International Journal of Computational and Experimental Science and ENgineering
(IJCESEN)

Vol. 11-No.4 (2025) pp. 9485-9495
http://www.ijcesen.com

ISSN: 2149-9144

Research Article

Secure E-Healthcare System Based on Lightweight Key Management and Proof of Authority Blockchain

Abdelatif Djenaoui[1*], Hamza Reffad[2], Adel Altı[3]

[1]Faculty of Sciences, Computer Science Department, LRSD, University Ferhat Abbas Sétif 1, Sétif, 19000, Algeria
* **Corresponding Author Email:** abdelatif.djenaoui@univ-setif.dz - **ORCID:** 0009-0008-6272-4860

[1]Faculty of Sciences, Computer Science Department, LRSD, University Ferhat Abbas Sétif 1, Sétif, 19000, Algeria
Email: reffad.hamza@univ-setif.dz - **ORCID:** 0000-0003-4079-0249

[3]Faculty of Sciences, Computer Science Department, LRSD, University Ferhat Abbas Sétif 1, Sétif, 19000, Algeria
Email: a.alti@qu.edu.sa - **ORCID:** 0000-0001-8348-1679

Article Info:

DOI: 10.22399/ijcesen.4140
Received: 01 October 2025
Revised: 20 November 2025
Accepted: 30 November 2025

Keywords

Permissioned Blockchain
Proof-of-Authority (PoA)
Fog Computing
Privacy Preservation
Key Management
Healthcare Data Security

Abstract:

As Internet of Medical Things (IoMT) continues to evolve rapidly, ensuring secure health data exchange among diverse healthcare actors becomes essential, not only to protect sensitive healthcare data but also to safeguard user privacy and prevent unauthorized access. With IoMT transmitting sensitive data from home environments to specialist hospitals, the need for strong yet efficient protection has never been more urgent. IoMT healthcare environments require cryptographic algorithms to be robust and lightweight enough to run effectively on low-end devices. Traditional encryption techniques incur vulnerable centralized key management and typically significant delays and computational overheads, making them unsuitable for low-power IoMT devices designed for these constrained environments. In this paper, an innovative lightweight key management and encryption method is proposed. The proposed system employs Post-Quantum Ciphertext-Policy Attribute-Based Encryption (Q-PA-ABE) to generate a shared key and ensure fine-grained one-to-many access control. A permissioned blockchain with Proof-of-Authority (PoA) consensus is decentralized Key-Generation Authorities (KGCs) management and auditability, and fog computing is low-latency data relaying to secure data transfer after setting up the keys. A Python-based prototype was implemented to enable real-time key exchange and secure data transmission. Experiments show lowest gas consumption and archives efficiency of 1.16% and removes single points of failure, while ensuring auditable data logs, demonstrating secure and efficient healthcare data services for IoMT.

1. Introduction

Currently, the Internet of Medical Things (IoMT) is transforming smart healthcare by introducing automated and intelligent services such as continuous patient monitoring, smart control systems, and advanced medical technologies [**1**]. Through real-time data sensing and remote diagnostics, IoMT continues to expand the digital scope of healthcare, improving comfort, efficiency, and overall system performance [**2**]. However, the highly interconnected nature of IoMT ecosystems also introduces a serious and increasing cybersecurity vulnerability [**3**]. As trillions of devices connect to Internet, many constrained by limited battery life and processing power, the risk of exploitation rises exponentially [**4**]. Among the most critical security threats are man-in-the-middle attacks, replay attacks, and denial-of-service attacks, which pose significant risks to system integrity and service availability [**5**]. These types of exploitation in mission-critical IoMT deployments could compromise sensitive medical records, interrupt vital services, and even lead to physical harm to patients [**6**]. While conventional cryptographic schemes are generally reliable, they often require high computational resources and memory overhead, making them impractical for widespread deployment on low-power IoMT devices [**7**]. The growing divide between robust cryptographic solutions and the constrained nature of typical IoT hardware has created a pressing need for tailored, lightweight security protocols.

The integration of IoMT and cloud computing into healthcare has also produced vast sensitive datasets ranging from Electronic Health Records (EHRs) and medical imaging to continuous sensor-based monitoring streams. These datasets demand secure, efficient, and privacy-preserving sharing mechanisms. Traditional cloud-based EHR systems suffer from centralization risks, including semi-trusted providers, the single point of failure in key management, and exposure to both internal and external threats to data confidentiality [**8**]. For instance, conventional CP-ABE schemes rely on a centralized Key Generation Center (KGC) to issue decryption keys. If the KGC is ever compromised or fails, the entire protection framework collapses [**9**]. Moreover, cloud-only solutions incur high latency and bandwidth bottlenecks, limiting responsiveness for time-sensitive health monitoring and emergency scenarios [**10**] [**11**].

The present research introduces a decentralized IoMT-healthcare model that addresses the limitations of centralized key management by offering a lightweight and efficient cryptographic framework specifically designed for IoMT environments. This model enables secure communication between a mobile device acting as the user interface and a fog-based remote diagnostic service acting as the endpoint, thereby representing a practical and relatable use case of a remote smart health diagnostic system. The proposed solution is built on a permissioned blockchain with Proof-of-Authority (PoA) consensus, operated by trusted validators such as hospital-based fog servers. These fog nodes act as data relays for IoT health data sensing devices and as blockchain participants, ensuring real-time responsiveness and tamper-resistant record-keeping. To achieve efficient key management and forward secrecy, the model employs a Ciphertext-Policy Attribute-Based Encryption (CP-ABE) scheme with Elliptic Curve Diffie-Hellman (ECDH) key exchange protocol. This mechanism ensures that even if previous communication is intercepted, it cannot be decrypted later, thereby safeguarding long-term confidentiality. This key exchange is complemented using the Kyber algorithm, a post-quantum cryptographic scheme that provides resilience against quantum-enabled attacks.

