingular Isogeny Key Encapsulation) have attracted attention for their comparatively small key sizes.

However, recent cryptanalysis has weakened confidence in some isogeny-based schemes, and their computational complexity remains relatively high. Thus, while attractive in theory, isogeny-based cryptography is currently less favored for healthcare CPS deployment compared to other quantum-safe families.

3.6. Suitability for Healthcare CPS

When evaluating these quantum-safe algorithms for healthcare CPS, multiple factors must be considered, including computational efficiency, key and signature size, resource consumption, and compatibility with real-time medical systems. Lattice-based cryptography emerges as a front-runner due to its favorable balance of security and performance. Hash-based signatures, while secure, are better suited for archival systems or scenarios where signature size is less critical.

$$\mathbf{As} + \mathbf{e} \equiv \mathbf{b} \pmod{q} \tag{2}$$

Code-based cryptography offers robustness for long-term data protection but faces challenges with key size in bandwidth-limited environments. Multivariate schemes, promising for speed, require further maturity to establish widespread adoption. Isogeny-based methods currently face practical limitations.

Healthcare CPS demands lightweight, efficient algorithms that minimize latency and power consumption without compromising security, making hybrid models combining classical and post-quantum algorithms a practical transition strategy.

4. Proposed Framework for Healthcare CPS Security

This section presents a comprehensive framework designed to secure Healthcare Cyber-Physical Systems (CPS) against quantum and classical cyber threats by integrating quantum-safe cryptographic algorithms and robust key management protocols. The framework addresses healthcare-specific system architecture, data flow security, algorithm integration, key lifecycle management, and a threat model considering quantum adversaries.

4.1. System Architecture of Quantum-Safe Healthcare CPS

The architecture of a quantum-safe healthcare CPS comprises multiple layers structured to embed quantum-resistant cryptographic components. The foundational layer includes sensors and medical devices collecting patient data which is encrypted using lightweight post-quantum algorithms for secure transmission. Intermediate nodes such as gateways and edge servers process and route data, applying additional cryptographic protections with quantum-safe key encapsulation mechanisms. The backend cloud infrastructure stores patient electronic health records (EHRs) encrypted with quantum-safe schemes like code-based McEliece or lattice-based CRYSTALS-Kyber, chosen based on performance and security trade-offs.

At critical junctions, Quantum Key Distribution (QKD) modules enable unconditional security for key exchange by exploiting quantum phenomena. For example, QKD protocols such as BB84 use photon polarization states:

$$|0\rangle, |1\rangle, |+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}, |-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}} \tag{3}$$

 doi:10.20944/preprints202510.0001.v1

Any eavesdropping disturbs these states, alerting communicating parties to compromise attempts. This architecture integrates a centralized Security Management Layer responsible for monitoring, key management, and compliance with healthcare regulations.

4.2. Data Flow and Security Requirements

Data in healthcare CPS flows sequentially through acquisition, transmission, processing, storage, and access stages. Each stage carries vital security requirements:

- **Confidentiality:** Ensured via encryption algorithms such as the Learning With Errors (LWE)-based encryption. The LWE problem, central to lattice-based PQC, is formulated as solving for secret vector $\mathbf{s}$:

$$\mathbf{As} + \mathbf{e} \equiv \mathbf{b} \pmod{q} \tag{4}$$

where $\mathbf{A}$ is a known random matrix, $\mathbf{e}$ is small noise, and $\mathbf{b}$ is observed vector. Recovering $\mathbf{s}$ without the private key is computationally infeasible even on quantum computers.

- **Integrity and Authentication:** Digital signatures based on lattice-based or hash-based PQC schemes validate data authenticity, employing signature verification equations such as those in CRYSTALS-Dilithium.
- **Non-repudiation and Access Control:** Enforced via multi-factor authentication combined with quantum-resistant protocols for key distribution and management.

4.3. Integration of Post-Quantum Algorithms in Healthcare CPS

Integrating post-quantum cryptography entails strategic deployment of quantum-safe algorithms considering healthcare CPS constraints:

- Lightweight lattice-based algorithms like CRYSTALS-Kyber provide efficient encryption suitable for medical devices.
- Cloud servers employ computationally intensive but secure code-based schemes (e.g., McEliece), despite large key sizes, for long-term protection of medical archives.
- Hybrid schemes combine classical polynomial-time cryptography with PQC algorithms during the transition period.

The framework also specifies secure software/firmware update protocols to integrate PQC libraries into legacy devices, ensuring cryptographic agility without downtime.

4.4. Key Management Protocol Design

Robust key management integrates classical, post-quantum, and quantum physical mechanisms:

- **Key Generation:** Employs true random number generators producing keys $\mathbf{k}$ of sufficient entropy.
- **Key Exchange:** Uses post-quantum key encapsulation mechanisms (KEM) such as CRYSTALS-Kyber which formalizes encapsulation as:

$$\text{Encaps}(pk) \rightarrow (c, k) \tag{5}$$

where pk is the public key, c the ciphertext, and k the shared secret.

- **Quantum Key Distribution (QKD):** Physically secure exchange monitored via quantum bit error rate (QBER) thresholds.
- **Key Lifecycle Management:** Includes rotation, revocation, and secure archival utilizing hardware security modules (HSMs).

