



SPPDE: A Privacy-Preserving Data Exchange for Healthcare EHRs Using ECC Encryption, ZKP Authorization, and Capability-Token Delivery in a Permissioned Blockchain

Tsokwa Daniel¹ and Emmanuel Siman^{2*}

^{1,2}Department of Computer Science, College of Applied and Natural Sciences, Kwararafa University Wukari, Taraba State, Nigeria.

¹Department of Computer Science, Faculty of Computer Sciences, Federal University Wukari, Taraba State, Nigeria.

*Corresponding Author

Emmanuel Siman

Faculty of Engineering,
University Technology
Malaysia, Skudai 81310,
Malaysia.

Article History

Received: 22.11.2025
Accepted: 03.01.2026
Published: 11.02.2026

Abstract: The research presents a Privacy-Preserving Data Exchange (PPDE) framework for electronic health records (EHRs) that integrates elliptic-curve cryptography (ECC), zero-knowledge proofs (ZKPs), and capability tokens on a permissioned blockchain to create a cohesive, policy-compliant data-sharing workflow. In this system, IoT gateways establish ECC-based session keys to encrypt measurements at the edge, while only cryptographic hashes and pointers to the encrypted data are stored on a consortium blockchain, ensuring data confidentiality with tamper-evident integrity and auditable provenance. Healthcare providers issue Access Request Transactions that include ECC signatures and ZKPs to prove policy compliance (such as patient consent and role-based access) without revealing sensitive details. Off-chain ZKPs validate authorization decisions, with on-chain records providing verifiable evidence of conformance and access history, and a capability token is granted to authorize future data access within defined scopes and time windows. The framework emphasizes end-to-end confidentiality, privacy-preserving authorization, and tamper resistance through the blockchain. Our evaluation analyzes network throughput, end-to-end delay, packet delivery ratio, scalability, and energy efficiency, with particular attention to the overhead from blockchain operations, ECC, and ZKP verification. Results show improved privacy and security for EHR data, with only nominal overhead relative to the privacy and integrity gains, and favorable scalability and energy performance in realistic deployments.

Index Terms: Blockchain, Privacy, Security, IoT, EHR, ECC, ZKP, Tokenization Smart Contracts.

Cite this article:

Daniel, T., Emmanuel, S., (2026). SPPDE: A Privacy-Preserving Data Exchange for Healthcare EHRs Using ECC Encryption, ZKP Authorization, and Capability-Token Delivery in a Permissioned Blockchain. *ISAR Journal of Science and Technology*, 4(2), 12-28.

1.0 Introduction

Designing a privacy-preserving data exchange protocol for blockchain-enabled electronic health record (EHR) systems is no small feat. It comes with a host of challenges, including dealing with heterogeneous IoT devices, variable access patterns, stringent confidentiality needs, and the necessity to meet both clinical latency demands and regulatory audit requirements. Once the architectural layers are defined, there is need to ensure that encrypted EHR content is distributed across off-chain repositories. At the same time, fine-grained access decisions are enforced on-chain without exposing patient identities or provider credentials.

To address this, the Privacy-Preserving Data Exchange (PPDE) algorithm seamlessly coordinate ECC-based encryption, zero-knowledge-proof (ZKP) authorization, and capability-token delivery within a permissioned blockchain, all in one organized workflow. IoT gateways establishes ECC session keys, encrypting measurements, and only recording hashes and pointers on the ledger. Healthcare providers then send Access Request Transactions that include ECC signatures and ZKPs, confirming compliance with policies without disclosing any sensitive details. Access-control smart contracts verify signatures, check the proofs against registered policies, and log whether access is granted or denied. When access is granted, they issue short-lived tokens or



key handles instead of raw decryption keys, effectively keeping the data plane separate from the control plane. This section also assesses how sensitive the PPDE is to its design parameters like ZKP complexity, block interval, and token lifetime by looking at network throughput, end-to-end delay, packet delivery ratio (PDR), scalability, and energy efficiency. Finally, the PPDE's behaviour is compared with centralized EHR servers and existing blockchain-based schemes to test whether the promised security and privacy gains are achieved without unacceptable performance consequences.

