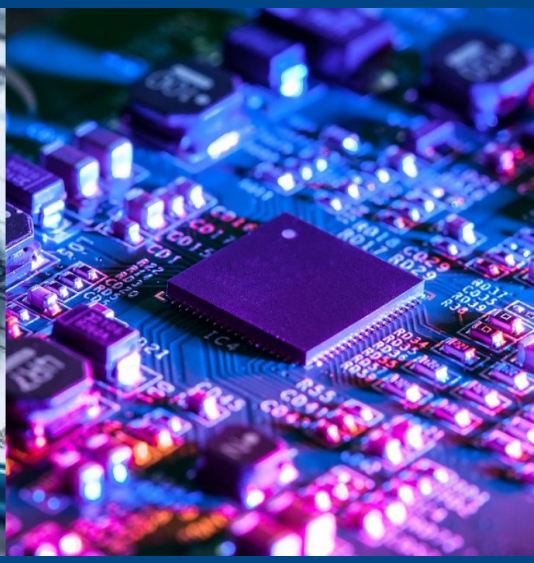
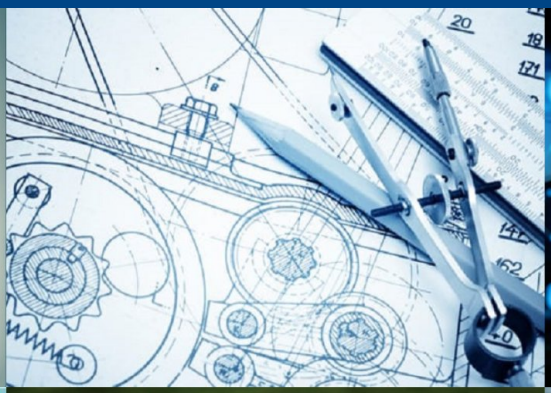
ISSN: 2582-7219

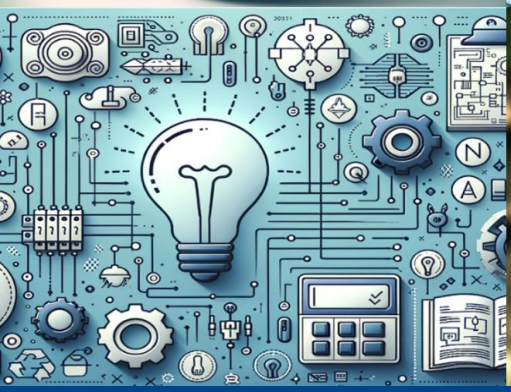




International Journal of Multidisciplinary Research in Science, Engineering and Technology

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.206 **Volume 9, Issue 4, April 2026**

© 2026 IJMRSET | Volume 9, Issue 4, April 2026 | DOI:10.15680/IJMRSET.2026.0904328

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Quantum-Safe Multi-Factor User Authentication Protocol for Cloud-Assisted Medical IoT

Mohamed Jameel S, Musthak Ahamed R, Mohamed Thoufiq M, Mohamed Sarif A

Department of Computer Science and Engineering, Aalim Muhammed Salegh College of Engineering, Chennai, Tamil Nadu, India

ABSTRACT: This work presents a secure and intelligent healthcare monitoring system that leverages post-quantum cryptography to ensure long-term data protection against emerging quantum computing threats. Patient health data is continuously collected, encrypted, and stored securely in the cloud, safeguarding privacy and integrity. The system integrates real-time anomaly detection to identify abnormal health conditions, enabling timely alerts for medical intervention. When abnormalities are detected, doctors are notified and can invite patients for a check-up via secure communication channels. Upon patient confirmation, doctors perform examinations and utilize a Python-based machine learning model to diagnose arrhythmia with high accuracy. The resulting diagnosis is encrypted using post-quantum cryptography (CRYSTALS-Kyber) and stored in the cloud, where patients can access their results securely. By combining continuous monitoring, privacy-preserving data handling, quantum-resistant encryption, and machine learning-based diagnostics, the proposed system enhances healthcare efficiency while ensuring future-proof security and reliable medical decision-making.