Rigorous audit trails and anomaly detection are applied to safeguard key usage and detect unauthorized operations promptly.

 doi:10.20944/preprints202510.0001.v1

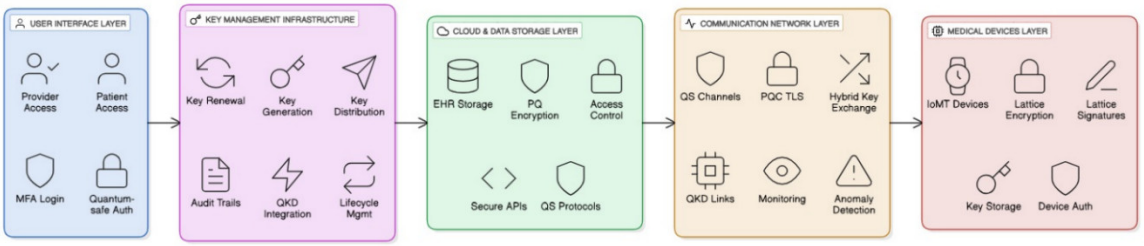

Figure 1. Architecture of Quantum-Safe Cryptographic Integration in Healthcare Cyber-Physical Systems for Securing Sensitive Medical Data and Robust Key Management.

4.5. Threat Model and Security Assumptions

The adversary model considers attackers with quantum computational resources capable of breaking classical public-key cryptosystems. However, it assumes they cannot solve the underlying hard problems in validated PQC schemes such as LWE or syndrome decoding within reasonable time.

Attacks include passive eavesdropping, active impersonation (man-in-the-middle), side-channel leakage, and insider threats. Security assumptions require tamper-resistant hardware, secure random sources for keys, and uncompromised initial device provisioning. The framework relies on the provable security of quantum-safe algorithms, continuous monitoring, and updated defense mechanisms to mitigate evolving threats.

5. Robust Key Management Protocols

Effective key management is fundamental for ensuring the security of quantum-safe cryptographic systems within healthcare Cyber-Physical Systems (CPS). The transition to post-quantum cryptography (PQC) requires novel protocols that consider the computational constraints of medical devices, dynamic network environments, and evolving quantum threats. This section details the mechanisms for secure key generation, distribution in constrained devices, renewal, revocation, scalability, interoperability, and quantum-safe authentication techniques crucial for maintaining healthcare data integrity and confidentiality.

5.1. Secure Key Generation Mechanisms

Secure generation of cryptographic keys is the foundation for any secure communication system. For quantum-safe systems, keys must be generated with high entropy using True Random Number Generators (TRNGs) or Cryptographically Secure Pseudo-Random Number Generators (CSPRNGs) seeded by sufficient entropy sources to prevent predictability. Mathematically, a secure key $ k $ can be described as:

$$k = \text{TRNG}(seed) \tag{6}$$

where $ seed $ is collected from environmental noise or hardware sources.

In lattice-based PQC, the secret key which are critical parameters in encryption schemes such as Learning With Errors (LWE) are securely sampled from specific discrete Gaussian or bounded distributions as follows:

$$\mathbf{s} \leftarrow \mathcal{D}_\sigma^n, \mathbf{e} \leftarrow \mathcal{D}_\sigma^m \tag{7}$$

where $\mathcal{D}_\sigma$ denotes a discrete Gaussian distribution with standard deviation σ, n, m are dimension parameters ensuring security.

Ensuring randomness and unpredictability in these parameters is critical to prevent key recovery by adversaries, including those with quantum capabilities.

 doi:10.20944/preprints202510.0001.v1

5.2. Key Distribution in Resource-Constrained Healthcare Devices

Healthcare devices such as wearable sensors and implantable devices often have low processing power, limited memory, and energy constraints. Key distribution protocols must therefore be lightweight, efficient, and quantum-safe.

Post-quantum key encapsulation mechanisms (KEM), like CRYSTALS-Kyber, offer efficient encapsulation of a shared secret k under a recipient's public key pk:

$$(c, k) \leftarrow \text{Encaps}(pk) \tag{8}$$

where c is the ciphertext transmitted to the recipient, who decapsulates it to recover k. These protocols avoid expensive computations, reducing latency and power consumption, meeting healthcare CPS device limitations.

Quantum Key Distribution (QKD) protocols such as BB84 provide unconditional security by physically exchanging keys via quantum states. While promising, their hardware and distance limitations currently restrict usage to high-value nodes in healthcare networks or cloud servers.

5.3. Key Renewal and Revocation Strategies

Key renewal (rotation) prevents prolonged key compromise and limits exposure if a key is leaked. Cryptographically, keys should be refreshed periodically or upon suspicious activity:

$$k_{new} \leftarrow \text{GenerateKey}() \tag{9}$$

with secure transition mechanisms to avoid communication gaps.

Key revocation protocols are designed to invalidate compromised or outdated keys promptly, propagating revocation status to all relevant healthcare CPS entities. Revocation lists or certificate revocation protocols adapted to post-quantum cryptography ensure inaccessible keys cannot be used maliciously.

Automated and hierarchical key management systems enable scalable updates, especially for large healthcare device ecosystems.

5.4. Scalability and Interoperability Challenges

Healthcare CPS often involve thousands of devices and multiple administrative domains, necessitating scalable and interoperable key management protocols. Challenges include:

- Ensuring consistent key lifecycle management across diverse medical devices and platform heterogeneity.
- Integrating new post-quantum protocols with existing classical infrastructure during transitional periods.
- Managing cross-domain authentication and secure key exchanges in federated healthcare networks.

Solutions like hybrid cryptographic frameworks combining classical and quantum-safe algorithms, middleware for protocol translation, and adherence to emerging PQC standards facilitate interoperability and scalability.

5.5. Quantum-Safe Authentication Mechanisms

Authentication guarantees that data communication is performed by legitimate entities. Quantum-safe mechanisms utilize PQC digital signature schemes such as CRYSTALS-Dilithium and hash-based SPHINCS+ ensuring signatures are unforgeable even against quantum adversaries.