The contributions of this work are summarized as follows:

- A consortium blockchain that combines blockchain technology with trusted fog computing to enforce PoA consensus and distribute attribute authorities without a central KGC, and stores transactions for attribute registration, data access logs, and key-related smart contract issuance.
- Enhanced confidentiality through a lightweight Q-CP-ABE with Elliptic Curve Diffie-Hellman (ECDH) key exchange for forward secrecy, complemented by the Kyber scheme to quantum-safe, future-proof communication.
- A real-world deployment scenario where doctors can monitor patient health directly from smartphones. The system runs smoothly on mobile devices, is lightweight for accessibility, and is hosted on fog and cloud platforms, making it scalable and accessible to users in remote locations.

The rest of the paper is organized as follows. Section 2 reviews related work on encryption algorithms and modern blockchain-based IoT security systems. Section 3 presents a lightweight, dynamic, and secure design. Section 4 presents and analyzes security and performance results. Section 5 concludes the work and outlines future research directions.

2. Related Work

2.1 Lightweight Encryption Schemes in e-healthcare Systems

Traditional cryptographic protocols like RSA, AES, and Diffie-Hellman have been very popular in protecting digital communication systems [**12**]. Although these algorithms provide robust security assurances, they usually depend on much processing power, therefore making them not ideal for IoMT devices with limited resources. In response to these limitations, lightweight encryption techniques such as SPECK and PRESENT have been developed. These ciphers are designed to be secure enough, use little computer processor and memory [**13**]. Among them, SPECK is considered a strong candidate for secure IoMT communication, as it supports authenticated encryption with fast and efficient performance on constrained devices. In parallel, elliptic-curve cryptography has gained prominence in IoT environments. Elliptic Curve Diffie–Hellman (ECDH) key exchange, in particular, offers a favorable balance between strong security and low computational overhead [**14**]. Compared to RSA, ECDH has smaller key sizes with equal security level, thereby having lower computational and bandwidth demands. For data confidentiality and fine-grained access control, CP-ABE schemes are often employed in IoMT systems [**15**]. CP-ABE enables only authorized maintain correct attribute keys may decrypt data under an access policy. It has been widely applied in healthcare IoT for fine-grained control. For instance, Zhao *et al.* integrate blockchain with verifiable CP-ABE to secure EHRs [**16**]. However, ABE approaches rely on a centralized Key Generation Center (KGC), which introduces a single point of trust and potential vulnerability [**10**]. Recent research seeks to overcome this limitation by decentralizing or removing the KGC. Cai *et al.* [**11**] propose a *registered ABE* scheme where users generate their own keys and register attributes with a transparent curator, while a blockchain ledger provides audits for key registrations [**9**]. Their approach ensures key issuance is publicly verifiable and no master secret is held by one entity. Similarly, Guo *et al.* design a *pairing-free* CP-ABE scheme for IoT using only elliptic-curve scalar multiplication [**17**], supporting multi-authority decryption and outsourced computation. Such approaches significantly reduce cryptographic overhead for constrained IoT devices. Despite these advancements, many attack vectors, including replay attacks, brute force intrusions, and man-in-the-middle (MITM) attacks, still threaten IoMT systems. IoMT systems remain vulnerable to a variety of attack vectors, including replay attacks, brute-force intrusions, and man-in-the-middle (MITM) attacks. To this end, lightweight cryptographic solutions must not only minimize resource consumption but also provide resilience against these threats. Contemporary IoT security frameworks increasingly employ nonce-based encryption, mutual authentication, and quantum-secure mechanisms to ensure long-term robustness in healthcare environments.

2.2 Blockchain to Secure e-Healthcare Systems

Reffad *et al.* [**18**] proposed a secure distributed mobile–fog–cloud framework that integrates Diffie–Hellman, RSA, and blockchain to ensure the privacy of documents and health data stored in the cloud. The approach leverages smart contracts to strengthen the security and trust of healthcare applications. Wu *et al.* [**19**] proposed SmartCheck, a blockchain-based smart contract solution for healthcare applications. SmartCheck analyses and flags vulnerabilities in smart contracts, thereby identifying potential threats. In addition, smart contracts are leveraged to automate supply chain management (SCM) operations, with transactions validated using the Proof-of-Work (PoW) consensus mechanism. Mallick *et al.* [**20**] presented a hybrid blockchain-IoT-based fog solution for monitoring attacks targeting mobile and wearable devices. Their approach employs fog nodes in IoMT environments to reduce bandwidth usage and avoid dependence on remote cloud servers. In contrast, decentralized storage systems like IPFS, while useful for large-scale archives, are not optimized for continuous streaming. Prior studies highlight their limitations in real-time data access and emergency scenarios [**21**]. For this reason, fog/edge layers are better suited for health data relay and preliminary processing in our proposed architecture. Xie *et al.* [**22**] presented a blockchain-based approach to enhance the safety of consumer devices in e-healthcare systems. Their findings show that PoA offers low latency and high throughput in real-time monitoring applications. Building on these insights, our proposed work adopts a permissioned blockchain with PoA, which is well-suited for healthcare consortia. In this model, a predefined set of trusted validators, such as hospitals acting as fog nodes, which are responsible for block validation, ensuring both efficiency and predictable consensus. Moulahi *et al.* [**23**] combined blockchain with Federated Learning (FL) to improve security and preserve data privacy through decentralized model training without revealing raw data. Similarly, Alsayegh *et al.* [24] developed an asymmetric searchable encryption scheme with proxy re-encryption based on patients' public keys, demonstrating that record length and key size significantly influence computational and communication overhead.