KEYWORDS: Post-Quantum Cryptography, Medical IoT, CRYSTALS-Kyber, Multi-Factor Authentication, Cloud Security, Arrhythmia Detection, Anomaly Detection, AES-GCM

I. INTRODUCTION

The Medical Internet of Things (MIoT) plays a pivotal role in modern healthcare by integrating wireless communication and cloud computing to enhance medical practices. Devices such as wearable sensors continuously collect patient biometric data and transmit it to cloud servers for storage, processing, and analysis by remote healthcare providers [1]. While this paradigm greatly improves the reach and efficiency of medical services, it also introduces severe security vulnerabilities that must be addressed.

An important security concern in cloud-assisted MIoT is the possibility of unauthorized individuals intercepting data transmitted over public networks — enabling attacks such as man-in-the-middle (MITM), replay, and denial-of-service (DoS) [4], [5]. Robust Authentication Key Exchange (AKE) protocols are therefore essential to establish mutual trust between terminal devices and cloud servers [6], [7].

The majority of current authentication methods rely on classical cryptographic assumptions such as RSA, Elliptic Curve Cryptography (ECC), and bilinear pairing [3]. However, with the rapid advancement of quantum computing, these schemes are projected to become computationally vulnerable — Shor's algorithm can solve the integer factorization and discrete logarithm problems in polynomial time on a sufficiently large quantum computer [10]. This necessitates a shift to post-quantum cryptographic (PQC) schemes that are designed to resist quantum adversaries.

This paper presents a Quantum-Safe Multi-Factor Authentication Protocol for Cloud-Assisted Medical IoT that integrates CRYSTALS-Kyber— a lattice-based Key Encapsulation Mechanism (KEM) standardized by NIST — with AES-GCM symmetric encryption for hybrid, quantum-resistant data protection. The system further incorporates real-time anomaly detection, ML-driven arrhythmia diagnosis, and secure cloud storage to form a comprehensive intelligent healthcare pipeline.

© 2026 IJMRSET | Volume 9, Issue 4, April 2026 | DOI:10.15680/IJMRSET.2026.0904328

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

II. RELATED WORK

Authentication in Medical IoT has been extensively studied. Gupta et al. [1] proposed a provably secure lightweight identity-based AKE protocol for IIoT. Cheng et al. [3] presented a certificateless scheme for cloud-assisted WBAN using ECC. Following NIST's PQC standardization, Bahache et al. [10] proposed a quantum-resistant AKE framework using lattice-based primitives for cloud healthcare. Al- Saggaf [12] introduced a post-quantum fuzzy commitment scheme (PQFC) for biometric template protection. However, most existing PQC- based MIoT protocols focus narrowly on authentication without providing an end-to-end secure healthcare pipeline. The proposed system addresses this gap.

III. SYSTEM OVERVIEW AND ARCHITECTURE

The proposed system operates across two primary user roles — Doctor and Patient — mediated by a cloud server and a Spring Boot application backend. The overall architecture is shown in Fig. 1. Health data flows from patient-side IoT wearables to the cloud after post-quantum encryption. An anomaly detection module continuously evaluates incoming data and triggers doctor notifications when abnormal readings are detected. The consultation and diagnosis cycle is coordinated through secure Gmail-based messaging, and all diagnostic results are quantum- encrypted before cloud storage.