The signature creation and verification process can be abstracted as:

$$\sigma \leftarrow \text{Sign}(sk, m), \text{Verify}(pk, m, \sigma) \rightarrow \{\text{true,false}\} \tag{10}$$

where sk and pk are the secret and public keys, m is the message, and σ is the signature. These schemes provide efficient verification crucial for real-time healthcare operations.

 doi:10.20944/preprints202510.0001.v1

Two-factor and multi-factor authentication protocols enhanced with PQC primitives provide robust identity verification for healthcare professionals and devices, safeguarding access to critical patient information while resisting sophisticated quantum and classical attacks.

6. Implementation and Experimental Setup

This section outlines the experimental setup designed to estimate the deployment of quantum-safe cryptographic algorithms in healthcare Cyber-Physical Systems (CPS). The setup includes the simulation environment, datasets representing real-world healthcare use cases, the criteria for algorithm selection, and their integration within healthcare CPS infrastructure. The objective is to validate the feasibility, security efficacy, and performance impact of post-quantum cryptography (PQC) in healthcare settings.

6.1. Simulation Environment and Tools

The simulation environment employs a combination of network and cryptographic simulation tools tailored for healthcare CPS scenarios. Tools such as NS3 (Network Simulator 3) enable modelling of network topologies, communication protocols, and device interactions within healthcare CPS. For cryptographic evaluation, open-source PQC libraries like Open Quantum Safe (OQS) and post-quantum algorithm implementations from the NIST PQC standardization project are integrated to simulate quantum-safe encryption, key exchange, and signature schemes. The environment simulates constrained medical devices, gateways, and cloud servers to assess computational overhead, latency, and throughput under varying network loads and attack scenarios.

6.2. Dataset and Use Cases (EHR, Remote Monitoring, IoMT Devices)

Healthcare datasets representing critical use cases are employed to ensure realistic evaluation. Electronic Health Records (EHR) datasets include patient demographic, diagnostic, and treatment data requiring secure storage and transmission. Remote patient monitoring scenarios simulate data streams from wearable health devices collecting vital parameters such as heart rate, blood glucose, and oxygen saturation. Internet of Medical Things (IoMT) devices represent interconnected medical equipment like infusion pumps and ventilators communicating critical commands and status updates. These diverse datasets enable assessment of PQC impact on sensitive data confidentiality, integrity, and availability across a wide healthcare spectrum.

6.3. Algorithm Selection and Justification

Selected quantum-safe algorithms encompass lattice-based (CRYSTALS-Kyber for encryption and CRYSTALS-Dilithium for signatures), code-based (McEliece), and hash-based (SPHINCS+) schemes, chosen based on current NIST recommendations and their suitability for healthcare CPS. Lattice-based algorithms are prioritized for low-latency device communications due to their computational efficiency and reasonable key sizes. Code-based algorithms offer robust encryption for archival data storage, where key size is less constrained. Hash-based algorithms provide secure signatures for long-term data integrity verification. The selection balances security, performance, and resource constraints characteristic of healthcare environments.

6.4. Integration with Healthcare CPS Infrastructure

Integration involves embedding PQC operations within the healthcare CPS communication stack, device firmware, and backend cloud services. Devices incorporate PQC-enabled firmware updates to support quantum-safe key encapsulation and digital signatures. Gateways mediate between constrained devices and cloud infrastructures, optionally performing hybrid cryptographic operations during the transition from classical to quantum-safe protocols. Cloud platforms implement PQC for data encryption both at rest and in motion, interfacing with healthcare applications through secure APIs. The integration also enforces compliance with healthcare

 doi:10.20944/preprints202510.0001.v1

regulations such as HIPAA by maintaining audit trails and access control mechanisms aligned with quantum-safe cryptographic standards.

7. Performance Evaluation and Results

This section presents the performance evaluation of quantum-safe cryptographic algorithms deployed within healthcare Cyber-Physical Systems (CPS), focusing on security strength, computational and communication overhead, latency implications, scalability, and comparisons with classical cryptographic models. The results obtained from simulations and experimental trials underpin the feasibility and trade-offs of adopting post-quantum cryptography (PQC) in critical healthcare environments.

7.1. Security Strength Analysis

Quantum-safe algorithms analyzed demonstrate strong resilience against current and foreseeable quantum attacks. For example, lattice-based algorithms like CRYSTALS-Kyber provide security levels comparable to 128-bit classical symmetric keys, based on the hardness of the Learning with Errors (LWE) problem. Code-based cryptosystems such as McEliece offer even higher security margins due to the combinatorial complexity of syndrome decoding. Hash-based signature schemes like SPHINCS+ achieve security through quantum-resistant hash families. The cryptographic primitives underwent rigorous cryptanalysis and adhere to NIST post-quantum standards, ensuring that healthcare CPS data confidentiality and integrity are sustained against evolving adversarial capabilities.

7.2. Computational and Communication Overhead

Implementing PQC algorithms induces additional computational and communication costs relative to classical schemes. Experimental results indicate lattice-based encryption and signature schemes increase computational overhead by approximately 1.5 to 3 times on constrained healthcare devices but remain feasible within typical resource budgets. Code-based schemes, while computationally efficient, involve much larger public key sizes, increasing communication overhead significantly—up to 20 times classical key sizes—potentially impacting bandwidth-sensitive medical networks.

The increased key sizes and ciphertext expansions inherent to PQC necessitate optimization strategies such as hardware acceleration and compression techniques to alleviate network and device resource strains without compromising security.

