Received: 18 March 2026 | Revised: 26 May 2026 | Accepted: 22 June 2026 | Published online: 7 July 2026

RESEARCH ARTICLE

Artificial Intelligence and Applications
2026, Vol. 00(00) 1–12
DOI: 10.47852/bonviewAIA62029685

BON VIEW PUBLISHING

Post-Quantum Blockchain and AI-Based Security Framework for Smart Healthcare Systems

Ahmad H. Alenezi[1,*]

[1] *Department of Computer Science, Taibah University, Saudi Arabia*

Abstract: The security of smart healthcare systems has become an important research topic as patient records are progressively digitalized, and new cyber threats continue to emerge. Traditional cryptographic mechanisms may become less reliable in the presence of quantum computing capabilities, which motivates the need for quantum-resistant security solutions. A simulation-based human-in-the-loop reference architecture for smart healthcare systems with post-quantum cryptographic mechanisms, blockchain-enabled auditability, and artificial intelligence (AI)-enabled threat detection to enhance security, privacy, and real-time monitoring is proposed. Our proposed framework integrates post-quantum digital signatures, quantum-resistant key establishment mechanisms with tamper-evident blockchain logging, and AI-based anomaly detection to facilitate secure and traceable healthcare data processing. Simulation experiments were performed using synthetic healthcare cybersecurity scenarios involving electronic health record access behavior and Internet of Medical Things traffic (e.g., unauthorized access attempts, anomalous data exfiltration, SQL injection, or distributed denial-of-service (DDoS)-like flooding attacks). The proposed AI-based detection model achieved an accuracy of 92.1%, a precision of 91.4%, a recall of 93.2%, an F1-score of 92.3%, and a false-positive rate (FPR) of 5.1%, with a detection-cycle latency of 200 ms. Scalability was evaluated using up to 10,000 simulated healthcare endpoints, with stable detection performance and blockchain-logging behavior observed in the simulation environment. The results indicate that the suggested framework can offer a scalable and privacy-aware security architecture for next-generation smart healthcare systems. The framework must be treated as a simulation-based reference that needs to be validated against real healthcare datasets and deployment scenarios.

Keywords: smart healthcare systems, post-quantum cryptography, blockchain security, federated learning

1. Introduction

The development of electronic healthcare systems incorporating the Internet of Medical Things (IoMT), cloud computing, and artificial intelligence (AI) has significantly improved the efficiency of patient care through real-time monitoring, assisted diagnosis, and faster data exchange. However, this technological development has also raised serious concerns related to data privacy, regulatory compliance, and the protection of sensitive personal health information. Healthcare is now a highly regulated sector, with strict legislation such as the Health Insurance Portability and Accountability Act (HIPAA) in the USA and the General Data Protection Regulation (GDPR) [1]. These regulations require patient data to be secured through both technical and procedural safeguards.

In the proposed architecture, patient privacy is first supported through post-quantum cryptographic primitives, including lattice-based mechanisms and zero-knowledge proofs, which contribute to the pseudonymization of patient identifiers. These mechanisms help protect patient information from unauthorized access and disclosure, in line with Articles 4 and 32 of the GDPR [2].

Another main pillar is access control, which we try to establish in the proposed framework. An architecture is based on role-based access control, smart contracts, and blockchain-backed identity management. User access is checked against pre-defined roles and permissions to ensure that one has the correct authorization prior to receiving sensitive healthcare data. This reinforces HIPAA technical safeguards that address access control and authentication as well as data minimization under the GDPR principle [3].

Through the blockchain layer, accountability is strengthened further because it places events of access and transaction data into a transparent and tamper-evident audit trail. To support the auditing of healthcare access, data provenance, and traceability requirements, the framework records all access operations in an immutable ledger. This design also complies with HIPAA audit control and meets the accountability principle of GDPR [4].

The analytics layer uses federated learning to avoid exposing unnecessary sensitive information. AI models can be trained in a federated manner where the patient data are not moved to a central repository but rather are locally stored on edge devices or institutional servers. It implements GDPR principles by

***Corresponding author:** Ahmad H. Alenezi, Department of Computer Science, Taibah University, Saudi Arabia. Email: aenzi@taibahu.edu.sa

constraining data processing only to what is needed for a specific task/purpose [5].

Data associated with patients exchanged using the architecture proposed are secured using cryptographic primitives resistant to quantum attacks. Post-quantum key encapsulation mechanisms like CRYSTALS-Kyber may be employed for secure key establishment and related functions, while CRYSTALS-Dilithium is used as a post-quantum digital signature scheme, providing authentication and integrity verification. This distinction is crucial as encryption and digital signatures provide different security services. Such mechanisms lower the long-term risks of quantum attacks, including those whose use is based on Shor's algorithm [6, 7].

Finally, the AI threat detection layer enables breach response and allows continuous monitoring for abnormal behavior and potential cyberattacks. Supervised models (e.g., logistic regression) and adaptive mechanisms (e.g., reinforcement learning [8]).

The main contribution of this work is the design and simulation-based evaluation of an integrated post-quantum blockchain and AI-enabled healthcare security framework. Unlike existing studies that address post-quantum cryptography, blockchain auditability, AI-based threat detection, or federated learning separately, the proposed framework combines these components into a unified layered architecture for smart healthcare environments.

The aims of the study are as follows:

a. To introduce post-quantum blockchain and AI technologies to support healthcare data security and privacy in view of HIPAA- and GDPR-oriented requirements.
b. To design a layered architecture that combines quantum-resistant cryptographic mechanisms, blockchain-based auditability, and real-time AI-based threat detection for smart healthcare systems.
c. To clarify the respective roles of post-quantum cryptographic mechanisms, particularly key encapsulation/encryption mechanisms and digital signature schemes, within the proposed healthcare security framework.
d. To evaluate the proposed architecture through simulation-based experiments focusing on detection accuracy, latency, scalability, and security-related performance indicators.

The remainder of the paper is structured as follows: a related work review is provided in Section 2, the proposed methodology in Section 3, and the results and analysis in Section 4, in addition to a conclusion and future research directions in Section 5.

2. Related Work

Recent research on smart healthcare security has increasingly focused on the convergence of the IoMT, AI, blockchain, post-quantum cryptography, and privacy-preserving data analytics. Smart healthcare systems rely on distributed sensors, electronic health records (EHRs), cloud platforms, and intelligent decision-support tools [9]. However, this interconnection increases exposure to unauthorized access, data leakage, adversarial attacks, and service disruption. Recent studies have also highlighted Zero Trust security architectures as a promising approach for mitigating authentication and access-control vulnerabilities in IoMT-based healthcare environments [10]. Recent studies on IoMT intrusion detection emphasize the importance of machine learning (ML) and deep learning models for identifying abnormal traffic patterns and cyberattacks in healthcare networks [11, 12]. Recent surveys further indicate that hybrid AI-driven cybersecurity frameworks integrating deep learning, explainable AI, and adaptive threat intelligence are becoming increasingly relevant for securing large-scale IoMT deployments in healthcare environments [13]. AI-assisted risk management approaches have also been proposed for healthcare systems in smart cities, highlighting the role of intelligent models in detecting and responding to operational and cybersecurity risks [2]. The broader deployment of Internet of Things (IoT) technologies in smart-city infrastructures further increases the need for secure and resilient healthcare services connected to urban digital ecosystems [14].