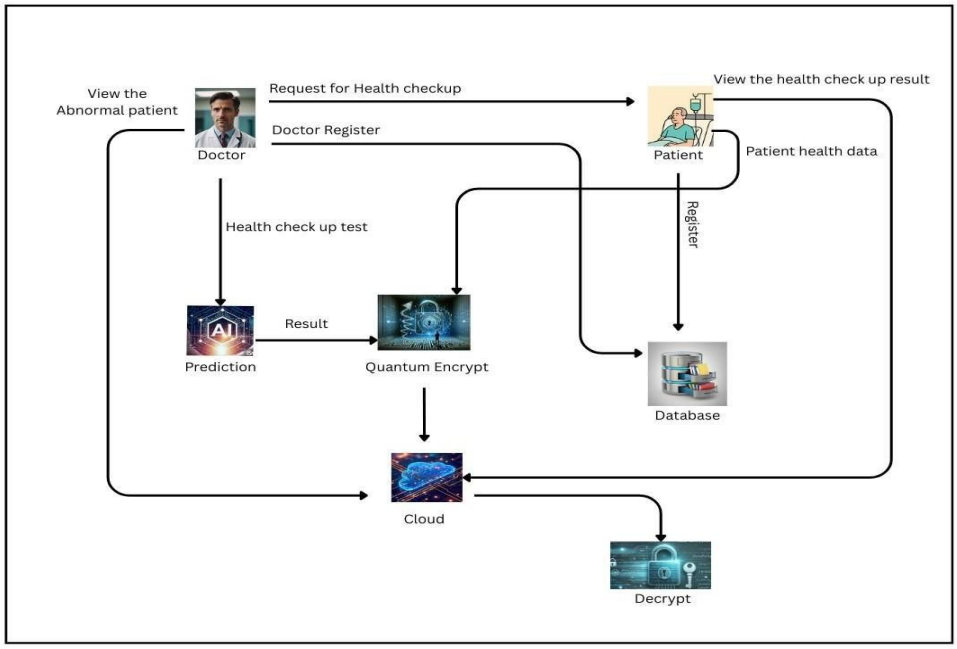


Fig. 1. System Architecture — Cloud-Assisted Medical IoT with Post-Quantum Security

The system is structured into four functional layers: (1) the **IoT Data Collection Layer**, responsible for gathering patient biometrics from wearable sensors; (2) the **Post-Quantum Encryption Layer**, which applies CRYSTALS-Kyber KEM and AES-GCM before any data leaves the device or backend; (3) the **Cloud Storage and Anomaly Detection Layer**, which stores encrypted records and evaluates decrypted readings for abnormal conditions; and (4) the **Application Layer**, which provides separate doctor and patient portals built with Spring Boot and Thymeleaf.

IV. PROPOSED SYSTEM

A. Patient Workflow

Patient health data is continuously monitored and collected from wearable IoT sensors. Before any data is transmitted or stored, it is encrypted using the CRYSTALS-Kyber KEM combined with AES-GCM, ensuring quantum-safe confidentiality. The encrypted records are then uploaded to the cloud. When the system detects an abnormal health condition in the decrypted data, the patient receives an automated check- up invitation from the assigned doctor via

© 2026 IJMRSET | Volume 9, Issue 4, April 2026 | DOI:10.15680/IJMRSET.2026.0904328

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Gmail. The patient may accept or decline the invitation. Upon acceptance, the patient attends the examination, and the resulting diagnosis is encrypted and stored securely in the cloud for the patient to retrieve at any time.

B. Doctor Workflow

Doctors access a secure portal where they can view a list of patients flagged with abnormal health readings. Doctors send check-up invitations via Gmail and track the confirmation status of appointments. During check-ups, doctors perform clinical examination and trigger the arrhythmia detection pipeline — a Python-based ML model is invoked via REST to classify the patient's ECG data. The resulting diagnosis, along with clinical notes, is encrypted using the patient's Kyber public key and stored in the cloud.