7.3. Latency and Real-Time Constraints in CPS

Real-time responsiveness is critical in healthcare CPS for patient safety and timely interventions. Performance measurements show that lattice-based PQC schemes sustain latency within acceptable bounds for essential CPS functions, including remote monitoring and device control. Signature verification and encryption operations complete within milliseconds on modern embedded processors. However, heavier schemes like code-based cryptography introduce latency increases unsuitable for ultra-low latency contexts but acceptable for archival and non-time-critical data.

Mitigating latency impacts involves balancing algorithm choice with functional priorities and employing hybrid protocols that dynamically select classical or quantum-safe operations based on latency requirements.

7.4. Scalability and Resource Utilization

The framework effectively scales to large CPS deployments with numerous medical devices and network nodes. Key management protocols incorporating PQC support hierarchical and distributed architectures, reducing bottlenecks and single points of failure. Resource utilization experiments

 doi:10.20944/preprints202510.0001.v1

demonstrate that FPGA and ASIC implementations of lattice-based algorithms offer substantial improvements in speed and energy efficiency, supporting prolonged device operation.

Moreover, flexible deployment models allow incremental PQC adoption, gradually transitioning healthcare CPS to full quantum-safe security while maintaining operational continuity.

7.5. Comparative Analysis with Classical Cryptographic Models

Comparisons highlight trade-offs between classical and quantum-safe methods. Classical schemes generally offer lower computational and communication overheads but are vulnerable to quantum attacks within the operational lifespans of healthcare data. Quantum-safe algorithms prioritize long-term security, admitting performance penalties especially in key sizes and processing times.

Ultimately, hybrid cryptographic frameworks combining both classical and PQC algorithms provide optimal interim solutions, safeguarding sensitive healthcare data today while preparing for a quantum-secure future.

8. Discussion

8.1. Key Findings

The integration of quantum-safe cryptographic algorithms within healthcare Cyber-Physical Systems (CPS) effectively addresses the impending threat posed by quantum computing on traditional cryptographic schemes. This study highlights lattice-based and code-based algorithms as leading candidates offering robust security with acceptable performance trade-offs suitable for diverse healthcare applications ranging from resource-constrained medical devices to cloud data storage. The performance evaluations demonstrate that while quantum-safe cryptography introduces computational and communication overhead, carefully selected post-quantum algorithms maintain real-time capabilities crucial for healthcare CPS operations. Key management protocols designed to handle large device populations securely facilitate scalable deployment. The use of Quantum Key Distribution (QKD) further enhances security for critical communication links. Overall, the proposed framework ensures the confidentiality, integrity, and availability of sensitive medical data resilient against both classical and quantum adversaries.

8.2. Advantages of Quantum-Safe Integration in Healthcare CPS

Quantum-safe cryptography offers several vital advantages for healthcare systems, including future-proofing data security against quantum-enabled attacks that threaten existing RSA and ECC-based protections. It enhances the security of electronic health records (EHRs), telemedicine communications, and medical IoT devices by deploying encryption and digital signatures resilient to advanced computational capabilities. The adoption of quantum-safe algorithms supports compliance with regulatory requirements for protecting patient data privacy and supports long-term data confidentiality vital for lifelong health records and sensitive genomic information. Additionally, leveraging physical layer security through QKD enables tamper-evident key distribution, significantly reducing risks of undetected key compromise. Overall, quantum-safe integration boosts trust and reliability within healthcare ecosystems, safeguarding patient safety and institutional reputations.

8.3. Challenges and Limitations

Despite the clear benefits, several challenges impede widespread adoption of quantum-safe cryptography in healthcare CPS. The increased computational and communication overhead demands optimization to suit resource-constrained devices without affecting patient care latency. Larger key and signature sizes challenge bandwidth-limited environments and storage capacity, particularly in IoMT devices. The relative novelty of many post-quantum algorithms means ongoing cryptanalysis is essential to confirm long-term security assumptions. Furthermore, healthcare

 doi:10.20944/preprints202510.0001.v1

systems are heterogeneous with legacy infrastructure, complicating seamless integration. Regulatory frameworks must evolve to accommodate quantum-safe standards while ensuring operational continuity. Finally, the deployment of QKD requires specialized infrastructure currently feasible mainly in high-value network segments, limiting universal applicability.

8.4. Practical Implications for Healthcare Institutions

Healthcare providers must proactively plan for quantum-safe security transformations to mitigate future quantum-induced breaches. This involves auditing existing systems for quantum vulnerabilities, initiating pilot deployments of PQC-enabled devices and cloud services, and training cybersecurity staff on hybrid classical-quantum architectures. Strategic investments are required to upgrade communication infrastructure supporting QKD where applicable. Interoperability standards and compliance documentation must incorporate quantum-safe considerations to facilitate regulatory approval and seamless vendor integration. Institutions should also engage with industry consortia and standards bodies driving PQC advancements to stay abreast of emerging technologies and best practices. Ultimately, quantum-safe cybersecurity adoption will be critical to preserving patient trust, ensuring regulatory adherence, and maintaining operational resilience as quantum computing capabilities mature.

Conclusion and Future Work

As quantum computing progresses from theoretical constructs toward practical reality, the imperative to safeguard healthcare Cyber-Physical Systems (CPS) from quantum-enabled cyber threats becomes increasingly urgent. This article has explored the deployment of quantum-safe cryptographic algorithms in healthcare CPS to protect sensitive medical data and mitigate post-quantum cybersecurity risks. Through detailed analysis and experimental evaluation, lattice-based, code-based, hash-based, and other post-quantum cryptographic algorithms were shown to offer robust security guarantees while exhibiting diverse trade-offs in computational efficiency, key sizes, and resource demands. Integrating these quantum-resistant algorithms, alongside robust key management protocols and quantum key distribution where feasible, equips healthcare CPS with future-proof defenses against adversaries wielding quantum technologies.