Blockchain has been extensively explored as a tool for enhancing auditability, transparency, and data provenance in healthcare systems. Recent studies have demonstrated some solutions that can be experienced when blockchain is combined with EHR access auditing to log who had accessed patient data, when the access happened, and even what the purpose of it was [4]. Several other studies suggest mechanisms of policy-based access-control functions built upon the blockchain framework, enforcing smart contracts and constituting pre-defined access policies to limit unwarranted access to EHRs [15]. These methods are evidence of the utility of blockchain for healthcare auditability and also reinforce that storing raw patient data directly on-chain is infeasible due to privacy, storage, and regulatory controls. Recent systematic reviews suggest that combining blockchain with AI-based analytics can improve trustworthiness, traceability, and automated threat response while preserving healthcare data integrity across distributed infrastructures [16].

At the same time, long-term cybersecurity strategies necessitated post-quantum cryptography. The delineation between key encapsulation mechanisms (KEMs) and digital signature schemes has been clarified in the post-quantum cryptographic mechanism standardization by the National Institute of Standards and Technology (NIST). For key establishment resistant against quantum computers, FIPS 203 specifies ML-KEM derived from CRYSTALS-Kyber, and for post-quantum digital signatures, FIPS 204 provides guidelines for the use of the Module-Lattice-Based Digital Signature Algorithm (ML-DSA) from CRYSTALS-Dilithium [6, 7]. Recent research on generic authenticated key exchange for IoT-based e-health systems has validated the relevance of lattice-based post-quantum mechanics to secure healthcare-connected devices from cyberattacks [17].

Privacy-preserving AI has also recently become a hot topic, particularly using federated learning. Specifically tailored to healthcare settings that are generally subject to stringent privacy regulations, federated learning allows models to be trained in a distributed manner without the need for collaborating institutions to centralize sensitive patient data. Federated learning has the potential to enable privacy-preserving smart healthcare analytics, but it also brings challenges such as adversarial attack, data poisoning, model inversion, interoperability, and scalability [18, 19]. Also, to improve privacy-preserving cybersecurity solutions in the distributed environment, federated-learning-based intrusion detection has been thoroughly reviewed [20].

Recent IoMT cybersecurity studies have further shown that hybrid AI models, including convolutional neural networks (CNNs), long short-term memory (LSTM), and reinforcement learning, can improve intrusion detection under dynamic healthcare network conditions [11]. Recent surveys emphasize that intrusion detection in IoMT increasingly combines ML, federated learning, blockchain, and explainable AI to address distributed healthcare cybersecurity requirements [21]. Moreover, adversarial attack detection frameworks using federated learning in medical IoT networks show that AI-based detection remains an active and critical research direction for healthcare cybersecurity [22].

However, even with these advances, most current studies treat AI-based threat detection, blockchain auditability, post-quantum cryptography, and federated learning as independent research directions. Only a handful of works offer a unified framework that integrates both post-quantum key establishment and digital signatures, blockchain transparency and immutability, AI-based anomaly detection, and privacy-preserving analytics in the context of a modular smart healthcare security architecture. This gap lays the foundation of the current study, which presents a simulation-based reference architecture for the integration of post-quantum blockchain and AI technologies in smart healthcare systems.

To better explain the positioning of the suggested job, Table 1 provides a summary of recent studies using representative ones sorted by their methods, benefits, and drawbacks, as well as remaining gaps in research. Through the comparison, we show that the existing works make contributions to post-quantum cryptography, AI-enabled healthcare risk management, federated learning, and IoMT intrusion detection. But most of these works only address a single security dimension each, and no work has provided a unified framework that combines protection against post-quantum attacks, auditability based on blockchain technology for health data, detection of advanced threats through AI technologies, and privacy-preserving analytics for smart healthcare systems.

The most significant research gap, as highlighted in Table 1, is the absence of a broadly focused security architecture built upon an intersecting analytics-as-a-service-based integrated healthcare solution applying quantum-resistant cryptographic protection, blockchain-supported traceability capabilities, and AI-based anomaly detection techniques to privacy-preserving analytics. The identified components are incorporated into a reference architecture based on simulation, which was derived to fill the gap. However, as shown in the last row of Table 1, the future validation on real healthcare datasets and deployed settings is still required to be performed under our framework.

Our key contribution is a simulation-based healthcare security reference architecture that integrates post-quantum key establishment, post-quantum digital signatures, blockchain-based auditability, AI-driven threat detection, and federated healthcare analytics. This contribution addresses a gap in the literature, as existing studies generally examine these components separately rather than integrating them into a unified healthcare information-security framework.

3. Methodology and Proposed Architecture

3.1. Overview of the proposed framework

In this section, the methodological background of the post-quantum blockchain and AI-based security framework for smart healthcare systems is presented. The framework is a layered reference architecture using post-quantum cryptography, blockchain-based approach to implement auditability, and AI-involved threat detection functionality in healthcare data confidentiality, integrity, traceability, and resilience.

The methodology is structured around three main components. First, post-quantum cryptographic mechanisms protect healthcare data and authentication processes from future quantum-enabled attacks. Second, blockchain technology is used to add a level of non-repudiation logging, access provenance, and decentralized auditability of healthcare transactions. Third, AI models are integrated to monitor anomalous access patterns or

Table 1
Comparative analysis of recent related work

Refs.	Methods	Advantages	Disadvantages	Research gap
[7]	Post-quantum key encapsulation	Standardized quantum-resistant key establishment	Does not address healthcare architecture or AI detection	No integration with blockchain or healthcare threat monitoring
[6]	Post-quantum digital signatures	Standardized quantum-resistant authentication	Does not provide encryption or anomaly detection	Needs integration into healthcare auditability workflows
[23]	Quantum computing impact on IoT security	Highlights quantum risks in IoT systems	General IoT focus, not healthcare-specific architecture	Limited integration with blockchain and AI response
[2]	AI-assisted risk management in healthcare	Healthcare-oriented AI risk analysis	Does not address post-quantum cryptography	No quantum-resistant security layer
[18]	Privacy-preserving federated learning healthcare	Supports decentralized privacy-aware learning	Focuses mainly on FL privacy, not blockchain/post-quantum cryptography (PQC)	Lacks integrated post-quantum blockchain security
[12]	ML-based intrusion detection in IoMT	Strong focus on IoMT threat detection	Limited emphasis on quantum-era cryptographic risks	No post-quantum blockchain auditability
[24]	Federated learning for cybersecurity	Supports decentralized intrusion detection	General cybersecurity focus, not healthcare-specific PQC	Limited healthcare blockchain integration
Proposed framework	PQC + blockchain + AI for smart healthcare	Integrates quantum-resistant security, auditability, and AI monitoring	Simulation-based evaluation only	Requires future validation using real healthcare datasets

suspicious IoMT communication with potential threat detection in near real time.

The proposed work should be understood as a simulation-based reference architecture rather than showing off a fully deployed production system. It is to clearly state the integration of post-quantum cryptography, blockchain, and AI in a unified healthcare security system with evaluations against metrics relevant to security, for example, detection accuracy, false positive rate (FPR), latency, and scalability.