3. Quantum-Secure PoA Blockchain with CP-ABE for Healthcare Systems

We propose Q-PoA–CP-ABE Fog Chain, a Mobile–Fog–Cloud architecture that integrates Ciphertext-Policy Attribute-Based Encryption (CP-ABE), Proof-of-Authority (PoA) blockchain consensus, and fog-enabled low-latency relaying with post-quantum cryptography (PQC) for enhanced resilience against quantum-enabled adversaries. The proposed system ensures fine-grained access control, decentralized trust, auditable logging, and long-term quantum-safe protection of sensitive healthcare data.

3.1 System Design Overview

Fig.1 illustrates the pivotal layers of our approach to secure e-health information systems. We opted for IoT perception, fog computing, blockchain, and Cloud layers. These layers are detailed as follows:

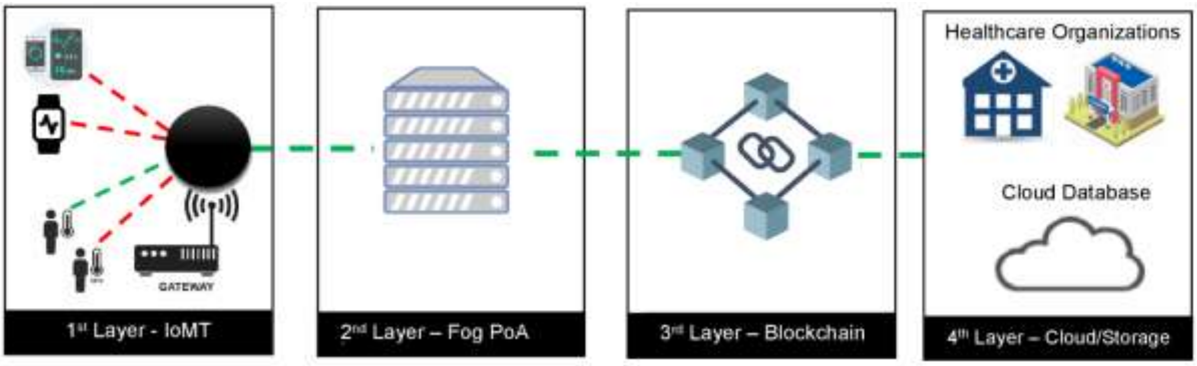

Figure 1. *The proposed approach to secure e-healthcare system.*

1. **IoMT/Perception Layer**

- **IoT Devices (Sensors):** Wearable medical sensors that continuously generate patient data (e.g., ECG, heart rate, or vital signs). These devices are resource-constrained but support lightweight encryption and communicate with nearby fog nodes via Bluetooth, Wi-Fi, or similar protocols. Fog nodes maintain reliable interconnections for blockchain consensus and provide links to cloud storage for backup.
- **Data Owners (Patients):** Patients or authorized entities that manage the IoT devices. They ensure that sensed data is encrypted under Q-CP-ABE policies, which define access based on the attributes of intended recipients (e.g., role, department, or specialization).

2. **Fog PoA Layer**

- **Fog Nodes:** Edge servers or gateways (e.g., hospital servers) that connect to IoT devices. Fog nodes perform local aggregation, encryption assistance, provide short-term storage, and act as blockchain validators with PoA consensus. The nodes are semi-trusted, while they may be curious. Cryptographic mechanisms and a continuous blockchain constrain their behavior.
- **Local Enforcement:** Fog nodes enforce attribute-based policies close to the data source, reducing latency and ensuring timely responses. Cryptographic controls and full blockchain auditability constrain their potential curiosity. Although they are semi-trusted, their potential curiosity is mitigated through pairing-free Q-CP-ABE encryption and full on-chain auditability, ensuring both confidentiality and accountability.

3. **Blockchain Layer**

- **Blockchain Network (Validators):** A permissioned blockchain composed of selected fog nodes (and other hospital IT nodes) running under a PoA consensus. This blockchain ledger stores transactions such as attribute registration, data access logs and smart contracts governing key issuance.
- **Smart Contracts:** Deployed on the blockchain to automate enforcement of attribute-based policies, manage secure key distribution, and record access operations. The smart contracts guarantee immutable and auditable records, strengthened by the integration of post-quantum cryptography (PQC) mechanisms for long-term security against quantum adversaries.

4. **Cloud/Storage Layer**

- **Data Users (Healthcare Providers):** Authorized doctors, nurses, or medical applications equipped with defined attribute sets (e.g., role, department). They hold PQC-hardened ABE decryption keys, allowing secure and fine-grained access to patient data.
- **Cloud Servers:** Provide scalable, long-term encrypted data storage while interoperating with the fog and blockchain layers to enforce CP-ABE policies and ensure secure data retrieval.

3.2 Threat and Trust Models

Trust Model. There is no fully trusted central authority. Instead, trust is decentralized and distributed among fog nodes, which collectively maintain the permissioned blockchain using PoA consensus. We assume that a threshold subset of these nodes behaves honestly as an assumption suitable for a consortium-based healthcare environment. Attribute assignment is governed by a multi-authority ABE (MA-ABE) model: independent authorities (or smart contracts) manage separate attribute domains (e.g., roles, departments, medical specialties). Attribute keys are generated through the combination of contributions from these authorities, preventing any single party from holding all keys or secrets [**10**]. In practice, fog nodes can implement these authorities, decentralizing trust.

Threat Model. We assume an adversary (A) who may attempt the following:

- **Passive attacks:** Dropping on IoT–fog or fog–cloud communications or monitoring blockchain traffic.
- **Active attacks:** Launching man-in-the-middle attacks, replaying stale messages, or altering transmitted data.
- **Compromise of endpoints:** Trying to take control of IoT devices (resource-constrained and vulnerable) or fog nodes (semi-trusted but critical for validation).
- **Validator collusion:** A subset of PoA validators may collude to bias consensus or delay block generation
- **User collusion: Malicious users with disjoint attribute sets may attempt to combine keys to gain unauthorized access.** The blockchain itself is assumed secure under standard consensus assumptions (authorities do not maliciously produce blocks beyond protocol rules).