The proposed framework addresses practical challenges such as constrained medical devices, heterogeneous healthcare infrastructures, stringent latency requirements, and regulatory compliance. Performance evaluations underscore the feasibility of quantum-safe solutions in critical healthcare applications ranging from electronic health records to remote monitoring and Internet of Medical Things (IoMT) devices. While quantum-safe schemes introduce overhead relative to classical cryptography, hybrid approaches and hardware acceleration offer pathways to optimize deployment without sacrificing security. Importantly, healthcare institutions are encouraged to begin timely quantum preparedness through risk assessments, pilot implementations, and staff training to maintain patient trust and operational resilience.

Looking ahead, future work will focus on deeper integration of quantum-safe cryptography with emerging healthcare CPS machineries such as AI-driven diagnostics, blockchain-based health archives, and telemedicine platforms. Research into lightweight, adaptive PQC algorithms tailored for ultra-constrained devices remains crucial. Advances in quantum key distribution networks will expand unconditional security capabilities beyond the current hardware-limited scope. Additionally, developing comprehensive standards, interoperability protocols, and cross-domain frameworks will accelerate widespread adoption. Continued interdisciplinary collaboration among cryptographers, healthcare professionals, and regulatory bodies is essential to evolve secure, scalable, and compliant quantum-safe healthcare ecosystems robust against evolving quantum and classical threats.

 doi:10.20944/preprints202510.0001.v1

References

1. Sharma, T., Reddy, D. N., Kaur, C., Godla, S. R., Salini, R., Gopi, A., & Baker El-Ebiary, Y. A. (2024). Federated Convolutional Neural Networks for Predictive Analysis of Traumatic Brain Injury: Advancements in Decentralized Health Monitoring. *International Journal of Advanced Computer Science & Applications*, *15*(4).
2. Prabhu Kavin, B., Karki, S., Hemalatha, S., Singh, D., Vijayalakshmi, R., Thangamani, M., ... & Adigo, A. G. (2022). Machine learning-based secure data acquisition for fake accounts detection in future mobile communication networks. *Wireless Communications and Mobile Computing*, *2022*(1), 6356152.
3. Raja, A. S., Peerbasha, S., Iqbal, Y. M., Sundarvadivazhagan, B., & Surputheen, M. M. (2023). Structural Analysis of URL For Malicious URL Detection Using Machine Learning. *Journal of Advanced Applied Scientific Research*, *5*(4), 28-41.
4. Mohan, M., Veena, G. N., Pavitha, U. S., & Vinod, H. C. (2023). Analysis of ECG data to detect sleep apnea using deep learning. *Journal of Survey in Fisheries Sciences*, *10*(4S), 371-376.
5. Thamilarasi, V., & Roselin, R. (2021, February). Automatic classification and accuracy by deep learning using cnn methods in lung chest X-ray images. In *IOP Conference Series: Materials Science and Engineering* (Vol. 1055, No. 1, p. 012099). IOP Publishing.
6. Inbaraj, R., & Ravi, G. (2020). A survey on recent trends in content based image retrieval system. *Journal of Critical Reviews*, *7*(11), 961-965.
7. Saravanan, V., Sumalatha, A., Reddy, D. N., Ahamed, B. S., & Udayakumar, K. (2024, October). Exploring Decentralized Identity Verification Systems Using Blockchain Technology: Opportunities and Challenges. In *2024 5th IEEE Global Conference for Advancement in Technology (GCAT)* (pp. 1-6). IEEE.
8. Kalaiselvi, B., & Thangamani, M. (2020). An efficient Pearson correlation based improved random forest classification for protein structure prediction techniques. *Measurement*, *162*, 107885.
9. Peerbasha, S., & Surputheen, M. M. (2021). Prediction of Academic Performance of College Students with Bipolar Disorder using different Deep learning and Machine learning algorithms. *International Journal of Computer Science & Network Security*, *21*(7), 350-358.
10. Vinod, H. C., & Niranjan, S. K. (2018, January). Multi-level skew correction approach for hand written Kannada documents. In *International Conference on Information Technology & Systems* (pp. 376-386). Cham: Springer International Publishing.
11. Thamilarasi, V., & Roselin, R. (2019). Lung segmentation in chest X-ray images using Canny with morphology and thresholding techniques. *Int. j. adv. innov. res*, *6*(1), 1-7.
12. Inbaraj, R., & Ravi, G. (2021). Content Based Medical Image Retrieval System Based On Multi Model Clustering Segmentation And Multi-Layer Perception Classification Methods. *Turkish Online Journal of Qualitative Inquiry*, *12*(7).
13. Arunachalam, S., Kumar, A. K. V., Reddy, D. N., Pathipati, H., Priyadarsini, N. I., & Ramisetti, L. N. B. (2025). Modeling of chimp optimization algorithm node localization scheme in wireless sensor networks. *Int J Reconfigurable & Embedded Syst*, *14*(1), 221-230.
14. Geeitha, S., & Thangamani, M. (2018). Incorporating EBO-HSIC with SVM for gene selection associated with cervical cancer classification. *Journal of medical systems*, *42*(11), 225.
15. Peerbasha, S., & Surputheen, M. M. (2021). A Predictive Model to identify possible affected Bipolar disorder students using Naive Baye's, Random Forest and SVM machine learning techniques of data mining and Building a Sequential Deep Learning Model using Keras. *International Journal of Computer Science & Network Security*, *21*(5), 267-274.
16. Vinod, H. C., Niranjan, S. K., & Aradhya, V. M. (2014, November). An application of Fourier statistical features in scene text detection. In *2014 International Conference on Contemporary Computing and Informatics (IC3I)* (pp. 1154-1159). IEEE.
17. Thamilarasi, V., & Roselin, R. (2019). Automatic thresholding for segmentation in chest X-ray images based on green channel using mean and standard deviation. *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, *8*(8), 695-699.