1.1 Background of the Research

Blockchain technology is essentially a decentralized and distributed ledger system that guarantees transparency, immutability, and security through the use of cryptographic hashing and consensus mechanisms. Since it first emerged with Bitcoin [1]; [2], blockchain has made remarkable strides, paving the way for various platforms like Ethereum and Hyperledger [3]. Each of these platforms brings its own unique features, such as decentralized control, improved security, and the exciting potential for smart contracts [4]. On another front, the Internet of Things (IoT) has revolutionized the healthcare industry by facilitating remote monitoring, telemedicine, and the integration of smart medical devices [5]. In healthcare, the secure sharing of data is absolutely crucial and data is vital for improving patient care outcomes and supporting medical research [6]. Therefore, robust security and privacy measures are essential to safeguard sensitive patient information from breaches and unauthorized access, especially in light of regulatory requirements like HIPAA and GDPR that enforce strict data protection practices [7].

The main contributions of the paper are as follows:

- i. The paper introduces a privacy-preserving data exchange (PPDE) system for electronic health records (EHRs). The system integrates elliptic-curve cryptography (ECC), zero-knowledge proofs (ZKPs), and capability tokens on a permissioned blockchain to ensure secure and confidential data sharing in healthcare environments.
- ii. By utilizing ECC for encryption and ZKPs for proving policy compliance without revealing sensitive information, the framework maintains high levels of data confidentiality and integrity. Only encrypted data is stored on-chain, while cryptographic hashes and pointers to this data are recorded, ensuring tamper-evident integrity.
- iii. The use of ZKPs enables healthcare providers to request access to sensitive data without revealing patient details or their credentials, ensuring that only authorized users can access the data based on predefined roles and policies.
- iv. The framework generates capability tokens that provide temporary, granular access to encrypted data within defined time frames and scope, supporting fine-grained control over EHR data access.
- v. The paper evaluates the framework's performance based on various metrics such as network throughput, end-to-end delay, packet delivery ratio, scalability, and energy efficiency. It demonstrates that the PPDE system provides improved security and privacy with only nominal overhead,

offering scalable performance suitable for realistic deployments.

- vi. The PPDE framework is compared with centralized EHR systems and other blockchain-based healthcare solutions, showing that it offers a better balance of security, privacy, scalability, and efficiency, outperforming centralized systems and traditional blockchain approaches in certain aspects.
- vii. The research highlights that the proposed framework is capable of scaling effectively for large IoT deployments in healthcare, where many devices interact with the system, while still maintaining secure, privacy-preserving access controls.

The programming organization of the framework is structured as follows: Section 3.1 (Research Design) details the integration of Elliptic Curve Cryptography (ECC) and Zero-Knowledge Proofs (ZKP) for secure data encryption and authorization. Section 4.1 (Cryptographic Foundations) explains the cryptographic methods, while Section 4.2 (Smart Contracts) covers access control via smart contracts and capability tokens. Section 4.3 (EHR System Model) outlines the architecture separating the data and control planes. Section 4.4 (PPDE Algorithm) describes the process for managing access requests and token issuance, and Section 4.5 (Performance Evaluation) evaluates system performance in terms of scalability and efficiency. This organization ensures security, scalability, and efficient data sharing in healthcare IoT environments.

2. Literature Review

The section of the paper titled *Literature Review* explores core principles, frameworks, and technologies central to the effective management of healthcare data, with a particular focus on blockchain and privacy-preserving mechanisms. This review emphasizes how blockchain's cryptographic methods and distributed ledger technology provide robust, tamper-proof systems, which are essential for managing Electronic Health Records (EHRs) [8]; [9]. Blockchain's decentralized nature helps ensure that sensitive healthcare data remains secure, transparent, and auditable, aligning with the strict confidentiality demands of healthcare systems. The paper delves into Hyperledger Fabric blockchain models, assessing their ability to meet healthcare regulations while providing necessary privacy protections. This technology uses a permissioned blockchain to ensure that only authorized personnel can access specific data, preventing breaches and unauthorized access [10]. Additionally, the review examines Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) frameworks, which offer dynamic, flexible access management solutions. Both RBAC and ABAC are enhanced by blockchain, facilitating decentralized access control that empowers patients and healthcare providers. These systems allow for more secure and adaptable access to health records, aligning with healthcare regulatory frameworks such as GDPR and HIPAA, which emphasize data privacy and the control patients have over their information. Electronic Health Records (EHRs) are increasingly recognized as essential tools for improving the quality of healthcare. By consolidating medical histories, diagnoses, treatment plans, and more into a digital format, EHRs offer healthcare professionals immediate access to a patient's health information, improving the accuracy of diagnoses and treatment