3.2. Post-quantum cryptographic mechanisms

To secure smart healthcare systems against emerging quantum threats, the proposed framework integrates post-quantum cryptographic mechanisms for authentication, integrity verification, and secure data exchange. In particular, CRYSTALS-Dilithium is used as a post-quantum digital signature scheme, while Merkle-tree-based structures are employed for lightweight and tamper-evident integrity verification and blockchain-supported healthcare auditability [25].

CRYSTALS-Dilithium is built around the hardness of Module Learning With Errors (Module-LWE) and Module Short Integer Solution (Module-SIS) problems over polynomial rings. The architecture uses it to authenticate transactions on the blockchain, verify the integrity of exchanged healthcare records, and prohibit any unauthorized changes to audit logs. To clarify, CRYSTALS-Dilithium is not an encryption algorithm; it is a post-quantum digital signature scheme that provides authentication and integrity protection. Secure key establishment is handled separately using a post-quantum key-encapsulation mechanism, derived from CRYSTALS-Kyber, after which the established symmetric key can be used to encrypt healthcare data.

Merkle-tree-based structures are used to support efficient integrity verification and validation of healthcare transactions and IoMT data records. This data can be any kind of single transaction or record being processed, which is each hashed individually and then paired together with other hashes until a final Merkle root form. Alteration in a transaction will change the respective hash and propagate to the root, which makes it easily detectable when tampered with. This method is very appropriate for blockchain-based healthcare systems as it allows checks without requiring the reprocessing of all data records.

The post-quantum cryptographic model relies on the hardness of lattice-based problems. A simplified form of the Learning With Errors (LWE) problem can be expressed as:

$$A \cdot x + e = b \ (mod\, q) \tag{1}$$

In this formulation, A is a public matrix, x is a secret vector, e is a small random error vector, b is the resulting vector, and q is the modular arithmetic space used in lattice-based cryptographic constructions. Many lattice-based post-quantum cryptographic constructions rely on the computational hardness of recovering x from A and b in the presence of the error term e.

Secure hash functions are applied to blockchain data to generate transaction digests. In the framework, we hash the transaction data using SHA-3 as follows:

$$H(m) = SHA-3(m) \tag{2}$$

where m is the input message or transaction data and $H(m)$ is its hash value. This outputted digest is then utilized to verify the integrity of healthcare transactions, which is done via tamper-evident audit logs of the blockchain.

This is followed by batches of hashes from all transactions being aggregated together using a technology called Merkle trees. For example, A and B, two transaction hashes, can be merged as follows:

$$Root\ Hash = H(H(A) \,||\, H(B)) \tag{3}$$

where ‖ denotes concatenation. Such an implementation enables logging of healthcare transactions, which can be stored or pointed to on the blockchain layer in a tamper-proof manner and subsequently verified at low cost. This aggregation process makes it possible to verify integrity without having to fully re-enter all the transactions.

These mechanisms were chosen due to their capability of addressing quantum-secure authentication, integrity verification, and scalable auditability in smart healthcare environments. While the work presented here should not be viewed as a hardware-level implementation of all post-quantum cryptographic operations, it can instead be used as a simulation-based reference architecture. Extensive benchmarking of post-quantum cryptographic implementations targeting IoMT devices with limited resources is an avenue for future work.

The overall effect of the selected post-quantum mechanisms is to reinforce the integrity, authenticity, and auditability of healthcare data within the proposed architecture. CRYSTALS-Dilithium offers transaction authentication and integrity verification with quantum-resistant digital signatures, while Merkle-tree-based ones [23, 26] support lightweight and verifiable data integrity in IoT and medical records. Therefore, combining these mechanisms allows for secure data exchange, logging that is tamper-evident, and verification of access to be broken into even a decentralized network. They further enhance the resilience and privacy of your proposal at the same time retaining computational efficacy and scalability for a distributed smart healthcare environment. Yet, their complete deployment on resource-constrained IoMT devices will require more implementation-level benchmarks, which we define as future work.

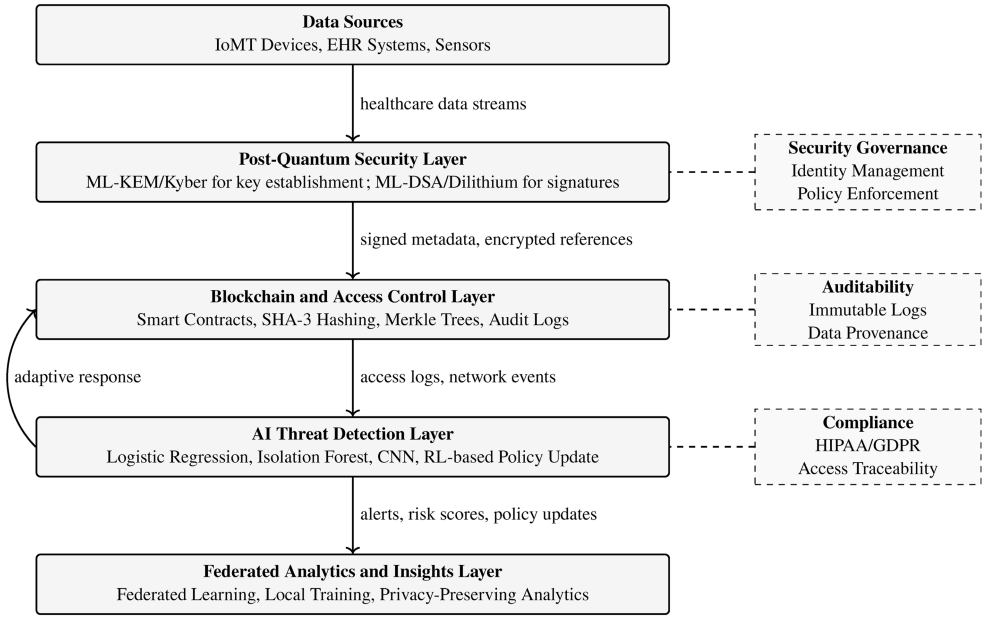
3.3. System architecture and operational workflow

This paper proposes a novel integrative architecture that integrates multiple post-quantum cryptographic ingredients with blockchain-based auditability and includes intelligence-driven threat detection and federated analytics for smart healthcare data protection across different stages of acquisition, communication, storage, monitoring, and analysis. Figure 1 shows that the architecture is divided into five different layers, namely, Data Sources, Post-Quantum Security, Blockchain and Access Control, AI Threat Detection, and Federated Analytics and Insights.

The Data Sources layer overviews the healthcare data obtained from IoMT devices as well as EHR systems and clinical sensors. The Post-Quantum Security layer secures these data before they are transmitted or referenced by the blockchain layer. This layer can utilize ML-KEM/Kyber for quantum-resilient key agreement and ML-DSA/Dilithium for digital signatures. This separation is essential for key establishment, and digital signatures provide different types of security guarantees.

The Blockchain and Access Control layer provides tamper-evident logging, access traceability, and policy-based authorization. The blockchain does not store raw patient records directly. The architecture, however, registers encrypted references and signed metadata as well as transaction hashes, access logs, and verification info. Transaction hashes are generated using SHA-3 (Equation (2)) and aggregated in Merkle-tree structures (Equation (3)). This gives you immutable logging and rapid integrity verification.