 doi:10.20944/preprints202510.0001.v1

18. Inbaraj, R., & Ravi, G. (2021). Multi Model Clustering Segmentation and Intensive Pragmatic Blossoms (Ipb) Classification Method based Medical Image Retrieval System. *Annals of the Romanian Society for Cell Biology*, *25*(3), 7841-7852.
19. Saravanan, V., Upender, T., Ruby, E. K., Deepalakshmi, P., Reddy, D. N., & SN, A. (2024, October). Machine Learning Approaches for Advanced Threat Detection in Cyber Security. In *2024 5th IEEE Global Conference for Advancement in Technology (GCAT)* (pp. 1-6). IEEE.
20. Thangamani, M., & Thangaraj, P. (2010). Integrated Clustering and Feature Selection Scheme for Text Documents. *Journal of Computer Science*, *6*(5), 536.
21. Naveen, I. G., Peerbasha, S., Fallah, M. H., Jebaseeli, S. K., & Das, A. (2024, October). A machine learning approach for wastewater treatment using feedforward neural network and batch normalization. In *2024 First International Conference on Software, Systems and Information Technology (SSITCON)* (pp. 1-5). IEEE.
22. Vinod, H. C., Niranjan, S. K., & Anoop, G. L. (2013). Detection, extraction and segmentation of video text in complex background. *International Journal on Advanced Computer Theory and Engineering*, *5*, 117-123.
23. Asaithambi, A., & Thamilarasi, V. (2023, March). Classification of lung chest X-ray images using deep learning with efficient optimizers. In *2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC)* (pp. 0465-0469). IEEE.
24. Inbaraj, R., & Ravi, G. (2020). Content Based Medical Image Retrieval Using Multilevel Hybrid Clustering Segmentation with Feed Forward Neural Network. *Journal of Computational and Theoretical Nanoscience*, *17*(12), 5550-5562.
25. Reddy, D. N., Venkateswararao, P., Vani, M. S., Pranathi, V., & Patil, A. (2025). HybridPPI: A Hybrid Machine Learning Framework for Protein-Protein Interaction Prediction. *Indonesian Journal of Electrical Engineering and Informatics (IJEEI)*, *13*(2).
26. Gangadhar, C., Chanthirasekaran, K., Chandra, K. R., Sharma, A., Thangamani, M., & Kumar, P. S. (2022). An energy efficient NOMA-based spectrum sharing techniques for cell-free massive MIMO. *International Journal of Engineering Systems Modelling and Simulation*, *13*(4), 284-288.
27. Peerbasha, S., Iqbal, Y. M., Surputheen, M. M., & Raja, A. S. (2023). Diabetes prediction using decision tree, random forest, support vector machine, k-nearest neighbors, logistic regression classifiers. *JOURNAL OF ADVANCED APPLIED SCIENTIFIC RESEARCH*, *5*(4), 42-54.
28. Vinod, H. C., & Niranjan, S. K. (2020). Camera captured document de-warping and de-skewing. *Journal of Computational and Theoretical Nanoscience*, *17*(9-10), 4398-4403.
29. Thamilarasi, V., & Roselin, R. (2021). U-NET: convolution neural network for lung image segmentation and classification in chest X-ray images. *INFOCOMP: Journal of Computer Science*, *20*(1), 101-108.
30. Rao, A. S., Reddy, Y. J., Navya, G., Gurrapu, N., Jeevan, J., Sridhar, M., ... & Anand, D. High-performance sentiment classification of product reviews using GPU (parallel)-optimized ensembled methods.
31. Peerbasha, S., Habelalmateen, M. I., & Saravanan, T. (2025, January). Multimodal Transformer Fusion for Sentiment Analysis using Audio, Text, and Visual Cues. In *2025 International Conference on Intelligent Systems and Computational Networks (ICISCN)* (pp. 1-6). IEEE.
32. Vinod, H. C., & Niranjan, S. K. (2018, August). Binarization and segmentation of Kannada handwritten document images. In *2018 Second International Conference on Green Computing and Internet of Things (ICGCIoT)* (pp. 488-493). IEEE.
33. Thamilarasi, V., Naik, P. K., Sharma, I., Porkodi, V., Sivaram, M., & Lawanyashri, M. (2024, March). Quantum computing-navigating the frontier with Shor's algorithm and quantum cryptography. In *2024 International conference on trends in quantum computing and emerging business technologies* (pp. 1-5). IEEE.
34. Kamatchi, S., Preethi, S., Kumar, K. S., Reddy, D. N., & Karthick, S. (2025, May). Multi-Objective Genetic Algorithm Optimised Convolutional Neural Networks for Improved Pancreatic Cancer Detection. In *2025 3rd International Conference on Data Science and Information System (ICDSIS)* (pp. 1-7). IEEE.
35. Abdul Samad, S. R., Ganesan, P., Al-Kaabi, A. S., Rajasekaran, J., & Basha, P. S. (2024). Automated Detection of Malevolent Domains in Cyberspace Using Natural Language Processing and Machine Learning. *International Journal of Advanced Computer Science & Applications*, *15*(10).
36. Vinod, H. C., & Niranjan, S. K. (2017, November). De-warping of camera captured document images. In *2017 IEEE International Symposium on Consumer Electronics (ISCE)* (pp. 13-18). IEEE.