decisions. EHRs also support healthcare analytics and research, ultimately enhancing patient safety and leading to more patient-centered care. However, the management of EHRs presents challenges, particularly regarding data security and interoperability. Blockchain technology, specifically the use of distributed ledger technology like Ethereum, offers solutions for improving data sharing and securing patient information, but also introduces issues such as scalability and consensus mechanisms [11]; [12]. The paper highlights that access control within EHR systems plays a crucial role in safeguarding patient privacy. Robust security measures ensure that only authorized individuals can access clinical documents, which is achieved through the principle of least privilege. Smart contracts implemented in blockchain systems enforce these access controls, ensuring that only the right parties access sensitive data. A challenge in this process is ensuring compliance with evolving privacy regulations and enabling patients to have control over who accesses their data [13]. The review also addresses the challenges in access control, such as preventing unauthorized access, managing complex user authentication processes, and maintaining privacy regulations. Blockchain's decentralized architecture aids in mitigating these risks by providing tamper-evident logs and transparent access control. Moreover, patients' preferences regarding who can access their data must be carefully captured and applied, a task that introduces further complexity [14].

Access control in decentralized systems requires more sophisticated models. Both centralized and decentralized EHR systems are discussed in the context of hospital networks and health ecosystems. Traditional centralized models, while easy to manage, pose risks like single points of failure, which can lead to insider misuse and decreased system auditability. Blockchain's permissioned models improve upon these issues, providing a more secure, transparent method of managing access. Another critical point covered is the role of IoT (Internet of Things) in healthcare, which significantly expands the scope of data collection through devices like wearables and medical sensors. These IoT systems facilitate real-time monitoring, but they also introduce new security and privacy concerns. The integration of blockchain with IoT healthcare systems helps address these concerns by providing secure data exchanges through blockchain-based access control mechanisms. By combining role-based access control (RBAC) and attribute-based access control (ABAC), the system can dynamically manage access rights according to real-time data and specific attributes of users and devices, enhancing the security of health data sharing [15].

Despite the promising advantages, challenges persist in ensuring secure and efficient access to EHRs, especially in mobile and IoT environments. One challenge is the increasing complexity of managing access control in healthcare systems that involve multiple stakeholders and ever-changing access patterns. To address this, systems like Secure Healthcare Access Control System (SHACS) and various hybrid blockchain models that incorporate biometric verification are proposed. These models improve security by utilizing biometric data to identify patients and grant access based on their unique attributes, mitigating the risks associated with lost private keys and unauthorized access [16]; [17]. The application of blockchain technology is identified as a potential game-changer for solving these access control challenges. Blockchain offers a decentralized approach to data sharing that