Figure 1
Proposed layered architecture for post-quantum blockchain and AI-based smart healthcare security



The AI Threat Detection layer checks access logs, network events, and various activities on the blockchain to detect anything suspicious or any potential cyberattacks. Logistic regression is used for supervised classification, Isolation Forest for unsupervised anomaly detection, and CNN-based models for learning complex patterns in healthcare and sensor data. Reinforcement learning supports adaptive policy updates and security responses when abnormal behavior is detected.

The Federated Analytics and Insights layer delivers privacy-preserving analytics without the need to centralize sensitive patient data. Local data are kept local to an institution, but model updates and risk indicators can be freely shared via authorized healthcare nodes. The layer provides decentralized learning, caters for local training, and performs analyses while preserving privacy.

The side modules are what governance and compliance objectives the architecture supports, as illustrated in Figure 1. This is where identity management and policy enforcement address security governance, auditability through immutable logs and data provenance, and regulatory alignment support for HIPAA/GDPR-oriented access traceability. In summary, this architecture creates a unified method for maintaining security across workflows with patient data being secured prior to transmission, access events recorded and protected by tamper-evident blockchain mechanisms, followed up with continuous AI model-based surveillance of abnormal behavior to adaptively mitigate threats.

The framework has layers including Data Collection, Post-Quantum Security, Blockchain and Access Control, AI Threat Detection, and Federated Analytics. Healthcare data originating from IoMT devices and EHR systems are protected by quantum-resistant cryptographic mechanisms prior to secure storage and audit logging. Blockchain mechanisms underline immutable traceability and verification of access, while AI-based models analyze network activity and access behavior continuously to detect cyberattack threats. Federated learning provides the option of distributing analytics without needing to centralize patient-specific data.

While this architecture is represented as a layering of components, there are frequent layer-to-layer interactions occurring continuously via audit logs, access-control events, anomaly alerts, and adaptive security policy updates.

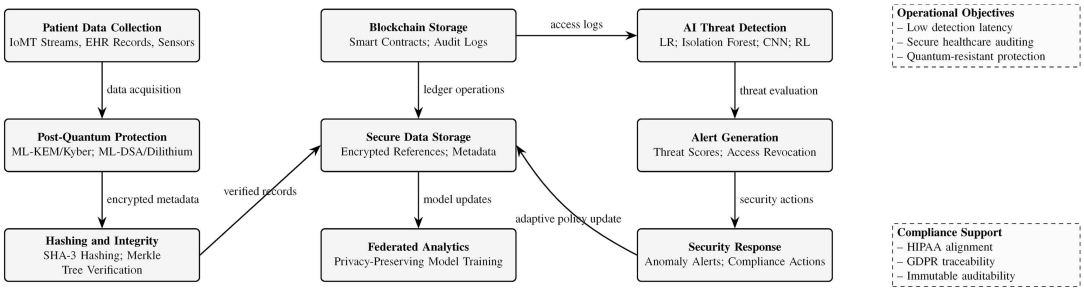
The operational workflow between data protection, blockchain auditability, AI-based monitoring, and compliance support when the proposed security framework is in effect is illustrated as a sequence diagram in Figure 2. The workflow starts with collecting the patient data from IoMT streams, EHR records, clinical sensors, and hospital systems. Such data are shielded in a post-quantum setting, where they employ ML-KEM/Kyber for key establishment and ML-DSA/Dilithium for digital signatures with SHA-3 hashing and Merkle-tree-based integrity checks.

Figure 2 shows that patient data in raw format are not stored directly on the blockchain. Encrypted references, metadata, hashes, and verified records are stored or logged to prove traceability while minimizing privacy exposure. Smart-contract operations and audit logs are recorded in the blockchain storage layer, which serve as inputs relevant to security for the AI Threat Detection Layer. It is significant to connect like that because the access logs and ledger operations result in evidence about abnormal behavior, unauthorized component access, or insufficient transaction patterns.

The AI Threat Detection Layer of the model combines (a) logistic regression, (b) isolation forest, and (c) CNN-based processing and reinforcement learning to support both detection and adaptive response. Once a potential threat is identified, the system will send out alerts and enforce security policies like access revocation or additional verification logs or even clear words as policy updates. Federated analytics reinforces privacy-preserving model training by enabling updating models without the sharing of sensitive patient data.

To sum up, from Figure 2, we can see that the proposed workflow is not a linear pipeline of data processing but rather a repeatable feedback-oriented security process. Secure application log audits are used to train AI systems, AI alerts for auto-response

Figure 2
Proposed operational flowchart of the post-quantum blockchain and AI-based security framework



adaptively in security onload, and federated analytics cast model updates while protecting privacy. It is designed to meet operational objectives of low detection latency, secure healthcare auditing, and quantum-resistant protection. At the same time, it accommodates regulatory alignment objectives subject to HIPAA-oriented access control, GDPR-oriented traceability, and immutable auditability.

3.4. Algorithmic workflow

Algorithm 1: Proposed Security Workflow for Post-Quantum Blockchain and AI-Based Smart Healthcare Systems

Input: PatientDataFile F, UserRequest R, BlockchainLedger B
Output: ProtectedRecordReference PR, ThreatDetectionOutcome E

1. Validate the format and compliance requirements of PatientDataFile F.
2. If F is invalid or non-compliant, reject the request and generate an audit event.
3. Preprocess F and extract the required metadata.
4. Generate a cryptographic hash h = SHA-3(F_metadata).
5. Establish a quantum-resistant session key using a post-quantum key establishment mechanism.
6. Encrypt or protect patient data using the derived session key.
7. Generate a post-quantum digital signature for the transaction metadata.
8. Store the encrypted data off-chain or in a secure distributed storage environment.
9. Record the protected data reference, hash value, signature, access event, and timestamp in BlockchainLedger B.
10. Aggregate transaction hashes using a Merkle tree structure for efficient integrity verification.
11. Extract security-relevant features from access logs, network activity, and IoMT data streams.
12. Apply the AI threat detection model to classify the activity as normal or suspicious.
13. If suspicious activity is detected, generate an alert and trigger an adaptive security response.
14. If the request is authorized, return the protected record reference PR to the healthcare provider.
15. Output the threat detection result E and update the audit trail.

4. Experimental Results and Analysis

We conducted simulation-based experiments for the proposed blockchain and AI-Enhanced Healthcare Security Framework with respect to operational security processing, AI-enhanced threat detection, and operational latency. We train on a blockchain simulator along with AI-based anomaly detection and quantum-resistant cryptographic mechanisms—all encapsulated in smart healthcare scenarios that encompass the collection of data streams from IoMT devices, which then interact with an EHR access scenario setting.

The experimental framework was implemented using a combination of Python-based AI libraries (TensorFlow, PyTorch, and Scikit-learn) for model development and Hyperledger Fabric components to simulate operations associated with blockchain. While the main goal of the evaluation is not to benchmark hardware-level post-quantum cryptographic implementations, it assesses the performance of the proposed integrated architecture based on representative healthcare cybersecurity scenarios.

4.1. Experimental dataset and evaluation protocol

The experimental assessment was made up of 20,000 records based on a simulated healthcare cybersecurity dataset. This dataset was generated in a way that resembles the access behavior of EHR oppositely toward IoMT traffic in a smart healthcare environment. It provides no patient identifiable information and should be seen as a synthetic evaluation dataset and not a public clinical dataset.

