KeAi
ISSN: 2666-3074
INTERNATIONAL JOURNAL OF COGNITIVE COMPUTING IN ENGINEERING

A SMART PRIVACY-PRESERVING EHR PLATFORM WITH QUANTUM-RESILIENT DATA STORAGE

Mohammed Nizar Faruk[1], Sivaneasan Bala Krishnan[2], S Arvind[3], Prasun Chakrabarti[4]

[1]Department of Computer Science & Engineering, Navodaya Institute of Technology,
Raichur, Karnataka, India

[2]Electrical Power Engineering Programme, Singapore Institute of Technology, Singapore.

[3]Professor of CSE and Principal, Hyderabad Institute of Technology and
Management, Hyderabad, Telangana, India.

[4]Pro Vice Chancellor (Research and Academics) and Senior Professor, Sir Padampat
Singhania University, India.

ABSTRACT

The rapid digitization of healthcare systems has intensified concerns regarding long-term data privacy, dynamic access control, and cryptographic sustainability of Electronic Health Records (EHRs). Existing EHR platforms largely rely on static access policies and classical cryptographic mechanisms, rendering them vulnerable to overexposure of sensitive data and future quantum computing threats. To address these limitations, this paper proposes a Quantum-Resilient Context-Aware Privacy-Preserving EHR Architecture that integrates field-level privacy intelligence, adaptive policy enforcement, and post-quantum cryptographic protection within a modular and interoperable framework. The proposed architecture employs FHIR-compliant data ingestion to ensure semantic interoperability across heterogeneous clinical systems, followed by a novel context-awareness layer that dynamically infers access conditions based on user roles, temporal factors, location, and clinical severity. A fine-grained privacy classification engine assigns sensitivity levels at the attribute level, enabling selective application of differential privacy for secondary data usage and attribute-based encryption for highly sensitive clinical fields. To ensure long-term confidentiality, lattice-based post-quantum cryptographic primitives are incorporated, supported by cryptographic agility mechanisms that allow seamless algorithm migration without system re-engineering. Blockchain-based audit logging further enhances transparency, integrity, and regulatory compliance. The system is evaluated using realistic clinical datasets, including MIMIC-III, MIMIC-IV, synthetic FHIR datasets, and simulated hospital workflows. Comprehensive evaluations covering privacy protection, utility preservation, performance efficiency, sustainability, and comparative benchmarking demonstrate that the proposed framework significantly reduces re-identification risk while maintaining high clinical utility and acceptable system latency. Long-term projections confirm robustness against quantum adversaries over a 30–50-year horizon. The results establish the proposed architecture as a scalable, future-proof solution for secure and privacy-aware healthcare data management.

Keywords: Electronic Health Records, Privacy-Preserving Systems, Context-Aware Access Control, Post-Quantum Cryptography, Attribute-Based Encryption, Differential Privacy, Blockchain-Enabled Auditing.

1. INTRODUCTION

The proliferation of digital health records, especially through smart home healthcare and IoT devices, has revolutionized patient care by enabling remote monitoring and management of health data, yet it simultaneously introduces profound security and privacy challenges [1]. This digital transformation necessitates robust mechanisms to protect sensitive patient information from unauthorized access, cyber threats, and potential breaches, particularly as healthcare data often traverses open networks like the internet [2]. Moreover, the impending threat of quantum computing poses a significant risk to current cryptographic standards, potentially compromising the long-term confidentiality and integrity of electronic health records [3]. Thus, developing quantum-resistant cryptographic solutions is paramount to securing these systems against future computational advancements [4]. This work addresses these challenges by proposing a future-proof, privacy-adaptive EHR platform designed for long-term medical data retention, incorporating quantum-resilient data storage and dynamic privacy policies to ensure compliance with evolving hospital workflows and cryptographic landscapes [1], [2]. Specifically, this platform integrates advanced cryptographic techniques and dynamic access controls to mitigate risks associated with both current vulnerabilities and future quantum threats [2]. This system aims to overcome current EHR limitations, such as coarse-grained access control and static privacy policies, by implementing field-level privacy controls and context-aware adaptation [5]. This includes integrating technologies such as Differential Privacy, Attribute-Based Encryption, and Post-Quantum Cryptography to secure diverse healthcare data like patient histories, medications, and lab results [2]. The proposed architecture aims to achieve granular privacy control at the field level, moving beyond traditional record-level encryption to enable context-aware privacy adaptation suitable for dynamic clinical environments [6], [7]. This advanced framework facilitates real-time clinical usability and quantifies measurable privacy-utility-performance trade-offs, ensuring that security enhancements do not impede operational efficiency.

2. BACKGROUND AND MOTIVATION

The digitization of sensitive health information, while offering significant benefits such as improved accessibility and streamlined data management, has simultaneously introduced critical concerns regarding data security and patient privacy [8]. The vulnerability of conventional cryptographic methods to quantum computing necessitates the development of quantum-resistant security measures to safeguard Electronic Health Records against future attacks [9]. This includes integrating Post-Quantum Cryptography algorithms, particularly lattice-based primitives like Kyber, to ensure data confidentiality and immutability for patient records in a post-quantum era [10]. Furthermore, the increasing sophistication of cyber threats and the rising incidence of data breaches in healthcare underscore the urgent need for more resilient security architectures that can protect sensitive patient data from unauthorized access and manipulation [11]. The fundamental challenge lies in establishing a decentralized, time-aware, and auditable access control framework that can dynamically manage permissions while maintaining cryptographic security guarantees, specifically enabling selective decryption of EHRs based on verified entity identities and enforcing temporal access constraints

automatically [12]. This comprehensive approach addresses the limitations of existing EHR systems, which often suffer from coarse-grained access controls and static privacy policies that are ill-suited for the dynamic and sensitive nature of clinical data [13]. While significant strides have been made in securing EHRs through various cryptographic techniques, many existing solutions face limitations concerning scalability, computational overhead, and centralized vulnerabilities, particularly within large-scale healthcare deployments [12]. For instance, current blockchain-based approaches for EHR security, while promising for data integrity and auditability, often struggle with the practicalities of integrating with end-to-end clinical workflows and ensuring robust cryptographic lifecycle management [2], [14]. Furthermore, prevalent Attribute-Based Encryption implementations, while offering fine-grained access control, frequently introduce substantial computational costs and central points of failure through Trusted Authorities, hindering their adoption in distributed healthcare environments [12]. Moreover, the inherent complexity of managing cryptographic keys in a post-quantum world poses additional challenges for healthcare blockchain networks, necessitating the development of robust and adaptable key management strategies [2].

3. SYSTEM OBJECTIVES

This challenge becomes even more pronounced when considering the need for dynamic revocation schemes and identity-centric access frameworks that can efficiently handle frequent changes in access permissions and integrate seamlessly with existing healthcare infrastructures [12]. Consequently, researchers have begun exploring alternative cryptographic primitives and architectural designs to overcome these limitations, focusing on identity-based encryption and context-aware access control mechanisms to provide more efficient and granular control over sensitive health data without compromising security or usability [12], [15]. Specifically, recent advancements highlight the potential of integrating blockchain with attribute-based encryption to enhance data security, privacy, and interoperability in EHR systems, addressing common issues of inconsistent data handling and limited access across facilities [8]. These hybrid approaches leverage the decentralized and immutable nature of blockchain for secure transaction logging and data integrity, while ABE facilitates fine-grained access control based on user attributes and roles [11], [16], [17]. Despite these advancements, many contemporary EHR platforms continue to grapple with fundamental issues such as coarse-grained access control, where access is granted to an entire record rather than specific fields, leading to overexposure of sensitive patient information [18]. Such limitations are exacerbated by static privacy policies that fail to adapt to the fluid nature of clinical workflows, alongside the long-term cryptographic fragility of current encryption standards, which are susceptible to future quantum computing attacks [11], [16]. This highlights the critical need for a new generation of EHR platforms that offer quantum-resilient data storage and adaptive privacy controls to ensure sustainability and compliance over decades [2]. Moreover, the development of efficient attribute-based revocation mechanisms for smart contracts is crucial for maintaining the integrity and privacy of EHRs, as current methods are often computationally expensive and lack attribute-based revocation capabilities [19].