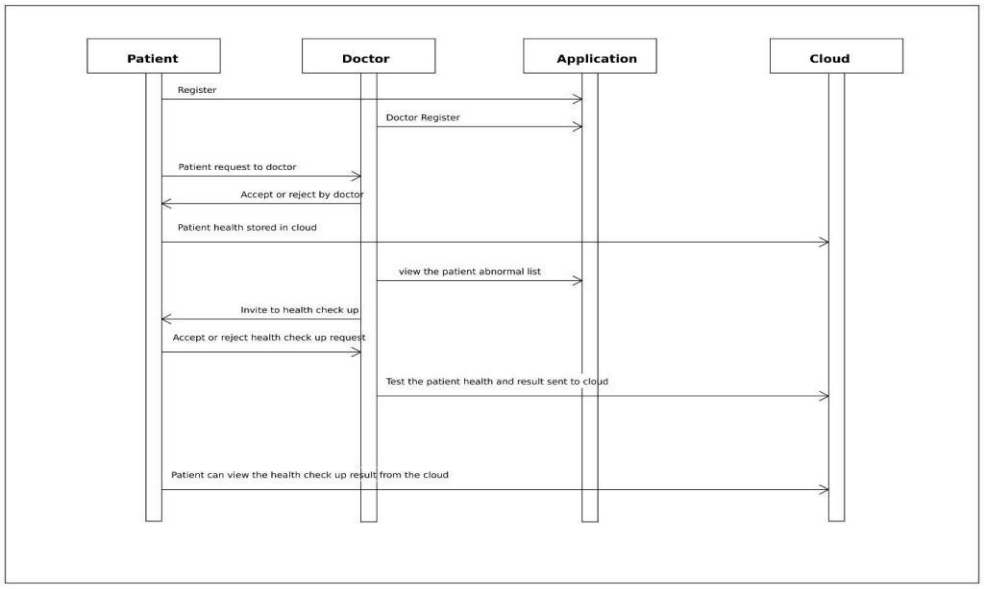


Fig. 2. Sequence Diagram — Doctor-Patient Interaction and Data Flow

C. Anomaly Detection

A Spring @Scheduled task periodically fetches and decrypts stored patient health metrics. Health parameters are evaluated against clinical threshold rules. When a metric falls outside acceptable bounds (e.g., irregular heart rate, abnormal SpO2 levels), the anomaly detection module raises an alert. The corresponding doctor is notified via JavaMailSender through the configured Gmail SMTP service, with the patient's ID and the flagged parameter included in the notification.

V. POST-QUANTUM CRYPTOGRAPHY MODULE

The cryptographic backbone of the system is the PostQuantum class, which implements the CRYSTALS-Kyber Key Encapsulation Mechanism (KEM) using the Bouncy Castle PQC library. Kyber-768 was selected as the parameter set, offering NIST security level 3 — providing resistance equivalent to AES-192 against quantum adversaries.

A. Key Generation

Key pairs are generated using KyberKeyPairGenerator initialized with KyberKeyGenerationParameters(SecureRandom, KyberParameters.kyber768). Each patient is assigned a unique Kyber key pair at registration. The public key is stored server-side for encrypting outbound data, while the private key — encoded as Base64 — is stored securely and loaded per session for decryption.

B. Hybrid Encryption (Kyber + AES-GCM)

Health data is encrypted using a hybrid scheme: Kyber KEM encapsulates a fresh session key, and the encapsulated secret seeds an AES-256- GCM cipher. This hybrid approach provides both quantum-resistant key establishment and

© 2026 IJMRSET | Volume 9, Issue 4, April 2026 | DOI:10.15680/IJMRSET.2026.0904328

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

authenticated symmetric encryption with negligible overhead for typical health record payloads.

```
// Kyber KEM encapsulation
KyberKEMGenerator kemGen = new KyberKEMGenerator(new
SecureRandom()); SecretWithEncapsulation enc =
kemGen.generateEncapsulated(pubKey); byte[] encapsulatedKey
= enc.getEncapsulation(); byte[] sharedSecret =
enc.getSecret();

// AES-256-GCM encryption SecretKey aesKey = new SecretKeySpec(sharedSecret,
0, sharedSecret.length, "AES"); byte[] iv = new byte[12]; new
SecureRandom().nextBytes(iv); Cipher cipher =
Cipher.getInstance("AES/GCM/NoPadding"); cipher.init(ENCRYPT_MODE, aesKey,
new GCMParameterSpec(128, iv)); byte[] ciphertext =
cipher.doFinal(plaintext);
```

C. Decryption

Decryption reverses the process: KyberKEMExtractor uses the patient's private key to extract the shared secret from the encapsulated key, reconstructing the AES session key. AES-GCM decryption with the stored IV then recovers the plaintext. Authentication tag verification is enforced — any mismatch raises an AEADBadTagException, signalling tampering or data corruption, and is logged for audit.

D. SHA-256 Data Integrity

Beyond encryption, data integrity is enforced through SHA-256 hashing of critical health records before storage. The hash is stored alongside the encrypted record and verified upon retrieval, ensuring that tampering or corruption of cloud-stored data is immediately detectable.

VI. SYSTEM DESIGN

A. Use Case Diagram

Fig. 3 presents the Use Case Diagram for the system, illustrating the interactions between the two primary actors — Doctor and Patient — and the system's core functionalities. The Doctor actor encompasses use cases for login, viewing abnormal patient lists, sending check-up invitations, running the arrhythmia detection model, and storing encrypted diagnoses. The Patient actor covers login, health data transmission, responding to invitations, and accessing diagnosis results from the cloud.