Since the dataset was recorded in the simulator environment with artificial logs resembling EHR access, as well as IoMT traffic patterns, it was not semantically extracted from any public clinical repositories or real patient records.

Table 2 provides an overview of the key security-related features used to characterize each synthetic healthcare cybersecurity record.

The dataset consists of 14,000 normal records and 6000 malicious records. As mentioned in section 3, normal records include some everyday health facilities (such as access to EHR permitted, regular communications of IoMT sensors, and valid data extraction operations). The malicious labels cover four classes of attacks involving unauthorized access attempts, anomalous data exfiltration from IoMT devices, SQL injection attempts to IoMT device databases, or DDoS-like flooding attacks against the devices as well.

Every record is expressed as a mixture of security-relevant features, including access frequency, count of invalid authentication (failed), session duration, request type class label (normal-abnormal), user role, device type, packet size, data transfer volume per hour, access time, source identifier (different servers with the same external address), destination service class labels (web/ftp/captcha, etc.), and abnormal request ratio. All categorical variables were one-hot encoded, and all numerical variables were normalized to 0–1 using min–max scaling. Preprocessing included the removal of missing values and duplicate entries.

Table 2
Dataset features used in the synthetic healthcare cybersecurity dataset

Feature	Description
Access frequency	Number of requests per session
Failed authentication count	Failed login attempts
Session duration	Active session duration
Packet size	IoMT traffic packet size
Request type	Access operation category
Device type	IoMT device category
Transfer volume	Data transmission size
Abnormal request ratio	Ratio of suspicious requests

An 80:20 stratified train-test split and 10-fold stratified cross-validation were employed for a fair evaluation of the classifiers with less sampling bias and better generalization. We performed a grid search for hyperparameter tuning using a 10% validation subset of the training data. The reported performance metrics were averaged over the folds, with standard deviation being reported only for the main detection metric (accuracy: 92.1% ± 2.1%).

The software environment contained Python 3.11, Scikit-learn for classical ML models, and TensorFlow/PyTorch for the neural-network-based components. It used Hyperledger Fabric components to simulate blockchain-related operations. The experiments were run on a standard workstation-class environment, that is, more than one core CPU, 32 GB RAM, and GPU acceleration only when necessary for neural-network-based components. To assess scalability, the number of simulated healthcare endpoints was gradually increased up to 10,000 while monitoring the stability in detection accuracy, processing latency, and blockchain logging throughput. Because this study focuses on a simulation-based reference architecture, the reported results should be interpreted as proof-of-concept performance evidence rather than deployment-level benchmarks. Under the simulated workload, detection accuracy and blockchain-logging throughput remained stable without substantial degradation in the main reported metrics.

Each record in the dataset was labeled based on the simulated scenario from which it was generated. Normal traffic consists of records generated from regular access and standard IoMT interaction, while malicious traffic includes all records produced by unauthorized access, injections, exfiltration, or flooding. Since the dataset was generated in simulations, the labeling process was driven by the attack scenario that was in place to generate it, and this guarantees a consistent assignment of labels for normal and malicious.

4.2. Operational security processing and blockchain performance

This subsection evaluates the operational security processing and blockchain-oriented performance of the proposed post-quantum security framework. The analysis focuses on processing time, throughput, quantum-resistance characteristics, and tamper-evident auditability within the simulated healthcare environment. The comparison includes the proposed post-quantum security workflow and representative classical mechanisms, including the Rivest–Shamir–Adleman (RSA), AES-256, and conventional symmetric encryption. These mechanisms are not identical in cryptographic function, and the comparison is therefore interpreted as an operational workflow-level comparison rather than a direct algorithm-level benchmark.

The objective of this evaluation is not to provide low-level cryptographic benchmarking but rather to assess the operational feasibility of integrating quantum-resistant protection and blockchain-based auditability into smart healthcare workflows.

Table 3 provides an operational comparison of the evaluated security mechanisms in terms of processing time, throughput, and quantum-resistance characteristics. The results show that RSA has the highest processing cost, requiring 500 ms to process 10 MB, which reflects the heavier computational burden of classical public-key encryption. In contrast, the proposed post-quantum security framework reduces the processing time to 150 ms and achieves a throughput of 66.67 MB/s, indicating a better balance between security strength and computational efficiency.

One more note that should be made is that cryptographic functions cannot be compared with those mechanisms in Table 3. RSA, which is a classical public-key mechanism, AES-256, and lightweight symmetric encryption are the symmetric mechanisms, while the transfer of post-quantum security workflow can be maintained through quantum-resistant key establishment, digital signatures, integrity verification, and blockchain-compliant auditability. Consequently, Table 3 cannot be interpreted as a straightforward cryptographic algorithm benchmark when interpreting the results but rather as an operational comparison of the security-processing behavior observed in the simulated healthcare workflow.

While lightweight symmetric encryption achieves the highest throughput, on its own, it does not provide post-quantum public-key establishment or digital signatures. AES-256 also has in-place strong symmetric protection, but AES-256 alone need not depend on a proper key establishment and authentication solution for a mayo-clinical like complete healthcare security architecture. Hence, an advantage of the proposed framework is not only in speed but also in providing a single security workflow that can combine all functions—quantum-resilient protection and authentication as well as integrity verification along with blockchain-compatible auditability.

Table 3
Operational security-processing comparison

Security mechanism	Processing time (ms)	Processing throughput (MB/s)	Quantum resistance
Proposed PQ security framework	150	66.67	Yes
RSA-based public-key mechanism	500	20	No
AES-256 symmetric encryption	250	40	Partial*
Lightweight symmetric encryption	120	83.33	Partial*

Note: Partial indicates that symmetric encryption is generally less vulnerable to quantum attacks than classical public-key cryptography, although Grover's algorithm may reduce its effective security level.

This trade-off is crucial from a healthcare point of view, as smart healthcare systems rely on both computational efficiency and long-term data protection. Medical records are sensitive and can remain valuable for decades, making them ideal targets for "harvest-now, decrypt-later" style attacks. The results thus suggest that the suggested framework can provide reasonable performance together with stronger quantum-era threat protection than pure classical public-key mechanisms.

The evolution of the security-processing behavior and security characteristics is depicted in Figures 3–5 based on their respective statistics reported in Table 3. As shown in Figure 4, RSA performs the slowest due to the computational overhead of classical public-key encryption. The proposed post-quantum framework alleviates this reduction in overhead, while also keeping stronger security goals than RSA according to the evolving quantum threat landscape. Though symmetric encryption is still the fastest component, quantifying this speed must be done carefully since symmetric encryption does not provide post-quantum public-key key establishment/digital signature warrant on its own.

The throughput trade-off that we have observed in Table 3 is validated in Figure 4. Lightweight symmetric encryption reaches the fastest encryption speed, followed by our proposed post-quantum framework. Compared to RSA, it has the lowest throughput, which makes it unsuitable for latency-sensitive smart healthcare environments. The focus of the proposed framework brings out a better and balanced trade-off between computational efficiency and quantum-resistant security properties.