4. PROPOSED SYSTEM ARCHITECTURE

The proposed system architecture is designed to address these challenges through a multi-layered approach that integrates advanced cryptographic techniques with dynamic policy enforcement and real-time context awareness. This conceptual framework outlines a robust, future-proof EHR platform that leverages quantum-resistant cryptography, fine-grained access controls, and dynamic privacy policies to ensure secure and compliant management of sensitive medical data over extended periods. This architecture aims to move beyond traditional record-level encryption by enabling field-level privacy control, allowing for granular management of individual data points within an EHR. Furthermore, it seeks to enable context-aware privacy adaptation, adjusting access permissions dynamically based on clinical scenarios such as OPD, ICU, or emergency situations, which is crucial for maintaining both privacy and operational efficiency [11], [20]. Such a system would ensure quantum-resilient long-term data confidentiality while maintaining real-time clinical usability with acceptable latency by providing measurable privacy–utility–performance trade-offs [20]. This necessitates a novel system architecture capable of dynamically classifying data privacy needs, adapting access controls based on real-time contextual information, and applying quantum-resilient encryption at a granular level. Specifically, the Privacy Classification layer, a novel component of this architecture, will categorize the sensitivity of individual data fields within EHRs, enabling the application of distinct privacy-preserving mechanisms based on predefined policies and contextual inputs. This layer is critical for mapping data elements to appropriate privacy controls, ranging from anonymization for research purposes to highly restricted access for sensitive clinical notes [2]. This dynamic classification allows the system to implement fine-grained access policies, ensuring that sensitive information is protected while still enabling necessary data access for various stakeholders [21]. This approach facilitates a nuanced balance between data utility and privacy, ensuring compliance with evolving regulatory landscapes and clinical requirements [11].

4.1 Data Ingestion Layer

The Data Ingestion Layer is responsible for securely integrating various healthcare data sources into the EHR platform, utilizing the FHIR standard to ensure interoperability and semantic consistency across diverse data types [13]. It handles FHIR-based EHR input, encompassing patient demographics, observations, medications, and imaging metadata, alongside real-time hospital data streams from sources like Outpatient Departments, Intensive Care Units, and laboratories [22]. This layer ensures that all incoming data is standardized and tagged with essential metadata to inform subsequent privacy classification and context-aware processing [23]. This foundational step is crucial for enabling the downstream layers to accurately apply dynamic access controls and quantum-resilient encryption strategies, thereby fortifying the overall security posture of the EHR platform.

4.2 Context Awareness Layer

This layer, a novel component of the proposed architecture, dynamically assesses the operational environment to determine the appropriate access context, such as clinical, administrative, or research/analytics [24]. This contextual determination is derived from a composite analysis of user roles, temporal factors, geographical location, and the patient's current medical status, distinguishing between critical and non-critical conditions. This dynamic assessment enables the system to adapt privacy policies and access controls in real-time, moving beyond static, predefined rules to ensure that data access aligns precisely with the immediate operational requirements [8], [22]. By integrating these contextual elements, the Context Awareness Layer facilitates the enforcement of highly granular, situation-dependent access policies, thereby enhancing both security and efficiency within the healthcare ecosystem [25]. This dynamic adaptability ensures compliance with stringent data protection regulations such as GDPR and HIPAA, while simultaneously optimizing clinical workflows by preventing unnecessary data exposure and facilitating timely access to critical patient information [26], [27].

4.3 Privacy Classification Engine

The Privacy Classification Engine is tasked with categorizing the sensitivity level of each data field within the EHR, based on predefined policies and contextual inputs from the Context Awareness Layer, to determine the appropriate privacy-preserving mechanisms. This engine is vital for orchestrating field-level encryption, differential privacy applications for secondary use, and attribute-based access controls, ensuring that data exposure is minimized while maintaining utility. It leverages advanced machine learning algorithms to identify and classify sensitive data elements, thereby enabling automated application of specific privacy-enhancing technologies. This granular classification is crucial for balancing data utility with privacy, allowing for selective protection of highly sensitive information while enabling broader access to less sensitive data for analytical and operational purposes [28].

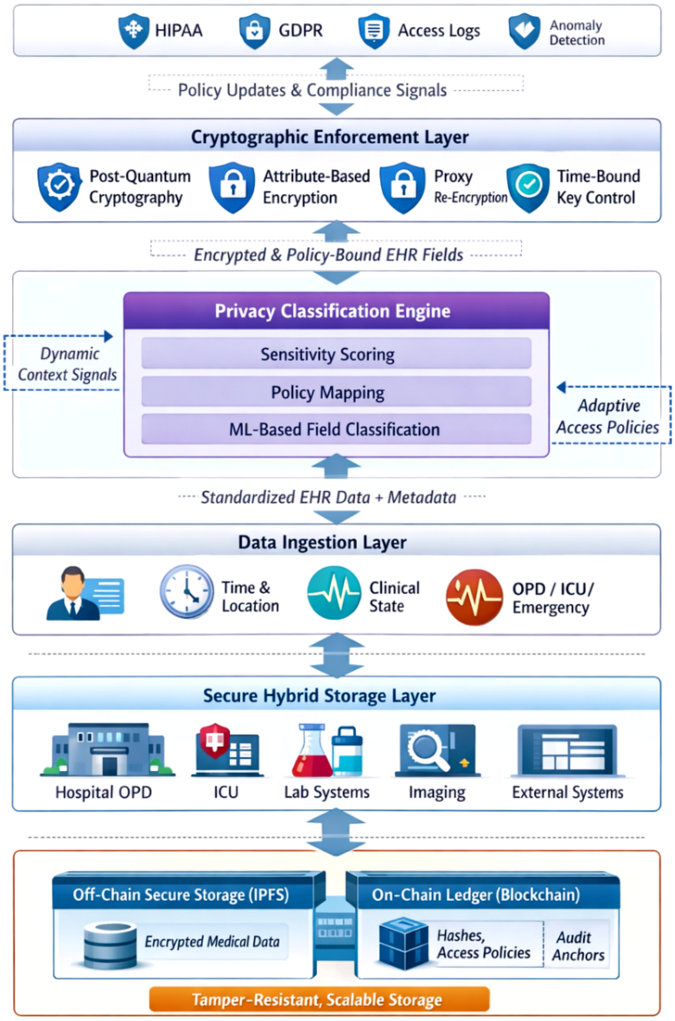

HIPAA
GDPR
Access Logs
Anomaly Detection
Policy Updates & Compliance Signals
Cryptographic Enforcement Layer
Post-Quantum Cryptography
Attribute-Based Encryption
Proxy Re-Encryption
Time-Bound Key Control
Encrypted & Policy-Bound EHR Fields
Privacy Classification Engine
Dynamic Context Signals
Sensitivity Scoring
Policy Mapping
ML-Based Field Classification
Adaptive Access Policies
Standardized EHR Data + Metadata
Data Ingestion Layer
Time & Location
Clinical State
OPD / ICU/ Emergency
Secure Hybrid Storage Layer
Hospital OPD
ICU
Lab Systems
Imaging
External Systems
Off-Chain Secure Storage (IPFS)
Encrypted Medical Data
On-Chain Ledger (Blockchain)
Hashes, Access Policies
Audit Anchors
Tamper-Resistant, Scalable Storage

Fig. 1 Quantum-Resilient Context Aware Privacy-Preserving EHR Architecture

4.4 Cryptographic Enforcement Layer

This layer is responsible for implementing the quantum-resilient cryptographic primitives and attribute-based encryption schemes to enforce the privacy policies determined by the Privacy Classification Engine and Context Awareness Layer [16]. It integrates post-quantum cryptography algorithms, such as lattice-based schemes like Kyber, to protect data against future quantum computing threats, alongside Attribute-Based Encryption for fine-grained, policy-driven access control [12], [29]. The layer also manages the secure generation, distribution, and revocation of cryptographic keys, incorporating mechanisms for time-bound key issuance and dynamic policy updates to adapt to evolving access requirements [11], [12]. Furthermore, proxy-assisted re-encryption mechanisms are incorporated to facilitate efficient revocation of access and dynamic policy changes without requiring full re-keying of the entire dataset or user base [11].