3.3 Operating principle of Q-PoA–CP-ABE

The proposed framework secures medical data in IoMT environments through two main processes.

- Secure data collection and registration that ensures that patient data generated by IoT devices is encrypted under attribute-based policies and immutably registered on a permissioned blockchain via fog nodes acting as PoA validators.
- Secure data access and retrieval, enabling authorized healthcare providers to request and obtain encrypted records, with access strictly governed by blockchain-logged policies and cryptographic mechanisms.

3.3.1 Process of Secure Data Collection and Registration

As shown in **Fig. 2**, the health data (i.e., blood pressure, temperature, patient location, ECG, etc.) and transactions are generated by the sensors and medical IoT devices ①. A patient defines in real-time a fine-grained policy such as *Role = Cardiologist ∧ Dept = HeartClinic* ②. Next, the mobile device encrypts the data using Q-CP-ABE based on elliptic curve operations ③, before uploading the ciphertext (CT) to the nearest fog node ④. The fog node stores the CT and generates its hash (hCT) ⑤, then builds metadata $M = \{timestamp, ownerID, policyCommit, hCT\}$ ⑥**.** This metadata is submitted as a blockchain transaction to PoA validators ⑦. The blockchain layer executes the PoA consensus protocol to validate the transaction ⑧ and appends it immutably to the ledger⑨. Afterwards, the fog node ⑩ receives the block receipt for confirmation. Optionally, multi-authority ABE key issuance events are triggered and logged on-chain whenever new authorized users (e.g., doctors, specialists) join the system ⑪.

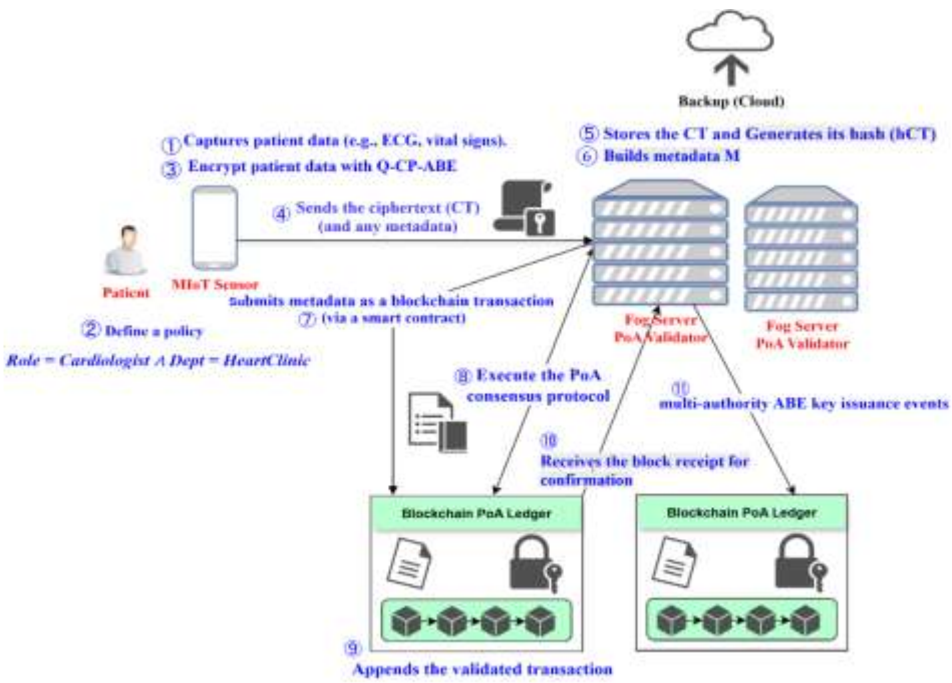

Figure 2. *Secure data collection and registration process***.**

3.3.2 Process of Secure Data Access and Retrieval

As shown in **Fig. 3**, the physician's mobile application ① initiates a secure session and ② establishes a forward-secure key exchange using ephemeral ECDH combined with the Kyber post-quantum. Once the session is active, the app ③ submits an access request (*patientID*, *recordID*) encrypted with Q-CP-ABE and a fresh nonce. The fog node ④ records this request as an on-chain *access-intent* transaction and ⑤ queries the ABE smart contract to verify the physician's attributes against the ciphertext policy. At the blockchain layer, ⑥ a decision is made: if attributes match, a *PERMIT* is issued; otherwise, a *DENY* is immutably logged and the process ends. In the permit case, the fog node ⑦ retrieves the ciphertext (CT) from storage and may ⑧ perform outsourced partial decryption to generate CT′ without exposing private keys. The result (CT or CT′) is then ⑨ transmitted securely back to the physician's mobile device. The mobile app ⑩ completes decryption locally using its ABE keys to recover the plaintext health record, while the fog node ⑪ logs the outcome (permit, timestamp, and hash) on-chain for immutable auditing.

3.4 PoA Consensus Protocol

In the proposed framework, the blockchain layer employs the Proof-of-Authority (PoA) consensus protocol to guarantee efficient, low-latency, and tamper-resistant validation of transactions. PoA leverages the identity and reputation of validators to establish trust. In the proposed scheme, fog nodes and hospital IT servers are designated as PoA validators. These entities are semi-trusted and authorized through cryptographic certificates. Each validator is responsible for proposing and validating new blocks, which contain transactions such as attribute registration and revocation, data access logs, and Smart contract executions for ABE key management. In this PoA protocol, fog nodes act as validators in a permissioned blockchain. First, the client submits a transaction to a fog node (proposer). Then the Proposer creates and signs a block and sends it to other fog validators. The validators verify and vote on the block. If the threshold is reached, the proposer commits the block to the blockchain ledger. The ledger returns a receipt to the client, ensuring finality and auditability. This process is illustrated in **Fig.4** as a UML sequence diagram.