 doi:10.20944/preprints202510.0001.v1

37. Thamilarasi, V., & Roselin, R. (2019). Survey on Lung Segmentation in Chest X-Ray Images. *The International Journal of Analytical and Experimental Modal Analysis*, 1-9.
38. Nimma, D., Rao, P. L., Ramesh, J. V. N., Dahan, F., Reddy, D. N., Selvakumar, V., ... & Jangir, P. (2025). Reinforcement Learning-Based Integrated Risk Aware Dynamic Treatment Strategy for Consumer-Centric Next-Gen Healthcare. *IEEE Transactions on Consumer Electronics*.
39. Peerbasha, S., Alsalami, Z., Almusawi, M., Sheeba, B., & Malathy, V. (2024, November). An Intelligent Personalized Music Recommendation System Using Content-Based Filtering with Convolutional Recurrent Neural Network. In *2024 International Conference on Integrated Intelligence and Communication Systems (ICIICS)* (pp. 1-5). IEEE.
40. Kakde, S., Pavitha, U. S., Veena, G. N., & Vinod, H. C. (2022). Implementation of A Semi-Automatic Approach to CAN Protocol Testing for Industry 4.0 Applications. *Advances in Industry 4.0: Concepts and Applications*, *5*, 203.
41. Thamilarasi, V., Asaithambi, A., & Roselin, R. (2025). ENHANCED ENSEMBLE SEGMENTATION OF LUNG CHEST X-RAY IMAGES BY DENOISING AUTOENCODER AND CLAHE. *ICTACT Journal on Image & Video Processing*, *15*(3).
42. Madhumathy, P., Saravanakumar, R., Umamaheswari, R., Juliette Albert, A., & Devasenapathy, D. (2024). Optimizing design and manufacturing processes with an effective algorithm using anti-collision enabled robot processor. *International Journal on Interactive Design and Manufacturing (IJIDeM)*, *18*(8), 5469-5477.
43. Boopathy, D., & Balaji, P. (2023). Effect of different plyometric training volume on selected motor fitness components and performance enhancement of soccer players. *Ovidius University Annals, Series Physical Education and Sport/Science, Movement and Health*, *23*(2), 146-154.
44. Raja, M. W., & Nirmala, D. K. (2016). Agile development methods for online training courses web application development. *International Journal of Applied Engineering Research ISSN*, 0973-4562.
45. Vidyabharathi, D., Mohanraj, V., Kumar, J. S., & Suresh, Y. (2023). Achieving generalization of deep learning models in a quick way by adapting T-HTR learning rate scheduler. *Personal and Ubiquitous Computing*, *27*(3), 1335-1353.
46. Niasi, K. S. K., Kannan, E., & Suhail, M. M. (2016). Page-level data extraction approach for web pages using data mining techniques. *International Journal of Computer Science and Information Technologies*, *7*(3), 1091-1096.
47. Thamilarasi, V. A Detection of Weed in Agriculture Using Digital Image Processing. *International Journal of Computational Research and Development, ISSN*, 2456-3137.
48. Sureshkumar, T. (2015). Usage of Electronic Resources Among Science Research Scholars in Tamil Nadu Universities A Study.
49. Arul Selvan, M. (2025). Detection of Chronic Kidney Disease Through Gradient Boosting Algorithm Combined with Feature Selection Techniques for Clinical Applications.
50. Shylaja, B., & Kumar, S. (2018). Traditional versus modern missing data handling techniques: An overview. *International Journal of Pure and Applied Mathematics*, *118*(14), 77-84.
51. Sureshkumar, T., Charanya, J., Kumaresan, T., Rajeshkumar, G., Kumar, P. K., & Anuj, B. (2024, April). Envisioning Educational Success Through Advanced Analytics and Intelligent Performance Prediction. In *2024 10th International Conference on Communication and Signal Processing (ICCSP)* (pp. 1649-1654). IEEE.
52. Niasi, K. S. K., & Kannan, E. Multi Agent Approach for Evolving Data Mining in Parallel and Distributed Systems using Genetic Algorithms and Semantic Ontology.
53. Jaishankar, B., Ashwini, A. M., Vidyabharathi, D., & Raja, L. (2023). A novel epilepsy seizure prediction model using deep learning and classification. *Healthcare analytics*, *4*, 100222.
54. Raja, M. W. (2024). Artificial intelligence-based healthcare data analysis using multi-perceptron neural network (MPNN) based on optimal feature selection. *SN Computer Science*, *5*(8), 1034.
55. Boopathy, D., & Balaji, D. P. Training outcomes of yogic practices and aerobic dance on selected health related physical fitness variables among tamilnadu male artistic gymnasts. *Sports and Fitness*, *28*.
56. Saravana Kumar, R., & Tholkappia Arasu, G. (2017). Rough set theory and fuzzy logic based warehousing of heterogeneous clinical databases. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, *25*(03), 385-408.