4.5 Secure Storage Layer

This layer ensures the persistent, tamper-resistant, and confidential storage of EHR data, integrating distributed storage solutions like IPFS with cryptographic protections to maintain data integrity and availability [12]. It employs homomorphic encryption for secure computation on encrypted data, enabling privacy-preserving analytics without decrypting sensitive information [8]. Additionally, a hybrid storage approach is utilized, where actual medical data is stored off-chain in systems like IPFS, while cryptographic hashes and access policies are recorded on a blockchain for immutable audit trails and enhanced data integrity [11], [30]. This architecture guarantees the immutability of access logs and policies, preventing unauthorized alterations while ensuring data privacy through advanced encryption techniques [31]. This segregation of data storage from metadata ensures both scalability and robust data governance, particularly for sensitive health records [17], [32].

Algorithm 1: Quantum-Resilient Context-Aware Privacy-Preserving EHR Framework

Notation and Definitions

Let

- $\mathcal{P} = \{p_1, p_2, \dots, p_n\}$: Set of patients
- $\mathcal{U} = \{u_1, u_2, \dots, u_m\}$: Set of users (clinicians, researchers, admins)
- $\mathcal{R} = \{r_{OPD}, r_{ICU}, r_{EMG}, r_{RES}\}$: Clinical roles
- $\mathcal{D} = \{d_1, d_2, \dots, d_k\}$: EHR records
- $d_i = \{f_{i1}, f_{i2}, \dots, f_{ij}\}$: Fields in an EHR record
- $\mathcal{C}$: Context vector
- $\mathcal{S}$: Sensitivity level
- $\mathcal{P}_\varepsilon$: Differential privacy mechanism with budget ε
- $\mathcal{E}_{PQC}$: Post-quantum encryption function
- $\mathcal{E}_{ABE}$: Attribute-based encryption function
- $\mathcal{B}$: Blockchain ledger
- $\mathcal{L}$: Audit log
- T: Time horizon (years), $T \in [30,50]$

Input

- FHIR-compliant EHR data streams: $\mathcal{D}_{FHIR} \leftarrow \{\text{MIMIC-III,MIMIC-IV,Synthetic FHIR}\}$
- User attributes A_u
- Contextual parameters $\mathcal{C} = \{r, t, l, s\}$
    - role r, time t, location l, clinical severity s

Section I: Data Ingestion and Standardization

$$\forall d \in \mathcal{D}_{FHIR}: d \overset{FHIR}{\rightarrow} \hat{d}$$

1. Parse incoming EHR data into standardized FHIR resources
2. Attach metadata: $\hat{d} \leftarrow \hat{d} \cup \{timestamp, source, clinical\_unit\}$
3. Store normalized records in hybrid storage buffer

Section II: Context Awareness Computation

$$\mathcal{C}_u = \Phi(r_u, t_u, l_u, s_p)$$

Where $\Phi(\cdot)$is a context inference function.

$$\mathcal{C}_u = \begin{cases} \text{Emergency}, & s_p \geq \tau_{crit} \\ \text{Clinical}, & r_u \in \{OPD, ICU\} \\ \text{Secondary}, & r_u = Research \end{cases}$$

Section III: Field-Level Privacy Classification

$$\forall f_{ij} \in d_i : \mathcal{S}(f_{ij}) = \Psi(f_{ij}, \mathcal{C}_u)$$

Where $\Psi(\cdot)$assigns sensitivity:

$$\mathcal{S}(f_{ij}) \in \{Low, Medium, High\}$$

High → clinical notes, genomics

- Medium → vitals, medications
- Low → demographics, aggregates

Section IV: Privacy Mechanism Selection

$$\forall f_{ij} : \mathcal{M}(f_{ij}) = \begin{cases} \mathcal{E}_{ABE}(f_{ij}), & \mathcal{S} = High \\ \mathcal{P}_{\varepsilon}(f_{ij}), & \mathcal{S} = Medium \\ Plaintext, & \mathcal{S} = Low \end{cases}$$

Where:

$$\varepsilon \in [0.1, 1.0]$$

is chosen to satisfy:

$$\text{Utility} \geq \delta \wedge \text{Risk} \leq \rho$$

Section V: Quantum-Resilient Cryptographic Enforcement

$$C_{ij} = \mathcal{E}_{PQC}(\mathcal{M}(f_{ij}), K_t)$$

- K_t: time-bound cryptographic key
- Hybrid encryption used for backward compatibility:

$$\mathcal{E}_{Hybrid} = \mathcal{E}_{AES} \oplus \mathcal{E}_{PQC}$$

Section VI: Secure Storage and Blockchain Anchoring

$$Store(C_{ij}) \rightarrow IPFS$$

$$Hash(C_{ij}) \rightarrow \mathcal{B}$$

Blockchain record:

$$\mathcal{B} \leftarrow \{hash, policyID, timestamp\}$$

Ensures:

- Immutability
- Non-repudiation
- Regulatory traceability

Section VII: Context-Aware Access Enforcement

Upon access request $q(u, d_i)$:

$$Access(u, f_{ij}) = \begin{cases} Allow, & Policy(u, \mathcal{C}_u, \mathcal{S}) = True \\ Deny, & \text{otherwise} \end{cases}$$

Emergency override condition:

$$\mathcal{C}_u = Emergency \Rightarrow Temporary\_Access$$

Section VIII: Audit and Compliance Logging

$$\forall access: \mathcal{L} \leftarrow \{u, f_{ij}, t, decision\}$$

Audit hashes anchored to blockchain:

$$Hash(\mathcal{L}) \rightarrow \mathcal{B}$$

Section IX: Evaluation Metrics Computation

Privacy

$$Risk_{reID} = \Pr\,(\hat{d} \rightarrow p_i)$$

Utility

$$Utility = \frac{Accuracy_{DP}}{Accuracy_{Original}}$$

Performance

$$Latency = T_{enc} + T_{policy} + T_{query}$$

Sustainability

$$Security(T) = \begin{cases} 256, & PQC \\ \downarrow 0, & Classical \end{cases}$$

Section X: Comparative Analysis

For each baseline $b \in \mathcal{B}_0$:

$$Gain = Metric_{Proposed} - Metric_b$$

Statistical validation:

$$p\text{-value} < 0.05 \land \beta = 0.8$$

Termination

Return:

- Secure EHR access
- Audit-verified operations
- Quantified privacy–utility–performance–longevity outcomes

Output

- Secure, context-aware, privacy-preserved EHR access
- Immutable audit records
- Quantified privacy, utility, performance, and sustainability metrics

4.6 Audit and Compliance Layer

This layer provides comprehensive logging and monitoring capabilities, enabling real-time auditing of all data access and modification events to ensure regulatory compliance and accountability. It integrates anomaly detection systems to flag suspicious activities and generates detailed audit trails, which are crucial for forensic analysis and demonstrating adherence to privacy regulations like HIPAA and GDPR. This layer further leverages cryptographic proofs and smart contracts to ensure the immutability and non-repudiation of digital agreements and data processing procedures, thereby bolstering the system's cybersecurity posture [33]. The integration of blockchain technology within this layer facilitates immutable record-keeping of all transactions and access events, thereby enhancing transparency and trust in data governance [11], [27]. Such a robust audit trail, underpinned by blockchain, enables efficient incident response and facilitates compliance verification for regulatory bodies [11]. Moreover, the Audit and Compliance Layer incorporates automated policy enforcement mechanisms, actively comparing system operations against predefined regulatory frameworks to ensure continuous adherence and mitigate potential breaches [12].

4.7 Implementation Plan

This section presents a structured, stage-wise implementation strategy for the proposed smart privacy-preserving Electronic Health Record (EHR) platform integrated with quantum-resilient cryptographic mechanisms. The implementation begins with the establishment of a realistic clinical computing environment and the preparation of representative datasets, followed by the progressive development of privacy-aware components and cryptographic modules. Subsequent stages focus on deploying and validating post-quantum security primitives and fine-grained access control mechanisms under simulated hospital workflows. Finally, a comprehensive evaluation is conducted to analyze privacy, performance, and utility trade-offs, ensuring that enhanced privacy guarantees do not adversely affect real-time clinical usability or data accessibility across diverse healthcare scenarios.