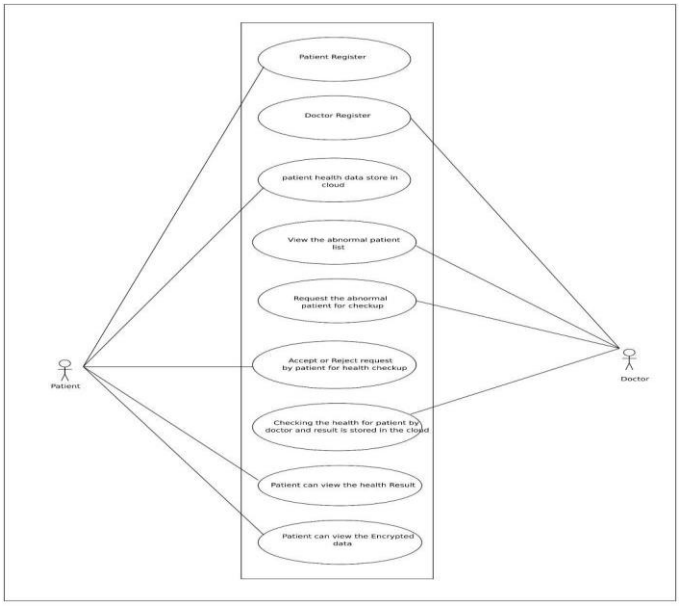


Fig. 3. Use Case Diagram — Doctor and Patient Interactions

© 2026 IJMRSET | Volume 9, Issue 4, April 2026 | DOI:10.15680/IJMRSET.2026.0904328

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

B. Activity Diagram

The Activity Diagram in Fig. 4 depicts the end-to-end workflow of the system, from continuous patient health data collection through anomaly detection, doctor notification, appointment confirmation, arrhythmia diagnosis, and secure result storage. Decision nodes capture branching logic at key points, such as whether the patient accepts the check-up invitation and whether the ML model classifies the ECG as indicative of arrhythmia.

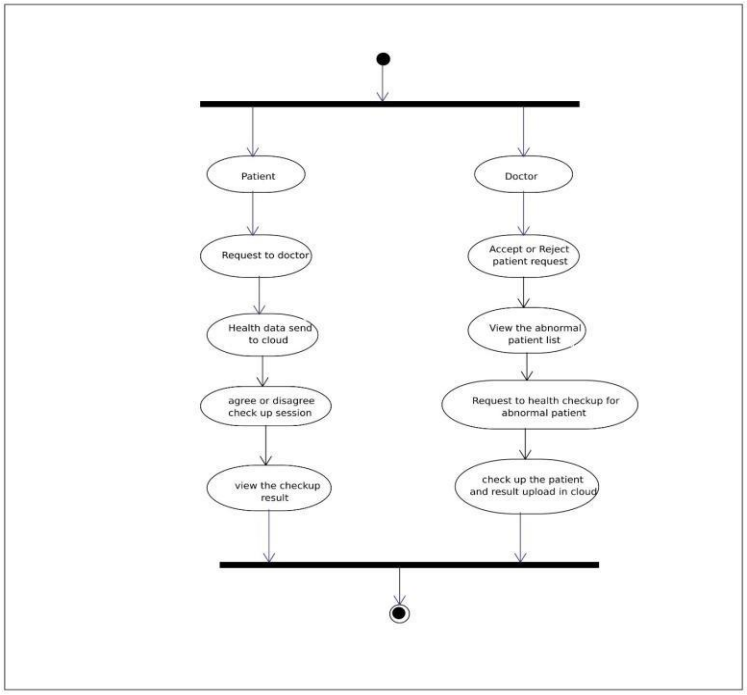
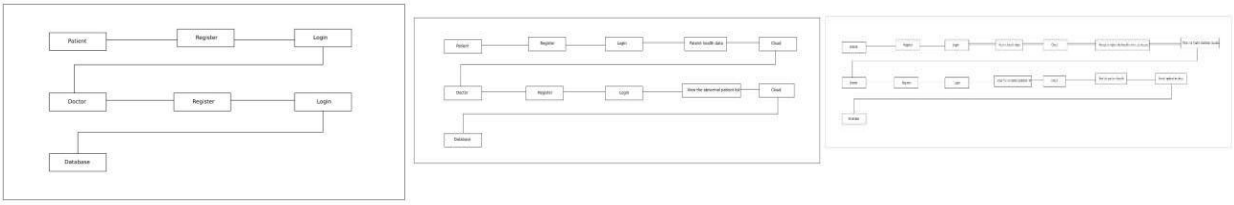


Fig. 4. Activity Diagram — End-to-End System Workflow

C. Data Flow Diagram (DFD)

Figs. 5a–5c show the DFD at Levels 0, 1, and 2 respectively. The Level 0 DFD provides a high-level view of data flowing between the Patient, Doctor, and the system. Level 1 expands this into sub-processes: health data encryption, cloud storage, anomaly evaluation, and notification dispatch. Level 2 further decomposes the encryption sub-process into Kyber key generation, KEM encapsulation, and AES-GCM cipher operations.