The quantum-resistance characteristics of the evaluated mechanisms are compared in Figure 5. Combining quantum-safe key establishments with post-quantum digital signatures delivers

Figure 3
Comparison of security-processing time across evaluated cryptographic approaches

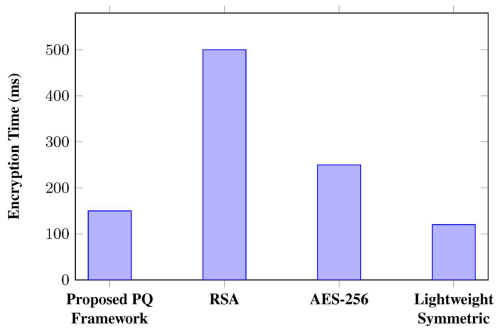


Figure 4
Comparison of processing throughput across evaluated security mechanisms

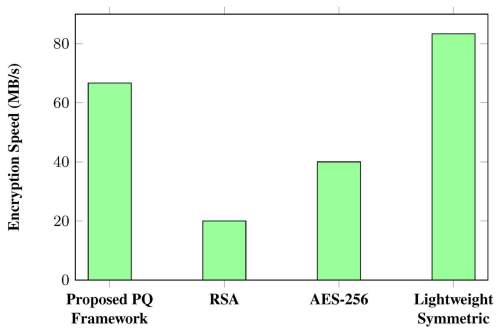
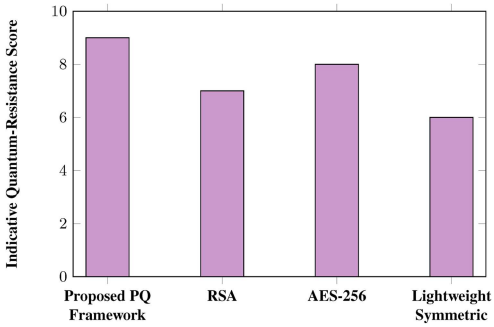


Figure 5
Comparison of quantum-resistance characteristics of evaluated security mechanisms



the maximum protection against quantum-era threats. AES-256 is cryptographically strong as a symmetric encryption mechanism, but by itself does not solve public-key key establishment or digital signatures. RSA is not quantum-resistant, and neither is lightweight symmetric encryption to an extent due to Grover's algorithm.

4.3. AI Threat detection performance

The AI-based threat detection module was compared to traditional rule- and signature-based detection techniques, as well as corresponding ML baselines. Their proposed AI pipeline is an integrated set of tools that incorporates supervised classification, data anomaly detection, and adaptive response strategies. L2 regularization was used with a maximum of 1000 iterations and the limited-memory Broyden–Fletcher–Goldfarb–Shanno (L-BFGS; lbfgs in Scikit-learn) solver for logistic regression. Isolation forest used 100 estimators (the default value) with a contamination of 0.1. Processing using CNN consists of two convolutional layers with ReLU before the max-pooling. An adaptation of the policy update based on Q-learning adapted to reinforcement learning components.

Table 4 summarizes the functional role of different AI components proposed in the framework. The AI layer is built as a detection and response pipeline—no single bloated model. Each of the components supports a specific function such as classifying known threats or anomaly detection, structured data analysis, and adaptive policy updates.

Table 4
Functional roles of AI components in the proposed threat detection pipeline

AI component	Primary function
Logistic regression	Supervised classification of known malicious access patterns and cyber threats
Isolation forest	Unsupervised anomaly detection for abnormal network or IoMT activity
CNN	Structured feature analysis for complex healthcare data and sensor-related patterns
Reinforcement learning	Adaptive policy update and dynamic response optimization under evolving threats

The logistic regression with a few supervised interpretable features, targeting known significantly blighted access patterns, is useful in highly regulated healthcare environments requiring explainable AI. In an additive way, isolation forest fulfills this role where it detects anomalies without requiring you to know all attack types a priori, which is good for zero-day attacks or threats that only occur under low frequency. Processing (using CNN) is included to enhance the representations learned from data-driven architectures, in case of datasets, such as structured sensor patterns or features derived from real medical data, when local patterns might be relevant for anomaly detection. At the response level, reinforcement learning is not directly treated as a classifier; rather, it aids in concurrency (adaptive policy updates) with changing threat conditions.

Hence, the AI layer proposed has both detection and response, as seen in Table 4. That design is more flexible and can help detect known threats and also support unknown anomaly identification.

In Table 5, the performance of our AI-based model for detection is compared with that of representative baseline approaches using precision, recall, F1-score, the area under the receiver operating characteristic curve (ROC-AUC), FPR, accuracy, and detection time. The proposed AI-based model for threat detection demonstrated the optimal results overall with an accuracy of 92.1%, precision of 91.4%, recall of 93.2%, F1-score of 92.3%, and ROC-AUC of 95.30%. These results justify that the model offers a sound trade-off between malicious activity detection and missed attacks.

The proposed model improves recall and F1-score compared to random forest and isolation forest, indicating higher detection of malicious events without diminishing classification quality. Importantly, the proposed model achieved the lowest false-positive rate, at 5.1%. This result is particularly relevant in healthcare environments, where excessive false alarms can contribute to alert fatigue and delay responses to genuine security incidents. The low accuracy results and high FPRs of traditional rule-based and signature-based methods confirmed their limitations in handling dynamic or previously unseen attack patterns.

Despite not having the best detection time, the 200 ms detection cycle is nevertheless reasonable for near real-time monitoring of healthcare security and other relevant domains. This indicates that the developed AI-based pipeline provides a viable compromise between accuracy, false-alarm reduction, and latency.

To complement the quantitative evaluation results summarized in Table 5, Figures 6–8 illustrate the same quantification of detection performance for three important evaluation dimensions: accuracy of positive and negative class detections (Figure 6), false-positive detections (Figure 7), and ROC-AUC score (Figure 8). These metrics were selected due to the fact that they observe the operational needs of the healthcare cybersecurity systems. Accuracy represents the overall correctness of the detection model, FPR is a measure of the false positive rate that signifies how likely an event would be raised as an alert even if it is non-malicious, while ROC-AUC evaluates the ability of a model in distinguishing normal from malicious activity for all possible thresholds.

Figure 6
Detection accuracy comparison of AI-based and baseline threat detection models

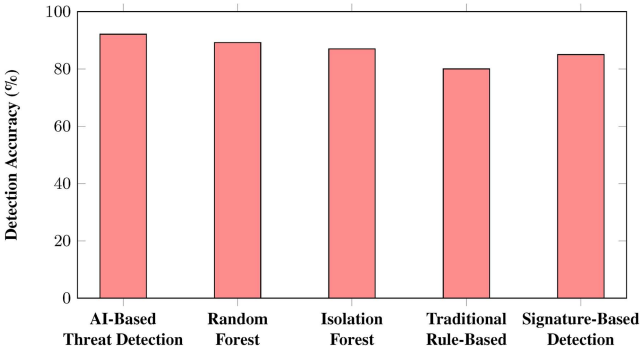
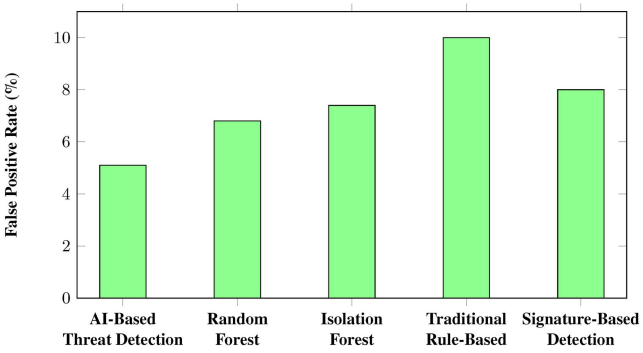