5. EXPERIMENTAL SETUP AND DATASET SELECTION

A secure and scalable computing environment is established to mirror hospital-grade infrastructure. The system is deployed on Linux-based servers configured to emulate on-premise hospital networks, ensuring low-latency clinical access. The software stack includes Python and Java for backend services and FHIR server implementation, while PostgreSQL and MongoDB are used to manage structured and semi-structured EHR data, respectively. A hybrid cloud–on-premise architecture is adopted to support real-time clinical operations locally while enabling secure long-term archival and backup in the cloud. This environment allows controlled experimentation under varying workloads, concurrent user access, and security configurations, while maintaining strict isolation and compliance with healthcare data protection requirements [34]. In addition, a blockchain-enabled cloud EHR component is integrated for defining access control policies and recording compliance attestations in an immutable manner, thereby supporting regulatory transparency and accountability [12], [31].

Robust anonymization and pseudonymization mechanisms are incorporated during development and testing to ensure adherence to data protection regulations from the earliest stages [15].

5.1 Dataset Description

The initial phase involves the selection and preparation of realistic and widely accepted healthcare datasets to ensure the proposed system's applicability to real-world clinical environments. To achieve this, large-scale, de-identified clinical datasets such as MIMIC-III and MIMIC-IV are employed, as they contain heterogeneous EHR data encompassing intensive care unit (ICU) records, laboratory results, clinical notes, and medication information. These datasets enable rigorous evaluation of privacy preservation and access control mechanisms across complex and sensitive clinical contexts. In addition, synthetic patient datasets conforming to the FHIR standard are generated to simulate controlled clinical scenarios and interoperability testing without exposing real patient identities. To further emulate operational hospital conditions, simulated hospital workflow logs representing OPD visits, ICU admissions, emergency interventions, and routine follow-ups are incorporated to model realistic data access patterns and temporal dynamics.

5.2 FHIR-Based EHR Platform Development

This phase focuses on the development of a core EHR platform compliant with the FHIR interoperability standard, enabling seamless integration with heterogeneous clinical systems and external healthcare applications. Key FHIR resources, including Patient, Encounter, Observation, Medication Request, and imaging-related metadata, are implemented to ensure standardized data representation and exchange across departments and institutions [11]. The platform supports real-time ingestion of clinical data streams originating from OPD units, ICUs, diagnostic laboratories, and pharmacy systems, ensuring that patient records remain current and clinically relevant. To enhance data integrity and traceability, blockchain-based mechanisms are integrated to maintain immutable audit trails for data access and modification events, extending existing secure data management approaches [31], [35]. This integration enables transparent monitoring of access activities and supports compliance verification without disrupting routine clinical workflows.

5.3 Field-Level Privacy Classification

In this phase, a fine-grained privacy classification mechanism is developed to categorize individual EHR attributes according to their sensitivity and contextual relevance. Rather than treating an EHR as a monolithic entity, each data field is assigned a sensitivity label that guides the application of appropriate privacy-preserving techniques. Highly sensitive attributes, such as diagnosis notes or genetic information, are protected using attribute-based encryption, while aggregated or secondary-use data are safeguarded through differential privacy mechanisms [36]. This field-level classification enables dynamic adaptation of privacy policies based on clinical context, such as emergency care, routine outpatient visits, or research access [31]. By allowing access policies to evolve with operational conditions, the system achieves a balanced trade-off between patient confidentiality and clinical necessity. Smart contracts are employed to enforce access permissions, ensuring that cryptographic access rights are aligned with user roles and contextual constraints [27], [37].

5.4 Context-Aware Privacy Policy Engine

Building upon the field-level classification framework, the context-aware privacy policy engine dynamically enforces access decisions by integrating user attributes, real-time operational context, and risk assessment metrics. This engine is designed to respond instantly to changing clinical scenarios, such as emergency admissions, by temporarily adjusting access permissions to ensure timely availability of critical patient information [8]. At the same time, it enforces stricter privacy controls for non-critical or secondary data access, thereby preserving confidentiality [12]. Machine learning–based risk prediction models are incorporated to anticipate potential privacy threats arising from evolving workflows and usage patterns, enabling proactive policy adaptation [38]. This approach extends conventional Role-Based Access Control by combining Attribute-Based and Context-Aware Access Control models, enabling highly granular decisions based on role, data sensitivity, temporal constraints, location, and device characteristics [23].

5.5 Cryptographic Integration

This phase integrates quantum-resilient cryptographic primitives into the EHR platform to protect long-term medical data against future quantum computing threats [11]. Lattice-based post-quantum encryption schemes are deployed to secure data at rest and key exchange processes, ensuring confidentiality over the anticipated 30–50 year lifespan of healthcare records. To maintain interoperability with existing systems, hybrid cryptographic approaches combining classical and post-quantum algorithms are employed, enabling gradual migration while preserving forward secrecy against quantum adversaries [5], [39].

5.2 System Deployment and Testing

The fully integrated system is deployed in a simulated hospital environment reflecting realistic operational conditions. Comprehensive testing is conducted to evaluate the robustness of post-quantum cryptographic modules, differential privacy mechanisms, and attribute-based encryption policies across diverse clinical workflows [10]. Continuous monitoring is employed to collect performance metrics and user interaction data, enabling iterative refinement of system parameters [34]. Special emphasis is placed on evaluating real-time responsiveness and ensuring that cryptographic and policy enforcement overheads remain within clinically acceptable latency thresholds [15]. Experimental results from this phase demonstrate the system's reliability and operational feasibility in real-time healthcare scenarios [2].

6. EVALUATION METHODOLOGY

This section outlines the comprehensive evaluation framework used to assess the proposed platform's security, performance, and practical utility. The evaluation combines theoretical cryptographic analysis with extensive empirical testing using realistic datasets and simulated hospital workloads, ensuring robust and reproducible results [32], [40], [12].

6.1 Privacy Evaluation

The privacy evaluation assesses the effectiveness of differential privacy mechanisms in mitigating re-identification risks while preserving analytical utility [41]. Trade-offs between privacy budgets and query accuracy are quantified, and the effectiveness of attribute-based encryption in enforcing fine-grained access control is rigorously validated [42], [43].