3.5 Q-PA-ABE Encryption scheme

Symmetric encryption algorithms such as AES provide strong security but are often implemented with static key distribution, relying on pre-shared keys or centralized servers. However, AES has major drawbacks. AES demands high computational power and memory, making it hard for small or limited IoT devices to handle the workload efficiently. Moreover, existing systems lack adaptive key synchronization and remain vulnerable to evolving threats like replay, key exposure, and side-channel attacks.

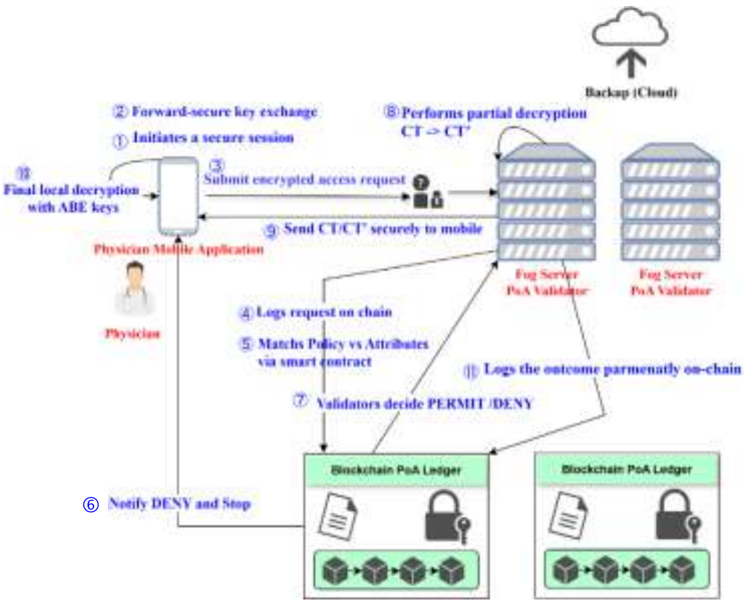

Figure 3. *Secure data access and retrieval process.*

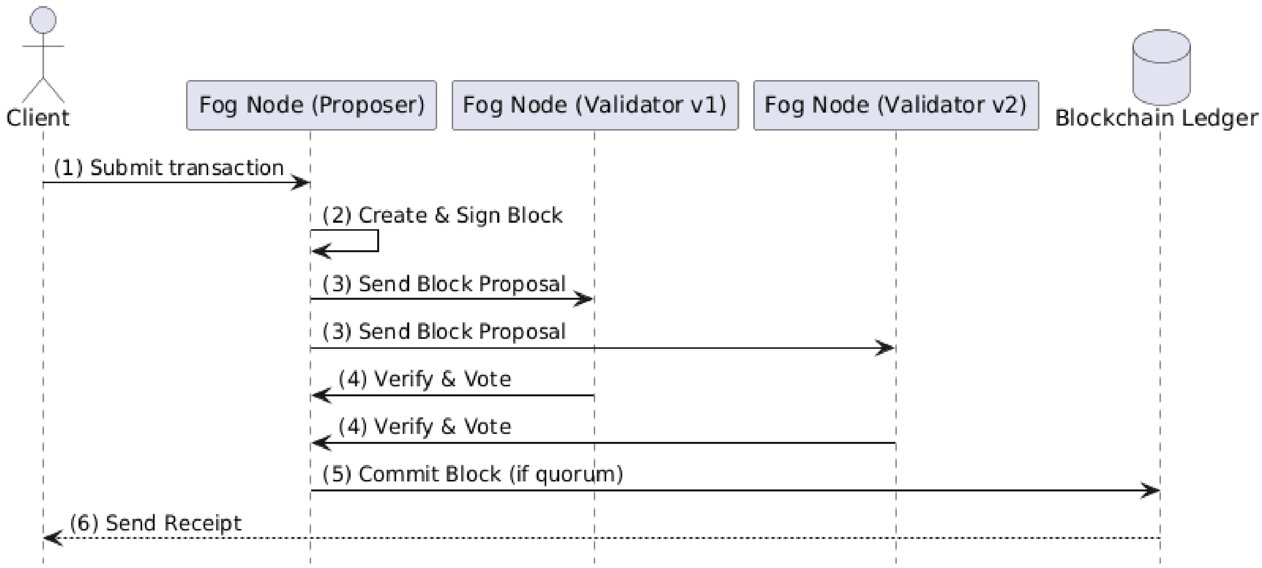

Figure 5. *PoA consensus protocol in the proposed system***.**

Centralized key management further weakens resilience and scalability, creating a single point of failure. These limitations underscore the need for a lightweight, dynamic, and secure key management paradigm tailored to the complexity of modern IoT networks.

A. Key Setup and Preparation

The system begins by initializing each IoT device, establishing the foundation for secure operations. To deliver a shared secret key, the system first applies Elliptic Curve Diffie–Hellman (ECDH) to provide forward secrecy and then reinforces this with the Kyber post-quantum key encapsulation mechanism (KEM), ensuring resilience against quantum adversaries. The ECDH shared secret is defined as follows:

$$K_{ECDH} = (x_A \cdot PK_B) = (x_B \cdot PK_A) \qquad (1)$$

where $x_A, x_B$are private keys, and PK_A, PK_B are the corresponding public keys of devices A and B.
In the Kyber encapsulation step, the sender A uses the recipient's public key PK_B to generate a random session key K_{Kyber} and produce a ciphertext CT that hides the key as follows:

$$(K_{Kyber}, CT) \leftarrow Encapsulate(PK_B) \qquad (2)$$

The recipient then uses its private key sk_B and the ciphertext CT to recover the session key K_{Kyber}

$$K_{Kyber} = Decapsulate(sk_B, C) \qquad (3)$$

This hybrid process (ECDH and Kyber) provides both forward secrecy and quantum resistance in the shared session key.