Figure 7
False positive rate comparison across threat detection approaches

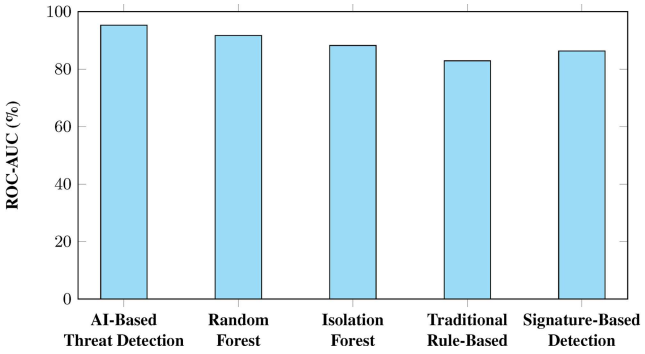


The evaluation results are presented in Figure 6, where the proposed AI-based threat detection model attains the highest accuracy compared to other approaches utilized for assessment. It means that a combination of supervised classification, anomaly detection, and adaptive response mechanisms (thus improving the identification of malicious behavior over traditional rule-based and signature-based systems). This performance gain is especially important to smart healthcare environments, where some attacks

Table 5
AI threat detection performance comparison

Detection Model	Precision (%)	Recall (%)	F1-score (%)	ROC-AUC (%)	FPR (%)	Accuracy (%)	Time (ms)
AI-based threat detection	91.4	93.2	92.3	95.3	5.1	92.1	200
Random forest	88.6	89.4	89.0	91.7	6.8	89.2	230
Isolation forest	86.1	87.5	86.8	88.2	7.4	87.0	210
Traditional rule-based	82.3	84.7	83.5	82.9	10.0	80.0	300
Signature-based detection	85.1	86.9	86.0	86.3	8.0	85.0	250

Figure 8
ROC-AUC comparison of threat detection models



involve heterogeneous IoMT traffic and abnormal access behavior (e.g., sudden spikes in requests) or can be impacted by changing threat patterns.

FPRs for each model are shown in Figure 7. The proposed model based on AI allows to obtain the lowest FPR, as excess false alarms may lead to alert fatigue and unnecessary administrative burden, thus delaying the response of healthcare professionals when actual adverse incidents occur. This is much better compared to the traditional rule-based detection, which shows the highest FPR and reveals it as a tool that cannot adapt to dynamically changing complex healthcare traffic.

The ROC-AUC values are summarized in Figure 8, which illustrates the stronger discrimination ability of the proposed AI-based model compared to the other three alternatives. A higher ROC-AUC might indicate that the model is better able to distinguish between normal activity and suspicious/malicious behavior at different thresholds for classification. This result is encouraging for the use of AI-based monitoring as a more dynamic solution than static rule-based or signature detection.

The reported detection time represents the end-to-end detection cycle, including feature preprocessing, model inference, and response generation. Performance metrics were aggregated across the cross-validation folds, and standard deviations were reported where applicable. Our AI-based detection model (described in Methods) performed with an accuracy of 92.1% ± 2.1%, confirming the stability of the metrics across folds (Methods). Nevertheless, these results should be viewed as proof-of-concept via computer simulation and not deployable benchmarks as further validation against true patient EHR data and in situ hospital infrastructure is still required.

Though the simulation results are encouraging, there are still many challenges ahead of a practical deployment. On the other hand, post-quantum cryptographic algorithms can add an extra computation burden on IoMT devices with limited resources. Blockchain-based auditability may also lead to unnecessary costs for storage and synchronization in healthcare infrastructures as its size grows. Moreover, real-world implementation also faces operational challenges of interoperability with existing healthcare information systems, regulatory governance, and secure key-management procedures.

5. Conclusion

This research introduced a reference architecture that integrates post-quantum cryptographic techniques, blockchain-based auditability, and AI exploitation for the cyber protection of smart healthcare services based on simulation analysis. It focuses on new types of cybersecurity issues that arise from IoMT contexts, EHRs, decentralized networks in healthcare, and potential quantum-based dangers in the future.

Our proposed hybrid architecture integrates quantum-resistant key establishment, post-quantum signatures, blockchain-supported traceability, and AI-powered anomaly detection to augment the transmission confidentiality, data integrity verification, and accountability along with adaptive threat monitoring in a healthcare environment. It also includes federated learning for the purpose of privacy-preserving analytics that do not rely on sensitive patient data being stored centrally.

We performed simulation-based experiments of synthetic healthcare cybersecurity scenarios where users accessed EHRs and traffic patterns from commercial medical devices such as Implants (i.e., implanted pacemakers). The assessment analyzed operational security-processing performance, AI-powered threat detection, detection latency, and scalability. Our experiments show that the proposed framework can deliver stable detection performance and FPRs lower than 5.1% at an acceptable operational latency, while enabling quantum-resilient security properties as well as blockchain-based auditability.

Contributions of this work should be viewed as a reference framework from a conceptual and simulation-oriented perspective. While the reported results are encouraging, it will be important to test using real-world health data, working hospital systems, and implementation-level post-quantum cryptographic benchmarking.

Evaluation of the framework will be done in further work using publicly available cybersecurity benchmark datasets as well as real healthcare environments with suitable ethical and regulatory requirements. Other future research scopes demand lightweight implementations of post-quantum-resistant schemes for IoMT devices with limited resources, integration and interoperability with existing health information systems, explainable AI-based threat detection, and secure connections to cloud-native healthcare environments.

Acknowledgement

The author thanks the reviewers and editorial team for their constructive comments.

Ethical Statement

This study does not contain any studies with human or animal subjects performed by the author.

Conflicts of Interest

The author declares that he has no conflicts of interest to this work.

Data Availability Statement

Data sharing is not applicable to this article as no new data were created or analyzed in this study.

Author Contribution Statement

Ahmad H. Alenezi: Conceptualization, Methodology, Software, Validation, Formal analysis, Investigation, Resources, Data

curation, Writing – original draft, Writing – review & editing, Visualization, Supervision, Project administration.