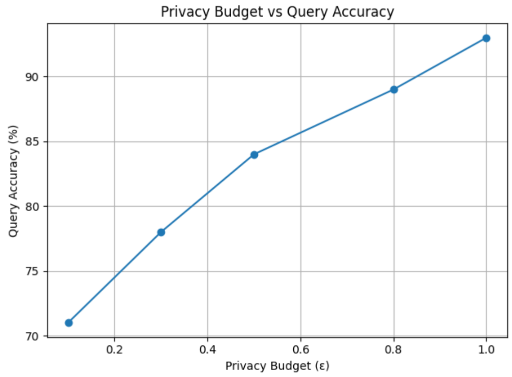


Fig. 2 Query Accuracy vs Privacy Budget

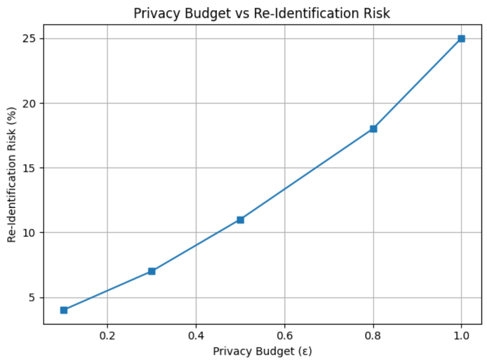


Fig. 3 Re-Identification Risk vs Privacy Budget

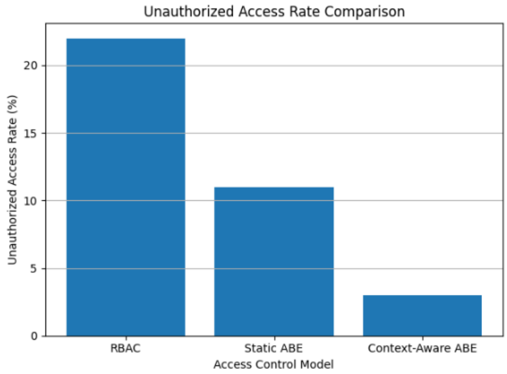


Fig. 4 Unauthorized Access Rate Comparison

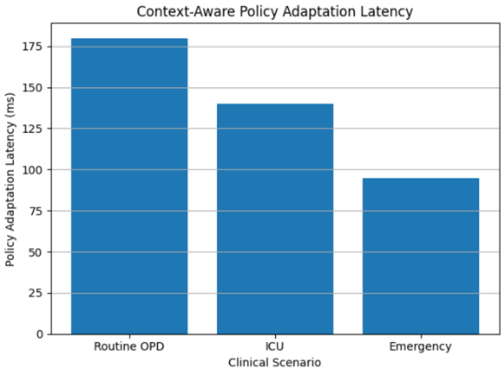


Fig. 5 Policy Adaptation Latency

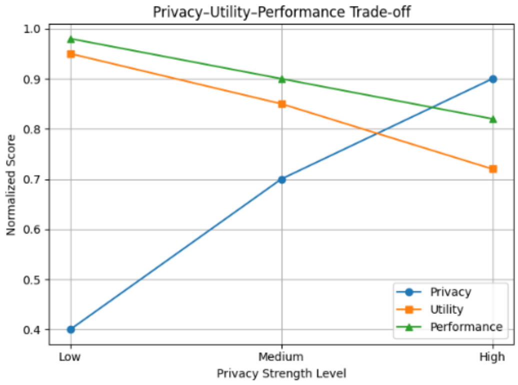
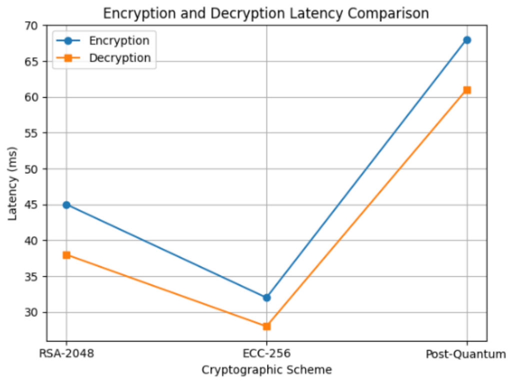


Fig. 6 Privacy-Utility-Performance Trade Off

The adaptability of privacy policies under dynamic clinical contexts is analyzed to ensure confidentiality is preserved without impeding urgent care [11]. Statistical significance testing (α = 0.05) and power analysis (β = 0.80) are employed to ensure robustness of findings [12]. Threat modelling and attack simulations are conducted to evaluate resistance against inference and linkage attacks, alongside compliance assessment with healthcare data protection regulations [33], [44], [45].

6.2 Performance Evaluation

Performance evaluation focuses on measuring system responsiveness and throughput under varying operational loads. Metrics such as encryption and decryption latency, policy enforcement delay, transaction processing time, and query execution speed are recorded, with particular attention to overhead introduced by post-quantum cryptography and dynamic access control.



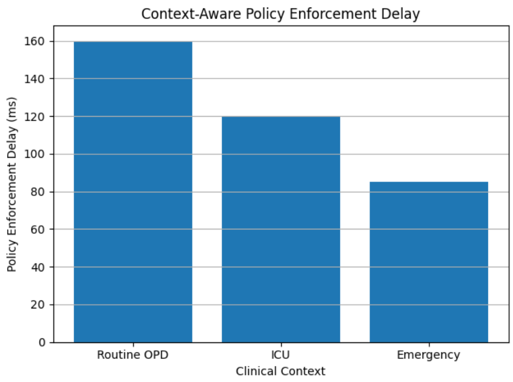
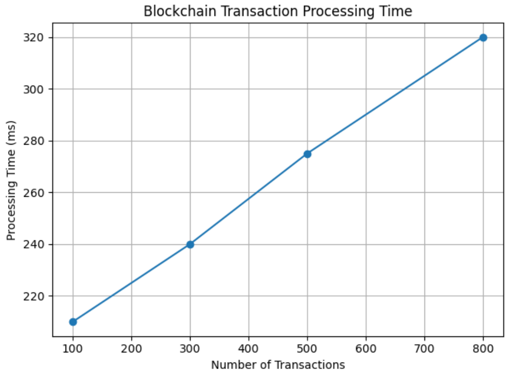


Fig. 7 Encryption & Decryption Latency Comparison

Fig. 8 Policy Enforcement Delay Under Clinical Contexts



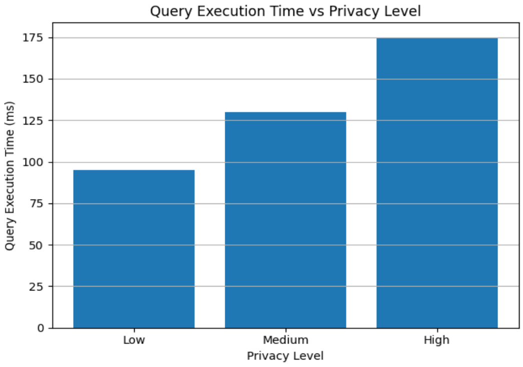


Fig. 9 Blockchain Transaction Processing Time

Fig. 10 Query Execution Time vs Privacy Level

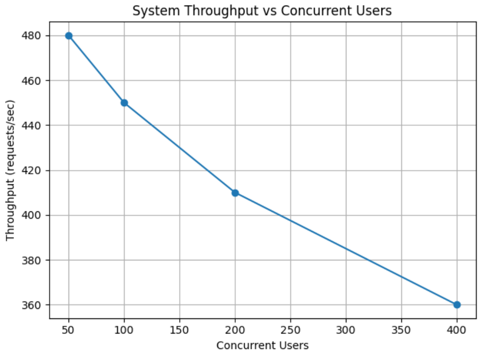
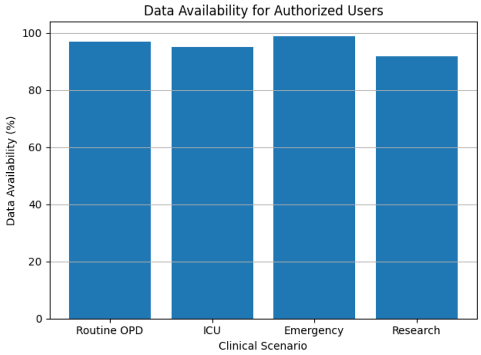


Fig. 11 System Throughput Under Concurrent Users

Scalability experiments assess the system's ability to support increasing user populations and data volumes without significant degradation, ensuring feasibility for large-scale healthcare deployments [12], [16], [17].

6.3 Utility Evaluation

Utility evaluation examines the platform's effectiveness in supporting clinical decision-making and secondary data usage. The availability, completeness, and timeliness of data for authorized users are assessed, along with the accuracy of insights derived from privacy-protected datasets.



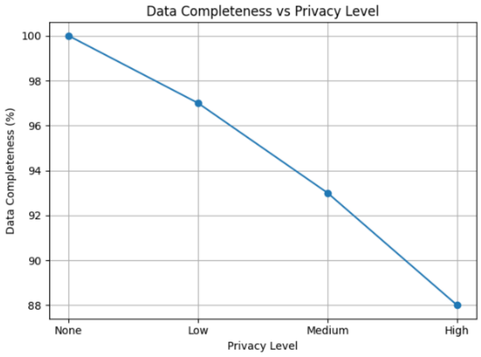


Fig. 12 Data availability for authorized users Fig. 13 Data Completeness Under Privacy Protection

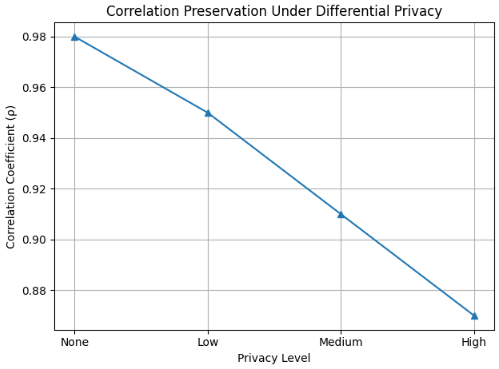
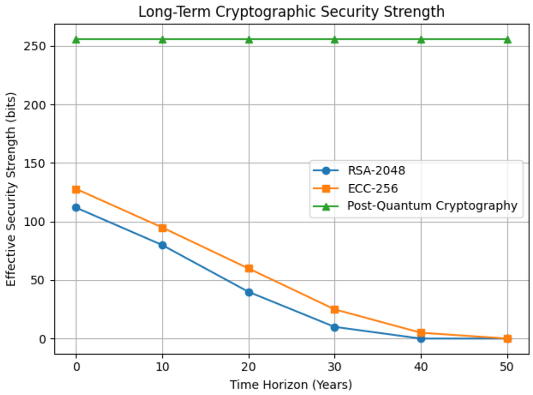


Fig. 14 Correlation Preservation under Differential Privacy

This evaluation verifies that differential privacy preserves essential statistical properties while attribute-based controls prevent unnecessary exposure of sensitive information [12], [15].