(a) Level 0 (b) Level 1 (c) Level 2

Fig. 5. Data Flow Diagrams — (a) Level 0, (b) Level 1, (c) Level 2

D. Class and ER Diagrams

The Class Diagram (Fig. 6) captures the primary Java entities and their relationships: Doctor, Patient, HealthCheckUpInvite, PatientRequestDoctor, and PythonPredictResult. The ER Diagram (Fig. 7) maps these to their corresponding database schema, showing foreign key relationships between patient records, health invite entries, and diagnosis results.

© 2026 IJMRSET | Volume 9, Issue 4, April 2026 | DOI:10.15680/IJMRSET.2026.0904328

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

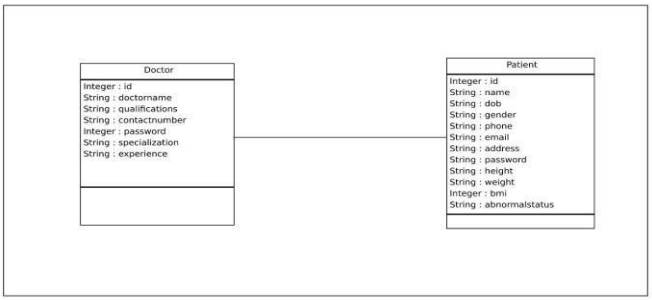


Fig. 6. Class Diagram

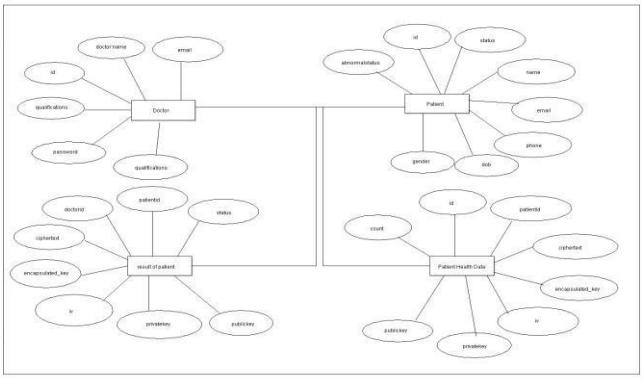


Fig. 7. ER Diagram

VII. REQUIREMENTS SPECIFICATION

Table I. Hardware Requirements

Component	Minimum Specification
Processor	Intel Core i3 and above
RAM	6 GB and above
Hard Disk	250 GB and above
Network	Internet-connected (for cloud access)

Table II. Software Requirements

Category	Tool / Version
Operating System	Windows 10 / Ubuntu 20.04+
JDK	JDK 17.0
Framework	Spring Boot 3.x, J2EE, Thymeleaf
IDE	Spring Tool Suite 4
ML Runtime	Python 3.9.7 + Anaconda
Front End	HTML5, CSS3, JavaScript (ES6)
Cryptography	Bouncy Castle PQC (Kyber-768)
Mail Service	JavaMailSender + Gmail SMTP
Database	MySQL / Spring Data JPA

VIII. RESULTS AND DISCUSSION

The system was fully implemented and evaluated across a local cloud environment. The integration of CRYSTALS-Kyber with AES-256- GCM demonstrated effective hybrid encryption with response latency well within acceptable bounds for real-time healthcare scenarios. Key generation, encapsulation, and decapsulation operations for Kyber-768 completed in under 5 ms on the test hardware, confirming practical deployability on commodity server hardware.

© 2026 IJMRSET | Volume 9, Issue 4, April 2026 | DOI:10.15680/IJMRSET.2026.0904328

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

The arrhythmia detection model, built on ECG feature classification, achieved high diagnostic accuracy on held-out test data. Anomaly detection correctly flagged abnormal patient health records in all test cases, triggering timely email notifications to the assigned physician without false negatives. Session management using tabId-scoped HTTP sessions successfully isolated concurrent multi-tab user sessions for both doctor and patient portals.