 doi:10.20944/preprints202510.0001.v1

57. Boopathy, D. Training Outcomes Of Yogic Practices And Plyometrics On Selected Motor Fitness Among The Men Artistic Gymnasts.
58. Raja, M. W., & Nirmala, K. INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY AN EXTREME PROGRAMMING METHOD FOR E-LEARNING COURSE FOR WEB APPLICATION DEVELOPMENT.
59. Hamed, S., Mesleh, A., & Arabiyyat, A. (2021). Breast cancer detection using machine learning algorithms. *International Journal of Computer Science and Mobile Computing*, *10*(11), 4-11.
60. Boopathy, D., & Balaji, D. P. Research Paper Open Access.
61. Kaladevi, A. C., Saravanakumar, R., Veena, K., Muthukumaran, V., Thillaiarasu, N., & Kumar, S. S. (2022). Data analytics on eco-conditional factors affecting speech recognition rate of modern interaction systems. *Journal of Mobile Multimedia*, *18*(4), 1153-1176.
62. Marimuthu, M., Mohanraj, G., Karthikeyan, D., & Vidyabharathi, D. (2023). RETRACTED: Safeguard confidential web information from malicious browser extension using Encryption and Isolation techniques. Journal of Intelligent & Fuzzy Systems, 45(4), 6145-6160.
63. Banu, S. S., Niasi, K. S. K., & Kannan, E. (2019). Classification Techniques on Twitter Data: A Review. *Asian Journal of Computer Science and Technology*, *8*(S2), 66-69.
64. Sureshkumar, T., & Hussain, A. A. Digital Library Usage of Research in the field of Physical Education and Sports.
65. Boopathy, D., Balaji, D. P., & Dayanandan, K. J. THE TRAINING OUTCOMES OF COMBINED PLYOMETRICS AND YOGIC PRACTICES ON SELECTED MOTOR FITNESS VARIABLES AMONG MALE GYMNASTS.
66. Charanya, J., Sureshkumar, T., Kavitha, V., Nivetha, I., Pradeep, S. D., & Ajay, C. (2024, June). Customer Churn Prediction Analysis for Retention Using Ensemble Learning. In *2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT)* (pp. 1-10). IEEE.
67. Dhanwanth, B., Saravanakumar, R., Tamilselvi, T., & Revathi, K. (2023). A smart remote monitoring system for prenatal care in rural areas. *International Journal on Recent and Innovation Trends in Computing and Communication*, *11*(3), 30-36.
68. Boopathy, D., & PrasannaBalaji, D. EFFECT OF YOGASANAS ON ARM EXPLOSIVE POWER AMONG MALE ARTISTIC GYMNASTS.
69. Lavanya, R., Vidyabharathi, D., Kumar, S. S., Mali, M., Arunkumar, M., Aravinth, S. S., ... & Tesfayohanis, M. (2023). [Retracted] Wearable Sensor-Based Edge Computing Framework for Cardiac Arrhythmia Detection and Acute Stroke Prediction. *Journal of Sensors*, *2023*(1), 3082870.
70. Selvam, P., Faheem, M., Dakshinamurthi, V., Nevgi, A., Bhuvaneswari, R., Deepak, K., & Sundar, J. A. (2024). Batch normalization free rigorous feature flow neural network for grocery product recognition. *IEEE Access*, *12*, 68364-68381.
71. Mubsira, M., & Niasi, K. S. K. (2018). Prediction of Online Products using Recommendation Algorithm.
72. Vidyabharathi, D., & Mohanraj, V. (2023). Hyperparameter Tuning for Deep Neural Networks Based Optimization Algorithm. *Intelligent Automation & Soft Computing*, *36*(3).
73. Lalitha, T., Kumar, R. S., & Hamsaveni, R. (2014). Efficient key management and authentication scheme for wireless sensor networks. *American Journal of Applied Sciences*, *11*(6), 969.
74. Saravanakumar, R., & Nandini, C. (2017). A survey on the concepts and challenges of big data: Beyond the hype. *Advances in Computational Sciences and Technology*, *10*(5), 875-884.
75. Boopathy, D., & Prasanna, B. D. IMPACT OF PLYOMETRIC TRAINING ON SELECTED MOTOR FITNESS VARIABLE AMONG MEN ARTISTIC GYMNASTS.
76. Niasi, K. S. K., & Kannan, E. (2016). Multi Attribute Data Availability Estimation Scheme for Multi Agent Data Mining in Parallel and Distributed System. *International Journal of Applied Engineering Research*, *11*(5), 3404-3408.
77. Marimuthu, M., Vidhya, G., Dhaynithi, J., Mohanraj, G., Basker, N., Theetchenya, S., & Vidyabharathk, D. (2021). Detection of Parkinson's disease using Machine Learning Approach. *Annals of the Romanian Society for Cell Biology*, *25*(5), 2544-2550.

 doi:10.20944/preprints202510.0001.v1

78. Kumar, R. S., & Arasu, G. T. (2015). Modified particle swarm optimization based adaptive fuzzy k-modes clustering for heterogeneous medical databases. *J. Sci. Ind. Res*, *74*(1), 19-28.
79. Shylaja, B., & Kumar, R. S. (2022). Deep learning image inpainting techniques: An overview. *Grenze Int J Eng Technol*, *8*(1), 801.
80. Boopathy, D., Singh, S. S., & PrasannaBalaji, D. EFFECTS OF PLYOMETRIC TRAINING ON SOCCER RELATED PHYSICAL FITNESS VARIABLES OF ANNA UNIVERSITY INTERCOLLEGIATE FEMALE SOCCER PLAYERS. *EMERGING TRENDS OF PHYSICAL EDUCATION AND SPORTS SCIENCE*.
81. Revathy, G., Ramalingam, A., Karunamoorthi, R., & Saravanakumar, R. (2021). Prediction of long cancer severity with computational intelligence in COVID'19 pandemic.