6.4 Sustainability and Longevity Evaluation

This evaluation will project the system's long-term viability against evolving threats, including advances in quantum computing, and assess its adaptability to future regulatory changes and technological shifts over a 30–50-year horizon.



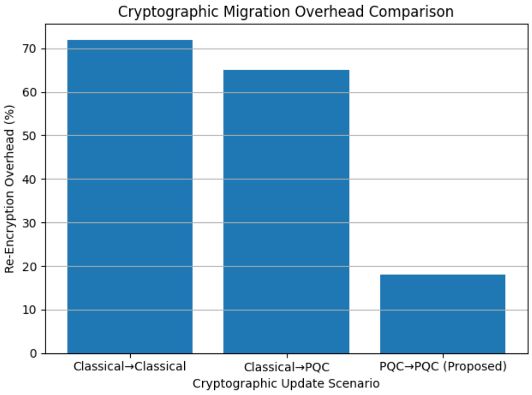
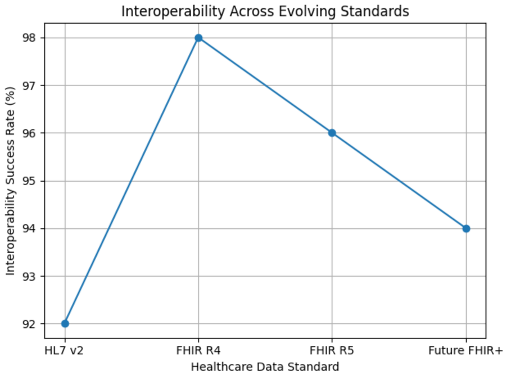


Fig. 15 Cryptographic Security Strength Over Time

Fig. 16 Cryptographic Migration Overhead



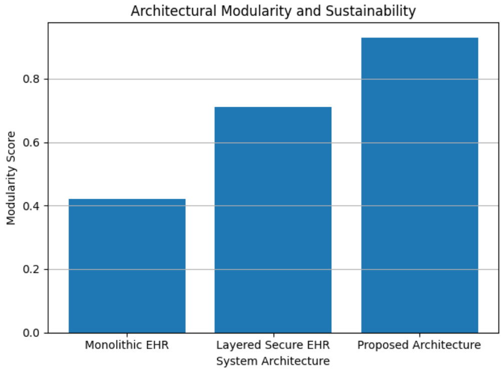


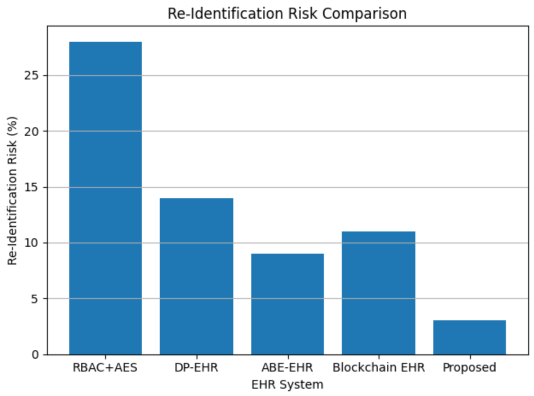
Fig. 17 Interoperability with Evolving Healthcare Standards

Fig. 18 System Modularity Impact on Long-Term Sustainability

This includes an analysis of cryptographic agility, examining the ease with which new post-quantum cryptographic primitives can be integrated as they mature and become standardized, without requiring a complete system overhaul. Furthermore, the evaluation will consider the system's modularity and interoperability with emerging healthcare technologies and data standards, critical for sustaining its relevance and functionality over several decades.

6.5 Comparative Evaluation

This section will juxtapose the proposed system against existing state-of-the-art EHR platforms and privacy-preserving techniques, highlighting its novel contributions in quantum resilience, dynamic privacy adaptation, and fine-grained access control [46]. This comparison will employ both quantitative metrics, such as performance benchmarks and security analyses, and qualitative assessments of architectural flexibility and policy enforcement capabilities.



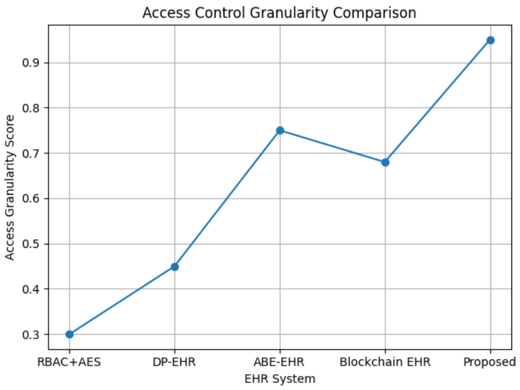
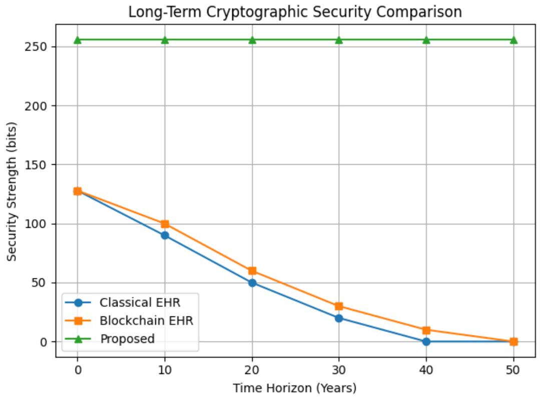


Fig. 19 Re-Identification Risk Comparison Fig. 20 Access Control Granularity Comparison



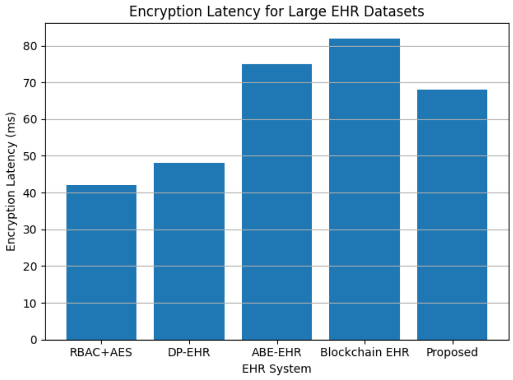


Fig. 20 Long-Term Cryptographic Security Strength Fig. 21 Encryption Latency for Large EHR Datasets

The analysis will specifically emphasize how the proposed system surpasses current solutions in terms of long-term cryptographic security and its ability to maintain privacy guarantees across evolving clinical contexts [42]. This comparative analysis will also consider the integration of distributed ledger technologies, such as blockchain, for enhanced transparency and secure sharing of medical records, as some existing frameworks have explored partitioning EHR data for performance gains [47], [48]. Additionally, the comparative evaluation will analyze the efficiency of encryption and decryption processes for large EHR datasets, particularly those containing extensive imaging files, to demonstrate superior performance [38].

7. KEY CONTRIBUTIONS

The proposed platform distinguishes itself through its multi-layered privacy framework, which integrates quantum-resistant cryptography with context-aware access policies to address the unique challenges of long-term EHR data retention and dynamic clinical environments. This innovative approach ensures robust data confidentiality against future quantum threats while providing the adaptability required for real-time clinical operations and

diverse research applications [1], [49]. Specifically, it pioneers a system capable of field-level encryption, moving beyond the coarse-grained access controls prevalent in current EHR systems [42]. Furthermore, the system's ability to provide measurable privacy-utility-performance trade-offs allows healthcare providers to optimize data access based on specific operational needs without compromising security or regulatory compliance [12].