balances data privacy with the need for accessibility. Hybrid architectures, combining blockchain with edge nodes, are explored for managing EHR data. These systems use blockchain to maintain an immutable log of access events while off-chain systems handle the storage and access control of data. Blockchain's tamper-proof nature ensures that any unauthorized access is detected and logged, providing strong evidence for compliance with privacy regulations [18]. The paper also addresses the persistent security challenges that arise in healthcare, such as the lack of robust auditing mechanisms. The absence of such mechanisms can leave data vulnerable to unauthorized changes that may go unnoticed, leading to security breaches. To address this, Purpose-Based Access Control (PBAC) combined with smart contracts is proposed, ensuring that only authorized users can view or modify sensitive health information [19]. In examining Role-Based Access Control (RBAC), the paper discusses its importance in maintaining a structured approach to managing user permissions within healthcare systems. Blockchain-enhanced RBAC ensures that healthcare professionals, based on their roles, have appropriate access to EHRs while maintaining security and compliance. This decentralized approach allows for more flexible and scalable access control, particularly in large healthcare networks that span multiple organizations. Attribute-Based Access Control (ABAC) is another framework explored, particularly for scenarios where access to data is contingent on attributes like the role of the healthcare provider, time of access, and location. When integrated with blockchain, ABAC can create tamper-proof logs and facilitate the sharing of healthcare data across multiple institutions without compromising security. This approach is highly adaptable, allowing for real-time data sharing based on policy and user attributes, while maintaining compliance with regulations such as GDPR and HIPAA [20]. The paper further explores privacy-preserving techniques within blockchain, such as Zero-Knowledge Proofs (ZKPs), homomorphic encryption, and federated learning, which enable data to be shared and processed without revealing sensitive details. ZKPs, for instance, allow healthcare providers to verify that they have the correct authorization to access data without disclosing the data itself. Homomorphic encryption allows for encrypted data to be processed without decryption, ensuring that the data remains secure throughout the computation process. Federated learning enables machine learning models to be trained across decentralized healthcare systems without transferring raw data, thus enhancing privacy and security [21]; [22]. Moreover, differential privacy and other privacy-preserving methods are discussed as key enablers of secure data sharing in healthcare. These techniques are especially useful in IoT environments, where large volumes of health data are generated and shared between multiple parties. Sharding and dynamic load distribution are highlighted as mechanisms to improve scalability in high-volume healthcare systems [23]. Finally, the review touches on the importance of compliance with healthcare regulations, including HIPAA and GDPR. Blockchain's transparent nature supports compliance by providing an immutable record of access events, ensuring that patient data is handled according to established privacy rules. Automated compliance mechanisms can help healthcare providers manage complex regulatory requirements more efficiently, while ensuring that patient rights are protected [24].

2.1 Summary of Related Literature Review Work

Table 2: Summary of Related Work

Study	Approach & Details	Decentralized	Key Findings/Contribution	Limitations
Abdellatif et al., 2021	Hybrid blockchain-based architecture for IoMT smart healthcare systems.	Yes	Improved efficiency and security through Federated Learning (FL) and Differential Privacy (DP).	Challenges in data integration, interoperability, and maintaining robust security measures.
Sammata & Parthiban, 2022	Hyperledger-based EHR management with SIMON block cipher and deep learning diagnosis.	Partially	Enhanced security and diagnosis accuracy through encrypted data sharing and AI integration.	High computational overhead for encryption and diagnosis integration.
Alsamhi et al., 2024	Leveraging FL for decentralized AI model training in healthcare systems.	Yes	Preserved patient privacy while enabling collaborative AI training.	Potential for high latency and computational inefficiency in real-time applications.
Gadiraju et al., 2024	Use of EOSIO blockchain for secure storage of healthcare IoT data.	Yes	High performance and scalability for IoT data storage with enhanced throughput.	Resource limitations of IoT devices create barriers to security and privacy improvements.
Madavarapu et al., 2024	IoT-based wearable health monitoring device leveraging blockchain for secure data analytics.	Yes	Improved tracking and monitoring using IoT sensors with blockchain-enhanced privacy.	Limited computational capabilities of IoT devices hinder advanced analytics.
Bhaskar & Kumaraswamy, 2024	Nano-integrated wearable devices for real-time healthcare monitoring.	Partially	Advanced accuracy in medical data collection and diagnostics using wearable technology.	Scalability and high energy consumption remain significant challenges.
Alam et al., 2023	Blockchain integrated with IoT for EHR monitoring using cryptographic techniques like AES and ZKP.	Yes	Enhanced data privacy, interoperability, and security for EHR systems.	Complexity in ensuring scalability and seamless integration with legacy systems.
Egala et al., 2021	Blockchain-based secure EHR system with Proof of Trust (PoT) consensus and Selective Ring Access Control (SRAC).	Yes	Efficiency in secure and private access to EHR with low energy consumption.	Limited computation power of IoT devices poses challenges.
Yang & Zhang, 2024	Blockchain framework for EHR sharing using smart contracts and IPFS.	Yes	Trusted medical data sharing with privacy-preserving mechanisms and secure access control.	Requires improvements in scalability and reduction in latency.
Zaman et al., 2022	Survey of enabling technologies (IoT, Blockchain, ML) for Internet of Health Things (IoHT).	Partially	Comprehensive review of IoHT technologies addressing performance, security, and advancements.	Lacks detailed practical implementation and comparative analysis.
Ullah et al., 2024	Auditing EHR access via blockchain-enabled policy-based access control (PBAC).	Yes	Enhanced compliance with GDPR and HIPAA through detailed audit logs.	Increased system complexity for real-time auditing.