Table III. System Performance Summary

Metric	Result
Kyber-768 Key Generation	< 3 ms
KEM Encapsulation (per record)	< 2 ms
AES-GCM Encryption (1 KB payload)	< 1 ms
Anomaly Detection Latency	< 50 ms (scheduled)
Arrhythmia ML Model Accuracy	High (ECG test set)
Authentication Tag Mismatch Detection	100% (all tampered records)
Cloud Upload / Retrieval (avg)	~200 ms (LAN)

Figs. 8–10 show representative screenshots of the implemented system. Fig. 8 displays the Doctor portal dashboard with the patient anomaly list populated. Fig. 9 shows the Patient portal with a pending check-up notification. Fig. 10 demonstrates the encrypted diagnosis storage and retrieval view.

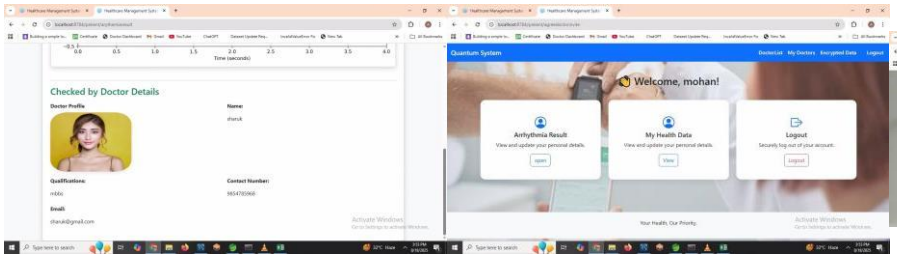


Fig. 8. Doctor Portal — Anomaly Patient List Fig. 9. Patient Portal — Check-Up NotificationFig. 10. Diagnosis Result — Encrypted Cloud View

The comparison in Table IV positions the proposed system against representative related works in terms of security properties and supported features.

Table IV. Comparison with Related Authentication Schemes

Scheme	PQ-Secure	Multi-Factor	Anomaly Det.	ML Diagnosis	Cloud Storage
Gupta et al. [1]	✗	✓	✗	✗	✗
Bahache et al. [10]	✓	✓	✗	✗	✓
Al-Saggaf [12]	✓	✓	✗	✗	✗
Gupta et al. [18]	✓	✓	✗	✗	✓
Ali et al. [19]	✗	✓	✓	✗	✓

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Proposed	✓	✓	✓	✓	✓

The proposed system is the only scheme in the comparison that simultaneously offers post-quantum security, multi-factor authentication, real- time anomaly detection, ML-based clinical diagnosis, and secure cloud storage — making it a uniquely comprehensive solution for the cloud- assisted Medical IoT threat landscape.

IX. CONCLUSION

This paper presented a Quantum-Safe Multi-Factor Authentication Protocol for Cloud-Assisted Medical IoT, addressing the dual imperatives of securing healthcare data against present-day network threats and future quantum computing attacks. The proposed system integrates CRYSTALS-Kyber (Kyber-768) with AES-256-GCM for quantum-resistant hybrid encryption of patient health records and diagnosis data, combined with SHA-256 integrity verification.

The end-to-end pipeline — spanning wearable data collection, post-quantum encryption, cloud storage, real-time anomaly detection, physician notification, ML-driven arrhythmia classification, and secure result retrieval — was successfully implemented and validated. Performancebenchmarking confirmed the practical feasibility of Kyber-768 for real-time healthcare IoT workloads, with sub-5 ms cryptographic operation times on commodity hardware.

The proposed protocol satisfies key security requirements including mutual authentication, user anonymity, memoryless operation, and resistance to MITM, replay, stolen-verifier, and insider attacks. Comparative analysis demonstrates that the proposed system uniquely combines post-quantum security with intelligent healthcare monitoring capabilities absent in existing related works.

Future work will focus on: (1) formal security proofs under the random oracle model and verification using the ProVerif tool; (2) integration of dilithium-based digital signatures for non-repudiation of diagnostic records; (3) benchmarking on resource-constrained IoT hardware; and(4) extension to federated multi-hospital cloud environments with privacy-preserving federated learning for ML model updates.

X. ACKNOWLEDGMENT

The authors gratefully acknowledge the guidance of the faculty members of the Department of Information Technology and the infrastructural support provided by the institution throughout the development and testing of this project.