8. CONCLUSION AND FUTURE WORK

The platform also incorporates a hybrid signature system, combining ECDSA (Elliptic Curve Digital Signature Algorithm) and Dilithium, to fortify defenses against quantum attacks and enhance security and flexibility [2]. This integration of quantum-enhanced blockchain technology significantly improves the confidentiality, integrity, and availability of sensitive healthcare data [2], [8]. Future work will involve real-world deployment and extensive evaluation within a hospital setting to validate its practical utility, scalability, and impact on clinical workflows. Further research will investigate the integration of homomorphic encryption or secure multi-party computation to enable privacy-preserving computations over encrypted EHR data, addressing challenges related to cross-border data sharing and diverse data modalities like genomic and IoT sensor data [12]. Additionally, exploration into blockchain sharding and sidechains could further enhance scalability and transaction processing capacity, particularly for managing large volumes of patient data efficiently [50].

REFERENCES

[1] O. Popoola, M. Rodrigues, J. Marchang, A. Shenfield, A. Ikpehai, and J. Popoola, “An optimized hybrid encryption framework for smart home healthcare: Ensuring data confidentiality and security,” *Internet of Things* , vol. 27, p. 101314, Aug. 2024, doi: 10.1016/j.iot.2024.101314.

[2] S. Alsubai, A. Alqahtani, H. Garg, M. Sha, and A. Gumaei, “A blockchain-based hybrid encryption technique with anti-quantum signature for securing electronic health records,” *Complex & Intelligent Systems* , vol. 10, no. 5, p. 6117, May 2024, doi: 10.1007/s40747-024-01477-1.

[3] A. Alif, K. F. Hasan, J. Laeuchli, and M. J. M. Chowdhury, “Quantum Threat in Healthcare IoT: Challenges and Mitigation Strategies,” *arXiv (Cornell University)* , Dec. 2024, doi: 10.48550/arxiv.2412.05904.

[4] M. SaberiKamarposhti *et al.* , “Post-quantum healthcare: A roadmap for cybersecurity resilience in medical data,” *Heliyon* , vol. 10, no. 10, May 2024, doi: 10.1016/j.heliyon.2024.e31406.

[5] R. Imam and F. Anwer, “Practically adaptable CPABE based Health-Records sharing framework,” *arXiv (Cornell University)* , Mar. 2024, doi: 10.48550/arxiv.2403.06347.

[6] M. N. Alruwaill, S. P. Mohanty, and E. Kougianos, “hChain 4.0: A Secure and Scalable Permissioned Blockchain for EHR Management in Smart Healthcare,” 2025, doi: 10.48550/ARXIV.2505.13861.

[7] R. Patil, “A secure privacy preserving and access control scheme for medical internet of things (MIoT) using attribute-based signcryption,” *International Journal of*

Information Technology , vol. 16, no. 1, p. 181, Oct. 2023, doi: 10.1007/s41870-023-01569-0.

[8] R. Benaich, S. E. Mendili, and Y. Gahi, “Advancing Healthcare Security: A Cutting-Edge Zero-Trust Blockchain Solution for Protecting Electronic Health Records,” *HighTech and Innovation Journal* , vol. 4, no. 3, p. 630, Sep. 2023, doi: 10.28991/hij-2023-04-03-012.

[9] J. Chen, C. Yi, S. D. Okegbile, J. Cai, and X. Shen, “Networking Architecture and Key Supporting Technologies for Human Digital Twin in Personalized Healthcare: A Comprehensive Survey,” *IEEE Communications Surveys & Tutorials* , vol. 26, no. 1, p. 706, Sep. 2023, doi: 10.1109/comst.2023.3308717.

[10] D. Roosan, R. Khan, S. Nirzhor, and F. Hai, “Post-Quantum Cryptography Resilience in Telehealth using Quantum Key Distribution,” *Blockchain in Healthcare Today* , vol. 8, no. 1, Apr. 2025, doi: 10.30953/bhty.v8.379.

[11] A. Ullah, Z. Ullah, S. S. Rizvi, L. Gul, and S. J. Kwon, “Toward blockchain based electronic health record management with fine grained attribute based encryption and decentralized storage mechanisms,” *Scientific Reports* , vol. 15, no. 1, Oct. 2025, doi: 10.1038/s41598-025-17875-5.

[12] S. T. Ha *et al.* , “CertiMed: Identity-Aware Access Framework for Electronic Health Records,” *Research Square (Research Square)* , Sep. 2025, doi: 10.21203/rs.3.rs-7442795/v1.

[13] R. Tertulino, N. Ivaki, and A. H. F. de Morais, “Design a Software Reference Architecture to Enhance Privacy and Security in Electronic Health Records,” *Research Square (Research Square)* , Mar. 2024, doi: 10.21203/rs.3.rs-4006291/v1.

[14] Y. Sharifzadeh, M. Daneshmand, H. Arhamigolmaei, and A. Fallahi, “A Quantitative Landscape Analysis of Blockchain for EHR Security and Interoperability,” *InfoScience Trends* , vol. 2, no. 8, p. 11, Aug. 2025, doi: 10.61882/ist.202502.08.02.

[15] R. Nowrozy, K. Ahmed, and H. Wang, “GPT, Ontology, and CAABAC: A Tripartite Personalized Access Control Model Anchored by Compliance, Context and Attribute,” *arXiv (Cornell University)* , Mar. 2024, doi: 10.48550/arxiv.2403.08264.

[16] R. Walid, K. P. Joshi, and S. G. Choi, “Comparison of attribute-based encryption schemes in securing healthcare systems,” *Scientific Reports* , vol. 14, no. 1, p. 7147, Mar. 2024, doi: 10.1038/s41598-024-57692-w.

[17] H. Guo, W. Li, M. Nejad, and C. Shen, “A Hybrid Blockchain-Edge Architecture for Electronic Health Record Management With Attribute-Based Cryptographic Mechanisms,” *IEEE Transactions on Network and Service Management* , vol. 20, no. 2, p. 1759, Jun. 2022, doi: 10.1109/tnsm.2022.3186006.

[18] T. Dou, Z. Zheng, W. Qiu, and C. Ge, “A Secure Medical Data Framework Integrating Blockchain and Edge Computing: An Attribute-Based Signcryption Approach,” *Sensors* , vol. 25, no. 9, p. 2859, Apr. 2025, doi: 10.3390/s25092859.

[19] A. M. Tawfik, A. Al-Ahwal, A. S. T. Eldien, and H. H. Zayed, “Blockchain-based access control and privacy preservation in healthcare: a comprehensive survey,” *Cluster Computing* , vol. 28, no. 8, Aug. 2025, doi: 10.1007/s10586-025-05308-x.

[20] N. Madhushree, “Blockchain Enabled Secure Electronic Health Records System Storage with Attribute-Based Signature Scheme,” *International Journal for Research in Applied Science and Engineering Technology* , vol. 7, no. 5, p. 2435, May 2019, doi: 10.22214/ijraset.2019.5403.

[21] R. Walid, K. P. Joshi, S. G. Choi, and D. Kim, “Cloud-based Encrypted EHR System with Semantically Rich Access Control and Searchable Encryption,” in *2021 IEEE International Conference on Big Data (Big Data)* , Dec. 2020, p. 4075. doi: 10.1109/bigdata50022.2020.9378002.

[22] R. Tertulino, N. Ivaki, and A. H. F. de Morais, “Design a Software Reference Architecture to Enhance Privacy and Security in Electronic Health Records,” *IEEE Access* , vol. 12, p. 112157, Jan. 2024, doi: 10.1109/access.2024.3441751.

[23] B. Lin, “The Gradient of Health Data Privacy,” *arXiv (Cornell University)* , Oct. 2024, doi: 10.48550/arxiv.2410.00897.

[24] Y. Zhang and M. M. Singh, “Privacy Risks in Health Big Data: A Systematic Literature Review,” *arXiv (Cornell University)* , Feb. 2025, doi: 10.48550/arxiv.2502.03811.