3. Research Methodology

In this section, the research outlines a methodology designed to meet the research goals. It details the main operational framework, the steps involved in creating the Privacy-Preserving Data Exchange (PPDE) algorithms, as well as the validation approach, which includes the simulation tools, environment, and performance evaluation. The entire framework is broken down into three key stages. The first stage sets the objectives, reviews current literature on blockchain-enabled EHR systems, pinpoints gaps in privacy, scalability, and access control, and formulates the problem

statement. The second stage focuses on the research design and the development of the blockchain-IoT architecture, along with the PPDE algorithms for secure and confidential data sharing. The next stage outlines the implementation and simulation setup, detailing the selected platform (Hyperledger Fabric), configurations for MATLAB and Hyperledger Caliper, and the key performance indicators (KPIs) used to evaluate latency, integrity, and privacy. The results from this stage provide a performance evaluation that highlights the main technical contributions of the study. The summary of the complete research methodology represented in Figure 3.1 below.

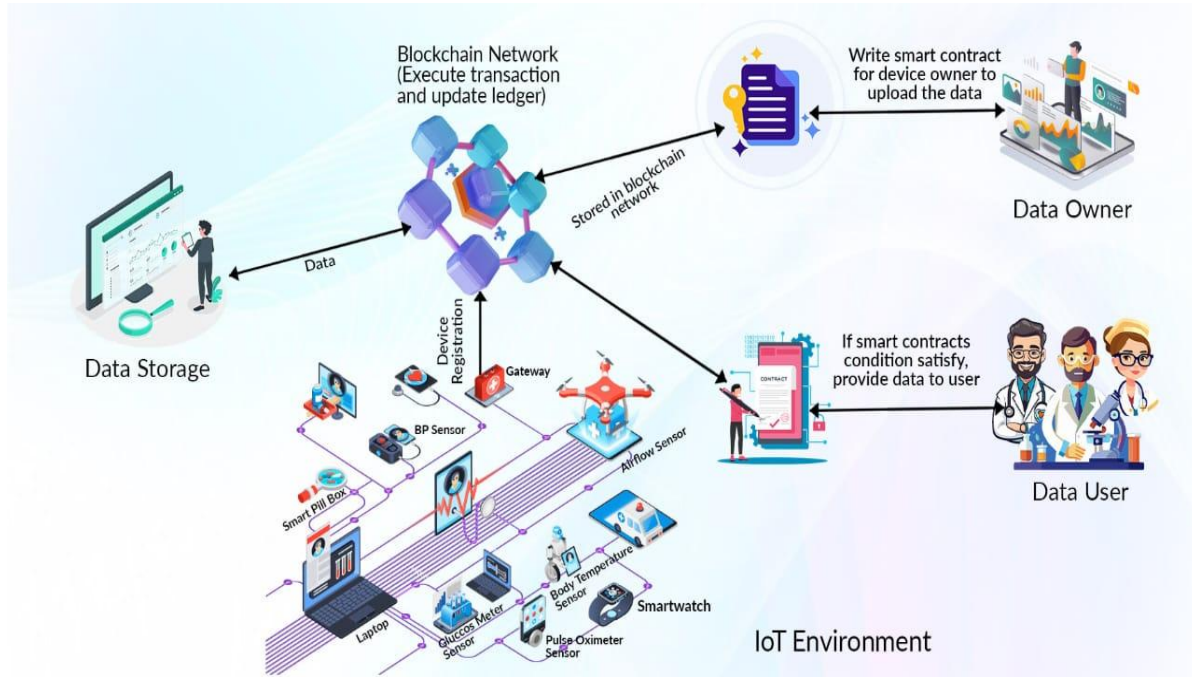


Figure 3.1: Proposed Model Architecture

3.1 Research Design and Development

In this section, the system model for the proposed blockchain-enabled Electronic Health Record (EHR) framework is introduced. Patients are viewed in this research as the primary owners of data, while IoT devices, gateways, and hospital information systems are responsible for generating and sending clinical data to an off-chain EHR repository. Each record is secured through encryption using symmetric keys that are derived from an ECC-based key agreement, and the study ensures that its hash, metadata, and access policy are anchored on the blockchain. Blockchain validator nodes, such as consortium hospitals, maintain a permissioned ledger and run smart contracts that enforce fine-grained access control and PPDE policies. Nodes are deemed trusted participants if they possess valid cryptographic credentials and operate within

the established permissioned network. When access requests come in, the PPDE mechanisms work to ensure secure policy evaluation.