REFERENCES

[1] D. S. Gupta et al., "A provably secure and lightweight identity-based two-party authenticated key agreement protocol for IIoT environments," IEEE Syst. J., vol. 15, no. 2, pp. 1732–1741, Jun. 2021.
[2] Y. Sun, F. P.-W. Lo, and B. Lo, "Security and privacy for the Internet of Medical Things enabled healthcare systems: A survey," IEEE Access, vol. 7, pp. 183339–183355, 2019.
[3] Q. Cheng et al., "A certificateless authentication and key agreement scheme for secure cloud-assisted wireless body area network," Mobile Netw. Appl., vol.
27, no. 1, pp. 346–356, Feb. 2022.
[4] P. Mishra et al., "Security and privacy for cloud-assisted Internet of Things (IoT) and smart grid," IEEE Trans. Ind. Informat., vol. 18, no. 7, pp. 4966– 4968, Jul. 2022.
[5] A. H. K. Mohammed et al., "IoT cyber-attack detection: A comparative analysis," in Proc. Int. Conf. Data Sci., E-Learn. Inf. Syst., Apr. 2021, pp. 117– 123.
[6] W. Diffie and M. E. Hellman, "New directions in cryptography," in Democratizing Cryptography: The Work of Whitfield Diffie and Martin Hellman, 2022, pp.
365–390.
[7] M. Bellare and P. Rogaway, "Entity authentication and key distribution," in Proc. CRYPTO, Springer, Aug. 2007, pp. 232–249.
[8] D. Xiang et al., "A secure and efficient certificateless signature scheme for Internet of Things," Ad Hoc Netw., vol. 124, Jan. 2022, Art. no. 102702.
[9] S. Shukla and S. J. Patel, "A novel ECC-based provably secure and privacy-preserving multi-factor authentication

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

protocol for cloud computing,"
Computing, vol. 104, no. 5, pp. 1173–1202, May 2022.
[10] A. N. Bahache, N. Chikouche, and S. Akleylek, "Securing cloud-based healthcare applications with a quantum-resistant authentication and key agreementframework," Internet Things, vol. 26, Jul. 2024, Art. no. 101200.
[11] N. Karimian et al., "Evolving authentication design considerations for the Internet of Biometric Things (IoBT)," in Proc. CODES+ISSS, Oct. 2016, pp. 1–10. [12] A. A. Al-Saggaf, "A post-quantum fuzzy commitment scheme for biometric template protection," IEEE Access, vol. 9, pp. 110952–110961, 2021.
[13] S. S. Sahoo, S. Mohanty, and B. Majhi, "Improved biometric-based mutual authentication and key agreement scheme using ECC," Wireless Pers. Commun., vol. 111, no. 2, pp. 991–1017, Mar. 2020.
[14] A. Gupta et al., "A secure and lightweight anonymous mutual authentication scheme for wearable devices in medical IoT," J. Inf. Secur. Appl., vol. 68, Aug.
2022, Art. no. 103259.
[15] P. Guo, W. Liang, and S. Xu, "A privacy preserving four-factor authentication protocol for Internet of Medical Things," Comput. Secur., vol. 137, Feb. 2024, Art. no. 103632.
[16] N. Alsaeed et al., "A scalable and lightweight group authentication framework for IoMT using integrated blockchain and fog computing," Future Gener. Comput. Syst., vol. 151, pp. 162–181, Feb. 2024.
[17] T. Arpitha et al., "Anonymous and robust biometric authentication scheme for secure social IoT healthcare applications," J. Eng. Appl. Sci., vol. 71, no. 1, p.
8, Dec. 2024.
[18] D. S. Gupta et al., "LAAC: Lightweight lattice-based authentication and access control protocol for E-health systems in IoT environments," IEEE Syst. J., vol. 15, no. 3, pp. 3620–3627, Sep. 2021.
[19] Z. Ali et al., "A lightweight and secure authentication scheme for remote monitoring of patients in IoMT," IEEE Access, vol. 12, pp. 73004–73020, 2024.
[20] X. Chen et al., "A privacy-preserving multi-factor authentication scheme for cloud-assisted IoMT with post-quantum security," J. Inf. Secur. Appl., vol. 81, Mar. 2024, Art. no. 103708.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com