[25] K. Al-hammuri, F. Gebali, and A. Kanan, “ZTCloudGuard: Zero Trust Context-Aware Access Management Framework to Avoid Misuse Cases in the Era of Generative AI and Cloud-based Health Information Ecosystem,” *arXiv (Cornell University)* , Dec. 2023, doi: 10.48550/arxiv.2312.02993.

[26] F. Yadegari and A. Asosheh, “A unified IoT architectural model for smart hospitals: enhancing interoperability, security, and efficiency through clinical information systems (CIS),” *Journal Of Big Data* , vol. 12, no. 1, Jun. 2025, doi: 10.1186/s40537-025-01197-4.

[27] R. Javan, M. Mohammadi, M. Beheshti-Atashgah, and M. R. Aref, “A Scalable Multi-Layered Blockchain Architecture for Enhanced EHR Sharing and Drug Supply Chain Management,” *arXiv (Cornell University)* , Feb. 2024, doi: 10.48550/arxiv.2402.17342.

[28] T. Kuo and H. Yang, “Multi-layer encrypted learning for distributed healthcare analytics,” *Scientific Reports* , vol. 15, no. 1, p. 39442, Nov. 2025, doi: 10.1038/s41598-025-23140-6.

[29] H. Sammangi, A. Jagatha, G. R. Bojja, and J. Liu, “Decentralized AI-driven IoT Architecture for Privacy-Preserving and Latency-Optimized Healthcare in Pandemic and Critical Care Scenarios,” *arXiv (Cornell University)* , Apr. 2025, doi: 10.48550/arxiv.2507.15859.

[30] V. M. Olowo, A. Ahouandjinou, A. F.-X. Ametepe, and P. M. A. F. Kiki, “Secure architecture for distributed governance and automated compliance applicable to mobile IoT,” *HAL (Le Centre pour la Communication Scientifique Directe)* , Oct. 2025, Accessed: Oct. 2025. [Online]. Available: https://inria.hal.science/hal-05318693

[31] A. D. Samala and S. Rawas, “Transforming Healthcare Data Management: A Blockchain-Based Cloud EHR System for Enhanced Security and Interoperability,” *International Journal of Online and Biomedical Engineering (iJOE)* , vol. 20, no. 2, p. 46, Feb. 2024, doi: 10.3991/ijoe.v20i02.45693.

[32] G. N. Brijwani, P. E. Ajmire, M. Junaid, S. A. Charasia, and D. Bhende, “Revolutionizing Healthcare Record Management: Secure Documentation Storage and Access through Advanced Blockchain Solutions,” *arXiv (Cornell University)* , Mar. 2025, doi: 10.48550/arxiv.2503.00742.

[33] H. Szczepaniuk and E. K. Szczepaniuk, “Cryptographic evidence-based cybersecurity for smart healthcare systems,” *Information Sciences* , vol. 649, p. 119633, Sep. 2023, doi: 10.1016/j.ins.2023.119633.

[34] V. Jha, “Blockchain Empowered Personal Health Records: Enhancing Security, Privacy, and Interoperability in Healthcare Management,” *International Journal for Research in Applied Science and Engineering Technology* , vol. 13, no. 4, p. 6145, Apr. 2025, doi: 10.22214/ijraset.2025.69731.

[35] A. S. Fathima and S. M. Basha, “DESIGN AND DEVELOPMENT OF EHR SPECIFIC BLOCK CREATION AND POS CUSTOMIZATION USING HIERARCHICAL INTERDEPENDENCY APPROACH,” *Malaysian Journal of Computer Science* , no. 1, p. 65, Dec. 2023, doi: 10.22452/mjcs.sp2023no1.6.

[36] J. R. Bautista *et al.* , “MediLinker: a blockchain-based decentralized health information management platform for patient-centric healthcare,” *Frontiers in Big Data* , vol. 6, Jun. 2023, doi: 10.3389/fdata.2023.1146023.

[37] E. E. C and S. Nagarajan, “Flexible Access Control Mechanism for Cloud stored EHR using Consortium Blockchain,” *Research Square (Research Square)* , Apr. 2021, doi: 10.21203/rs.3.rs-397642/v1.

[38] R. P. Puneeth and G. Parthasarathy, “Blockchain-Based Framework for Privacy Preservation and Securing EHR with Patient-Centric Access Control,” *Acta Informatica Pragensia* , vol. 13, no. 1, p. 1, Jan. 2024, doi: 10.18267/j.aip.225.

[39] A. Haddad, M. H. Habaebi, E. A. A. Elsheikh, Md. R. Islam, S. A. Zabidi, and F. E. M. Suliman, “E2EE enhanced patient-centric blockchain-based system for EHR management,” *PLoS ONE* , vol. 19, no. 4, Apr. 2024, doi: 10.1371/journal.pone.0301371.

[40] F. Niyasudeen and M. Mohan, “Adaptive Multi-Layered Cloud Security Framework Leveraging Artificial Intelligence, Quantum-Resistant Cryptography, and Systems for Robust Protection in Optical and Healthcare,” *Research Square (Research Square)* , Oct. 2023, doi: 10.21203/rs.3.rs-3408257/v1.

[41] M. I. Mihăilescu, “Security for Data Exchange in a Blockchain Ecosystem,” *Scientific Bulletin of Naval Academy* , no. 2, p. 63, Dec. 2024, doi: 10.21279/1454-864x-24-i2-006.

[42] R. Bose, S. Sutradhar, and S. Roy, “Quantum-Enhanced Blockchain and Digital Twin Integration for Enhanced Healthcare Data Security,” *Research Square (Research Square)* , Aug. 2024, doi: 10.21203/rs.3.rs-4707183/v1.

[43] M. Joshi, K. P. Joshi, and T. Finin, “Attribute Based Encryption for Secure Access to Cloud Based EHR Systems,” Jul. 2018, doi: 10.1109/cloud.2018.00139.

[44] D. P. Chakravarthy, R. Gopi, S. Murugan, and E. Joseph, “Enhancing confidentiality and access control in electronic health record systems using a hybrid hashing

blockchain framework," *Scientific Reports* , vol. 15, no. 1, Aug. 2025, doi: 10.1038/s41598-025-13831-5.

[45] C. Italina, B. Boihaki, and M. Iqbal, "AI-Driven Risk Management Framework for Decentralized IoT Systems: Integrating Blockchain Technology for Enhanced Security and Trust," *TEM Journal* , p. 2050, Aug. 2025, doi: 10.18421/tem143-12.

[46] S. Chenthara, K. Ahmed, and F. Whittaker, "Privacy-Preserving Data Sharing using Multi-layer Access Control Model in Electronic Health Environment," *ICST Transactions on Scalable Information Systems* , vol. 6, no. 22, p. 159356, Jul. 2019, doi: 10.4108/eai.13-7-2018.159356.

[47] R. G. Sonkamble, S. Phansalkar, V. Potdar, and A. M. Bongale, "Survey of Interoperability in Electronic Health Records Management and Proposed Blockchain Based Framework: MyBlockEHR," *IEEE Access* , vol. 9, p. 158367, Jan. 2021, doi: 10.1109/access.2021.3129284.

[48] F. H. Semantha, S. Azam, B. Shanmugam, and K. C. Yeo, "PbDinEHR: A Novel Privacy by Design Developed Framework Using Distributed Data Storage and Sharing for Secure and Scalable Electronic Health Records Management," *Journal of Sensor and Actuator Networks* , vol. 12, no. 2, p. 36, Apr. 2023, doi: 10.3390/jsan12020036.

[49] H. Yi, "Improving cloud storage and privacy security for digital twin based medical records," *Journal of Cloud Computing Advances Systems and Applications* , vol. 12, no. 1, Oct. 2023, doi: 10.1186/s13677-023-00523-6.

[50] A. F. Madni, M. A. Shah, and M. Al-Naeem, "An Investigation of Scalability in EHRs using Healthcare 4.0 and Blockchain," *International Journal of Advanced Computer Science and Applications* , vol. 15, no. 5, Jan. 2024, doi: 10.14569/ijacsa.2024.0150548.