References

[1] Almomani, I., Ahmed, M., & Maglaras, L. (2021). Cybersecurity maturity assessment framework for higher education institutions in Saudi Arabia. *PeerJ Computer Science*, *7*, 1–26. https://doi.org/10.7717/peerj-cs.703

[2] Alrashdi, I., Hossin, M. A., & Kamruzzaman, M. M. (2023). AI-assisted risk management systems in healthcare industries of smart cities. In *2023 IEEE Globecom Workshops*, 2113–2117. https://doi.org/10.1109/GCWkshps58843.2023.10464736

[3] U.S. Government Publishing Office. (2024). *45 CFR § 164.312 - Technical safeguards, Electronic Code of Federal Regulations*. https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C/section-164.312

[4] Ullah, F., He, J., Zhu, N., Wajahat, A., Nazir, A., Qureshi, S., . . . , & Dev, S. (2024). Blockchain-enabled EHR access auditing: Enhancing healthcare data security. *Heliyon*, *10*(16), 1–26. https://doi.org/10.1016/j.heliyon.2024.e34407

[5] Elhosseini, M. A., Gharaibeh, N. K., & Abu-Ain, W. A. (2023). Trends in smart healthcare systems for smart cities applications. In *2023 1st International Conference on Advanced Innovations in Smart Cities*, 1–6. https://doi.org/10.1109/ICAISC56366.2023.10085212

[6] National Institute of Standards and Technology. (2024). *Federal information processing standards publication 204: Module-lattice-based digital signature standard (FIPS 204)*. U.S. Department of Commerce. https://doi.org/10.6028/NIST.FIPS.204

[7] National Institute of Standards and Technology. (2024). *Federal information processing standards publication 203: Module-lattice-based key-encapsulation mechanism standard (FIPS 203)*. U.S. Department of Commerce. https://doi.org/10.6028/NIST.FIPS.203

[8] Nadeem, M. (2025). Analyze quantum security in software design using fuzzy-AHP. *International Journal of Information Technology*, *17*(9), 5563–5575. https://doi.org/10.1007/s41870-024-02002-w

[9] Zaw, T. O. K., Muthaiyah, S., & Jasbi, A. (2021). Contextualization of smart healthcare: A systematic review. In *2021 7th International Conference on Research and Innovation in Information Systems*, 1–6. https://doi.org/10.1109/ICRIIS53035.2021.9617060

[10] Hernandez-Jaimes, M. L., Martinez-Cruz, A., Ramírez-Gutiérrez, K. A., & Feregrino-Uribe, C. (2023). Artificial intelligence for IoMT security: A review of intrusion detection systems, attacks, datasets and Cloud–Fog–Edge architectures. *Internet of Things*, *23*, 1–33. https://doi.org/10.1016/j.iot.2023.100887

[11] Shaikh, J. A., Wang, C., Sima, M. W. U., Arshad, M., Owais, M., Hassan, D. S., . . . , & Muthanna, M. S. A. (2025). A deep reinforcement learning-based robust intrusion detection system for securing IoMT healthcare networks. *Frontiers in Medicine*, *12*, 1–17. https://doi.org/10.3389/fmed.2025.1524286

[12] Rehman, M., Kalakoti, R., & Bahşi, H. (2025). Comprehensive feature selection for machine learning-based intrusion detection in healthcare IoMT networks. In *11th International Conference on Information Systems Security and Privacy*, *2*, 248–259. https://doi.org/10.5220/0013313600003899

[13] Fonsêca, A. L. A., Barbalho, I. M. P., Fernandes, F., Arrais Júnior, E., Nagem, D. A. P., Cardoso, P. H., . . . , & Valentim, R. A. D. M. (2024). Blockchain in health information systems: A systematic review. *International Journal of Environmental Research and Public Health*, *21*(11), 1–18. https://doi.org/10.3390/ijerph21111512

[14] Ilyas, M. (2021). IoT applications in smart cities. In *2021 International Conference on Electronic Communications, Internet of Things and Big Data*, 44–47. https://doi.org/10.1109/ICEIB53692.2021.9686400

[15] Yaqub, N., Zhang, J., Khalid, M. I., Wang, W., Helfert, M., Ahmed, M., & Kim, J. (2025). Blockchain enabled policy-based access control mechanism to restrict unauthorized access to electronic health records. *PeerJ Computer Science*, *11*, 1–32. https://doi.org/10.7717/peerj-cs.2647

[16] Naghib, A., Gharehchopogh, F. S., & Zamanifar, A. (2025). A comprehensive and systematic literature review on intrusion detection systems in the internet of medical things: Current status, challenges, and opportunities. *Artificial Intelligence Review*, *58*(4), 114. https://doi.org/10.1007/s10462-024-11101-w

[17] Mansoor, K., Afzal, M., Iqbal, W., Abbas, Y., Mussiraliyeva, S., & Chehri, A. (2024). PQCAIE: Post quantum cryptographic authentication scheme for IoT-based e-health systems. *Internet of Things*, *27*, 101228. https://doi.org/10.1016/j.iot.2024.101228

[18] Kumar, K. S., Nelson, L., & Jibinsingh, B. R. (2025). Systematic review of privacy-preserving Federated Learning in decentralized healthcare systems. *Franklin Open*, *13*, 1–15. https://doi.org/10.1016/j.fraope.2025.100440

[19] Abbas, S. R., Abbas, Z., Zahir, A., & Lee, S. W. (2024). Federated learning in smart healthcare: A comprehensive review on privacy, security, and predictive analytics with IoT integration. *Healthcare*, *12*(24), 1–33. https://doi.org/10.3390/healthcare12242587

[20] Khraisat, A., Alazab, A., Singh, S., Jan, T., & Jr. Gomez, A. (2024). Survey on federated learning for intrusion detection system: Concept, architectures, aggregation strategies, challenges, and future directions. *ACM Computing Surveys*, *57*(1), 1–38. https://doi.org/10.1145/3687124

[21] Hassan, S. R., Tanveer, M. U., Prajapat, S., & Shabaz, M. (2025). A comprehensive survey on intrusion detection in internet of medical things: Datasets, federated learning, blockchain, and future research directions. *ICT Express*, *11*(6), 1–20. https://doi.org/10.1016/j.icte.2025.11.005

[22] Sharaf, S. A., & Nooh, S. (2025). Identifying significant features in adversarial attack detection framework using federated learning empowered medical IoT network security. *Scientific Reports*, *15*(1), 1–22. https://doi.org/10.1038/s41598-025-14913-0

[23] Alosaimi, W., Alharbi, A., Alyami, H., Alouffi, B., Almulihi, A., Nadeem, M., . . . , & Agrawal, A. (2024). Analyzing the impact of quantum computing on IoT security using computational based data analytics techniques. *AIMS Math*, *9*(3), 7017–7039. https://doi.org/10.3934/math.2024342

[24] Hernandez-Ramos, J. L., Karopoulos, G., Chatzoglou, E., Kouliaridis, V., Marmol, E., Gonzalez-Vidal, A., & Kambourakis, G. (2025). Intrusion detection based on federated learning: A systematic review. *ACM Computing Surveys*, *57*(12), 1–65. https://doi.org/10.1145/3731596

[25] Kasyapa, M. S., & Vanmathi, C. (2024). Blockchain integration in healthcare: A comprehensive investigation of use cases, performance issues, and mitigation strategies. *Frontiers in Digital Health*, *6*, 1359858. https://doi.org/10.3389/fdgth.2024.1359858

[26] Banegas, G., Zandberg, K., Baccelli, E., Herrmann, A., & Smith, B. (2022). Quantum-resistant software update security on low-power networked embedded devices. In *International Conference on Applied Cryptography and Network Security*, 872–891. https://doi.org/10.1007/978-3-031-09234-3_43

How to Cite: Alenezi, A. H. (2026). Post-Quantum Blockchain and AI-Based Security Framework for Smart Healthcare Systems. *Artificial Intelligence and Applications*. https://doi.org/10.47852/bonviewAIA62029685