B. Secure Communication Using Q-CP-ABE

Once the session key is established, patient or device data is encrypted using Quantum-secure Ciphertext-Policy Attribute-Based Encryption (Q-CP-ABE). This scheme combines classical CP-ABE fine-grained access policies with post-quantum key encapsulation for long-term confidentiality. Each ciphertext embeds an access policy P expressed as an attribute tree (e.g., *Role = Doctor AND Dept = Cardiology*).

- **Encryption.** The system encrypts patient data using Attribute-Based Encryption (ABE):

$$CT \leftarrow Enc(PK, M, P) \qquad (4)$$

where M is the patient data, PK is the system public key, P is the access policy and CT is the ciphertext, bound to the access policy P.

- **Decryption.** When a physician requests access to patient data, it performs encryption algorithm using the following formula:

$$CT \leftarrow Dec(SK_S, CT) \qquad IF\ S \vDash P \qquad (5)$$

where CT is the encrypted message, SK is the private key according to a physician's attribute set S.Decryption succeeds only if the physician's attributes satisfy the policy P denoted as $S \vDash P$.

4. Results and Discussions

In the proposed model, we used Google Colab and Python platform. Google Colab is cloud-based environment used for our analysis. It used Python programming language and leveraged essential libraries for cryptography and encryption, such as PyCryptodome and cryptography, which support AES, RSA, and advanced hybrid schemes. In addition, with the rise of post-quantum security, enabling simulation of quantum-resistant algorithms (e.g., Kyber) and experimentation with quantum key distribution. The implementation consists of testing the proposed approach on health data of different sizes from 0.2 MB to 20 MB. The system also includes simulated or actual modules to detect various attacks, such as replay attacks, man-in-the-middle (MITM) intrusions, and brute force attacks. By analyzing message patterns and failed authentication attempts, the system dynamically detects and mitigates potential threats. In the rest of this section, we will detail the evaluation results of each model across attack classification, using various metrics such as time efficiency, memory efficiency and CPU efficiency.

4.1 Prototype: Illustrative Case Study

In IoT healthcare environments, where physicians use smartphones to monitor the health status of patients continuously, high performance must be maintained despite limited computational power. These benchmarks validate the feasibility of deploying the system in real-world clinical conditions, ensuring secure communication with minimal overhead and providing strong resistance to common cyber threats, while remaining ready for live deployment. The following diagram illustrates the secure transmission of patient health data from the physician's mobile device to the monitoring system, ensuring confidentiality, integrity, and trust in the communication process.

An ECDH key pair is established, and patient health data is encrypted using Q-CP-ABE with a dynamically generated Nonce. The resulting ciphertext and nonce are transmitted securely, ensuring confidentiality and integrity of sensitive medical information. This process prevents tampering during transmission between the physician's smartphone and the monitoring system.

Fig.5. depicts the patient-side data encryption and submission to Fog server.

Fig. 6 depicts the doctor-side decryption and response in the healthcare system. Upon receiving the encrypted request, the fog server derives the shared key via ECDH, decrypts the message, and verifies its authenticity using Q-PoA–CP-ABE.

Figure 5 *Encrypted data heath (Mobile Patient).*

If valid (e.g., decrypted as PERMIT), the fog server grants access and sends confirmation. This process highlights the system's end-to-end security, ensuring only authenticated doctors can access sensitive health data while rejecting tampered or replayed requests.

Figure 6. *Decrypted data heath (Mobile Doctor).*

4.2 Evaluation Metrics

The metrics used are time efficiency, memory efficiency, and CPU efficiency. These metrics are often used in the prediction of attacks and the performance evaluation of encryption algorithms.

- **Time efficiency:** is a widely used metric for schema evaluation. It measures the execution speed of an algorithm during encryption and decryption. In real-time IoT or healthcare systems, high latency can disrupt continuous data streams. One way to calculate the time efficiency of encryption and decryption processes is defined by Eq. 6:

$$T_{enc} = \frac{t_{enc}}{S_{data}} \; ; \; T_{dec} = \frac{t_{dec}}{S_{data}} \qquad (6)$$

where total encryption (t_{enc}), total decryption (t_{dec}), size of data (S_{data}) in MB. The lower the time efficiency values, the better the scheme performance.

- **Memory efficiency:** It is defined as the ratio of total memory consumed during encryption (M_{used}) compared to the size of input data. The lower the memory efficiency, the better the scheme performance.

$$M_{eff} = \frac{M_{used}}{S_{data}} \times 100\% \qquad (7)$$

- **CPU efficiency:** It is defined as the percentage of active CPU time used by the encryption task (C_{used}) consumed on total available CPU time. The lower CPU usage per unit time, higher efficiency.

$$CPU_{eff} = \frac{C_{used}}{C_{total}} \times 100\% \qquad (8)$$

4.3 Comparison Analysis of Time Efficiency in Encryption Algorithms

Table 1 presents the time efficiency of five encryption algorithms. The results indicate that SPEK is the fastest algorithm (0.21 ms/Mb), ideal for lightweight applications. AES-256 also performs efficiently (4.62 ms/Mb), offering a good balance between speed and security. RSA is slower (6.16 ms/Mb) due to its asymmetric nature. CP-ABE is the slowest (78.00 ms/Mb), reflecting its complex access control, while Q-CP-ABE improves on this but remains relatively slow (39.69 ms/Mb). Overall, symmetric algorithms are more time-efficient than attribute-based or asymmetric ones.

Table 1. *Comparative analysis of time efficiency in encryption algorithms.*

Encryption Algorithm	Time Efficiency (ms/Mb)
AES-256	4.62
RSA	6.16
SPEK	0.21
CP-ABE	78.00
Q-CP-ABE	**39.69**

4.4 Comparison Analysis of Memory Efficiency in Encryption Algorithms

Table 2 highlights the memory efficiency of five encryption algorithms. Q-CP-ABE and CP-ABE use 0.29% and 0.31% of memory, respectively, indicating efficient memory demands. RSA requires 0.21% of memory, while AES-256 is slightly more memory-intensive at 0.44%. Overall, the proposed algorithm tends to be more memory-efficient compared to asymmetric approaches.

Table 2. *Comparison analysis of memory efficiency in encryption algorithms*

Encryption Algorithm	Memory Efficiency (%)
AES-256	0.44
RSA	0.21
SPEK	0
CP-ABE	0.31
Q-CP-ABE	**0.29**

4.5 Comparison Analysis of CPU Efficiency in Encryption Algorithms

Table 3 highlights the memory efficiency of five encryption algorithms. The comparative analysis shows that Q-CP-ABE achieves the highest CPU efficiency (1.16%), reflecting its optimized handling of attribute-based operations despite higher computational complexity. CP-ABE follows closely at 1.23%, indicating that quantum-resistant adaptations slightly increase overhead but remain efficient. AES-256 and SPEK maintain moderate efficiency (1.04% and 0.99%), suitable for lightweight and symmetric encryption scenarios. RSA, being computationally intensive due to key size and modular exponentiation, records the lowest efficiency (0.82%). Overall, CP-ABE and Q-CP-ABE demonstrate superior CPU utilization within secure and context-aware environments.

Table 3. *Comparison analysis of CPU efficiency in encryption algorithms*

Encryption Algorithm	CPU Efficiency (%)
AES-256	1.04
RSA	0.82
SPEK	0.99
CP-ABE	1.23
Q-CP-ABE	**1.16**

4.6 Comparison of Gas Consumption for Transactions

The gas consumption, storage requirements, and execution time of the proposed approach were evaluated and compared with other blockchain-based models, specifically Smart Contract Federated Learning (FL) [23] and Smart Contract with Decision Function (DF) [24], as shown in Table 4**.** The findings indicate that the Smart Contract FL model [23] is the most storage-efficient, making it particularly suitable for edge computing environments where storage is a critical constraint. The Smart Contract DF model [24] requires slightly higher storage and gas consumption but benefits from faster execution times. In comparison, the proposed Blockchain PoA model offers a balanced trade-off between gas consumption, storage efficiency, and execution cost. It consumes moderate storage and lower gas than the FL approach, while maintaining strong support for data encryption, access control, and resilience to critical attacks. These characteristics make it well-suited for moderately storage-constrained environments, such as fog computing layers in healthcare systems. However, a potential limitation lies in scaling the storage infrastructure for large-scale medical data. Despite this, the system remains efficient for transactional operations and secure data governance within distributed e-health networks.

Table 4. *Comparison of Gas consumption of different approaches.*

Model	Storage Requirement (Kb)	Average Gas Consumption (eth)	Total Execution Cost (s)
Blockchain FL [23]	$[n \times 20, n \times 30]$	4 150 540	2.2700
Smart Contract DF [24]	$[n \times 24, n \times 32]$	3 320 656	1.6808
Proposed PoA	[n×22, n×28]	2 710 420	1.9542

5. Conclusion

We have presented a secure and lightweight decentralized architecture for IoT-based healthcare systems by integrating Q-PoA–CP-ABE, permissioned blockchain (PoA), fog computing, and elliptic-curve cryptography. The framework ensures end-to-end privacy, auditability, and communication integrity. Patient data is encrypted under expressive access policies, keys are distributed via blockchain smart contracts which removes central KGC dependence, and all transactions are immutably logged. By combining ECDH key exchange with Q-PoA–CP-ABE optimizations, the system mitigates prevalent threats such as replay, MITM, and brute-force attacks, while remaining computationally efficient for resource-constrained IoT devices. The proposed approach addresses critical requirements of privacy by supporting fine-grained encrypted sharing, security by preventing tamper-proof and attack-resistant), and scalability by ensuring one-to-many access and distributed KGC. Benchmark analysis confirms its efficiency in terms of memory, CPU usage, and encryption speed, addressing the shortfalls of traditional schemes like AES and RSA while demonstrating a future-proof and scalable solution. Future work will focus on prototype implementation in hospital IoT testbeds and perform latency/throughput benchmarking, and the integration of homomorphic encryption and dynamic policy management via smart contracts.

Author Statements:

- **Ethical approval:** The conducted research is not related to either human or animal use.
- **Conflict of interest:** The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper
- **Acknowledgement:** The authors declare that they have nobody or no-company to acknowledge.
- **Author contributions:** The authors declare that they have equal right on this paper.
- **Funding information:** The authors declare that there is no funding to be acknowledged.
- **Data availability statement:** The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

References

[1]Suryateja, P. S., & Rao, K. V. (2024). A survey on lightweight cryptographic algorithms in IoT. *Cybernetics and Information Technologies*, *24*(1), 21-34. DOI: https://doi.org/10.2478/cait-2024-0002.

[2]Benjamin, M. (2025). Lightweight Cryptographic Protocols for Secure IoMT Communication in Edge Networks.

[3]Radhakrishnan, I., Jadon, S., & Honnavalli, P. B. (2024). Efficiency and security evaluation of lightweight cryptographic algorithms for resource-constrained IoT devices. *Sensors*, *24*(12), 4008. DOI: https://doi.org/10.3390/s24124008.

[4]Kumar, A., & Sharma, D. K. (2020). Survey and Analysis of Lightweight Authentication Mechanisms. In *Cryptography-Recent Advances and Future Developments*. IntechOpen. DOI: https://doi.org/10.5772/intechopen.94407

[5]Svandova, Katerina, and Zdenek Smutny. "Internet of medical things security frameworks for risk assessment and management: a scoping review." *Journal of Multidisciplinary* Healthcare (2024): 2281-2301. DOI: https://doi.org/10.2147/JMDH.S459987.

[6] Deb, S., Lupu, E., Drakakis, E. M., Bharath, A. A., Leung, Z. K., Ma, G. R., & Chattopadhyay, A. (2025). Securing the Internet of Medical Things (IoMT): Real-World Attack Taxonomy and Practical Security Measures. *arXiv preprint arXiv:2507.19609*.

[7] Zhong, Y., & Gu, J. (2024). Lightweight block ciphers for resource-constrained environments: A comprehensive survey. *Future Generation Computer Systems*, *157*, 288-302. DOI: https://doi.org/10.1016/j.future.2024.03.054.

[8] Cai, D., Chen, B., Zhang, L., & Kan, H. (2024). BA-ORABE: Blockchain-Based Auditable Registered Attribute-Based Encryption With Reliable Outsourced Decryption. *arXiv preprint arXiv:2412.08957*. DOI : https://doi.org/10.48550/arXiv.2412.08957.

[9] Zhao, L., Dong, G., & Yuan, H. (2025). A blockchain-based verifiable CP-ABE scheme for medical data privacy protection. *Scientific Reports*, *15*(1), 27325. DOI: https://doi.org/10.1038/s41598-025-13069-1.

[10] Almaiah, M. A., Hajjej, F., Ali, A., Pasha, M. F., & Almomani, O. (2022). A novel hybrid trustworthy decentralized authentication and data preservation model for digital healthcare IoT based CPS. *Sensors*, *22*(4), 1448. DOI: https://doi.org/10.3390/s22041448.

[11] Ge, C., Liu, Z., Susilo, W., Fang, L., & Wang, H. (2023). Attribute-based encryption with reliable outsourced decryption in cloud computing using smart contract. *IEEE Transactions on Dependable and Secure Computing*, *21*(2), 937-948. DOI: https://doi.org/10.48550/arXiv.2412.08957.

[12] Ahmed, S., & Ahmed, T. (2022). Comparative analysis of cryptographic algorithms in context of communication: A systematic review. *International Journal of Scientific and Research Publications*, *12*(7), 161-173. DOI: https://doi.org/10.29322/IJSRP.12.07.2022.p12720.

[13] Shree, M. S., Shrinath, S., Anandh, R. V., Inbamalar, T. Comprehensive Comparison of Lightweight Encryption Algorithms for Energy-Efficient IoT Applications (2025). IEEE *Int. Conf. on Advances in Modern Age Technologies for Health and Engineering Science (AMATHE)* (pp. 1-7).

[14] Thakor, V. A., Razzaque, M. A., & Khandaker, M. R. (2020). Lightweight cryptography for IoT: A state-of-the-art. *arXiv preprint arXiv:2006.13813*. DOI:https://doi.org/10.29322/IJSRP.12.07.2022.p12720.

[15] Peivandizadeh, A., Y. Adarbah, H., Molavi, B., Mohajerzadeh, A., & H. Al-Badi, A. (2024). A secure key exchange and authentication scheme for securing communications in the Internet of Things environment. *Future Internet*, *16*(10), 357. DOI: https://doi.org/10.3390/fi16100357.

[16] Rancea, A., Anghel, I., & Cioara, T. (2024). Edge computing in healthcare: Innovations, opportunities, and challenges. *Future internet*, *16*(9), 329. DOI: https://doi.org/10.3390/fi16090329.

[17] Guo, C., Gong, B., Waqas, M., Alasmary, H., Tu, S., & Chen, S. (2024). An efficient pairing-free ciphertext-policy attribute-based encryption scheme for Internet of Things. *Sensors (Basel, Switzerland)*, *24*(21), 6843. DOI: https://doi.org/10.3390/s24216843.

[18] Reffad, H., Djenaoui, A., & Alti, A. (2021). Distributed Secure Services Based on IoT and Blockchain for e-Health Remote Care. In *Proc. Int. Conf. Computer Science's Complex Systems and Their Applications, Oum El Bouaghi (Algeria)* (pp. 25-26). CEUR-WS. org.).

[19] Wu, G., Wang, H., Lai, X., Wang, M., He, D., & Chan, S. (2024). A comprehensive survey of smart contract security: State of the art and research directions. *Journal of Network and Computer Applications*, *226*, 103882. DOI: https://doi.org/10.1016/j.jnca.2024.103882.

[20] Mallick, S. R., Lenka, R. K., Tripathy, P. K., Rao, D. C., Sharma, S., & Ray, N. K. (2024). Fog-assisted blockchain-iomt healthcare framework with role-based access control for critically ill patients. *SN Computer Science*, *5*(6), 658. DOI: https://doi.org/10.1007/s42979-024-02987-y.

[21] Shahzad, A., Chen, W., Zhang, Y., & Kumar, R. (2025). Zero-Trust Medical Image Sharing: A Secure and Decentralized Approach Using Blockchain and the IPFS. *Symmetry (20738994)*, *17*(4). DOI : https://doi.org/10.3390/sym17040551.

[22] Xie, Z., Li, Z., & Liu, X. (2025). SHARP: Blockchain-Powered WSNs for Real-Time Student Health Monitoring and Personalized Learning. *Sensors*, *25*(16), 4885. DOI : https://doi.org/10.3390/s25164885.

[23] Moulahi, W., Jdey, I., Moulahi, T., Alawida, M., & Alabdulatif, A. (2023). A blockchain-based federated learning mechanism for privacy preservation of healthcare IoT data. *Computers in Biology and Medicine*, *167*, 107630. DOI: https://doi.org/10.1016/j.compbiomed.2023.107630

[23] Alabdulatif, A., Al Asqah, M., Moulahi, T., & Zidi, S. (2023). Leveraging artificial intelligence in blockchain-based e-health for safer decision-making framework. *Applied Sciences*, *13*(2), 1035. DOI: https://doi.org/10.3390/app13021035.