3.2 Privacy-Preserving Data Exchange (PPDE) Mechanism

In this proposed framework, the PPDE mechanism plays a crucial role in securely sharing electronic health records (EHR) among data owners (patients), data producers, which include IoT gateways and hospital systems, and authorized data consumers, such as clinicians and researchers. When an IoT gateway or a hospital information system creates new clinical data, it first sets up a secure connection to the EHR repository and the key-management service then obtains the relevant access policy and cryptographic material. Additionally, any updates to patient consent information and policies are sent to the PPDE layer, ensuring that both producers and consumers have a unified understanding of permissions.

Blockchain-Enhanced EHR Sharing Architecture

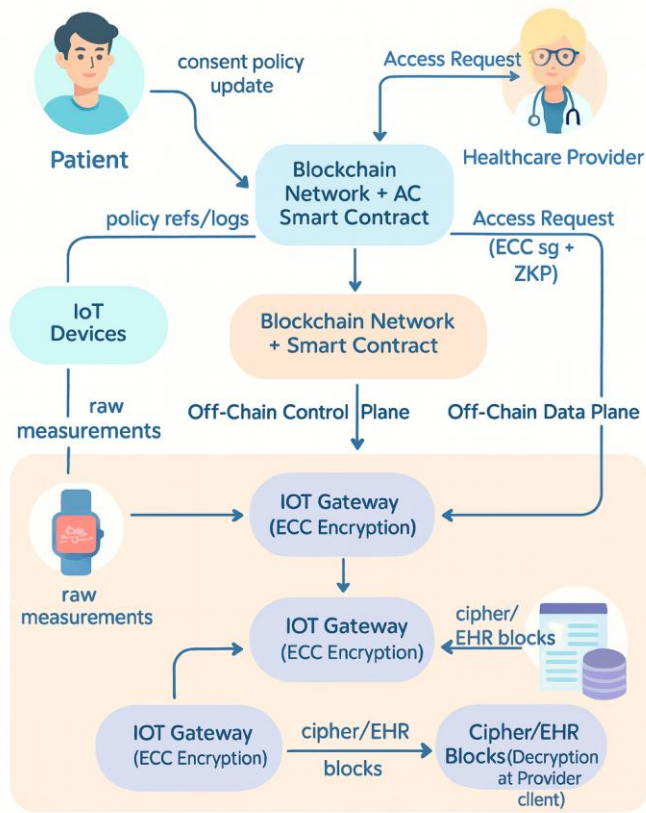


Figure 3.1: Layered Framework Architecture for Blockchain-Enhanced Privacy-Preserving EHR Access Control

Figure 3.1 showcases the proposed framework architecture, featuring a layered design that distinctly separates the data plane where encrypted EHR content is stored from the control plane, which enforces blockchain-based access control. In the data plane, various IoT devices continuously gather patient measurements and send them to an IoT gateway. This gateway generates session keys using ECC, encrypts the data, and only stores the ciphertext in distributed EHR repositories or IPFS. Meanwhile, the blockchain only receives hashes and location pointers to ensure integrity. In the control plane, access-control smart contracts manage EHR hashes, policy references, and minimal metadata. They also facilitate the registration of patients and providers, allow for policy updates, verify ECC signatures, and validate ZKP-based proofs of authorization. When a healthcare provider seeks access, they submit an Access Request Transaction that includes their digital signature and ZKP to the blockchain. The AC-SC then checks the validity of the signature, the correctness of the proof, and the consistency of the policy. If any of these checks fail, a deny event is logged. Conversely, a successful verification triggers the logging of a grant decision and the issuance of a short-lived capability token or decryption key handle that the provider then uses off-chain to retrieve and decrypt the corresponding encrypted EHR.

Blockchain-based EHR Access Request and Token Issuance Flow

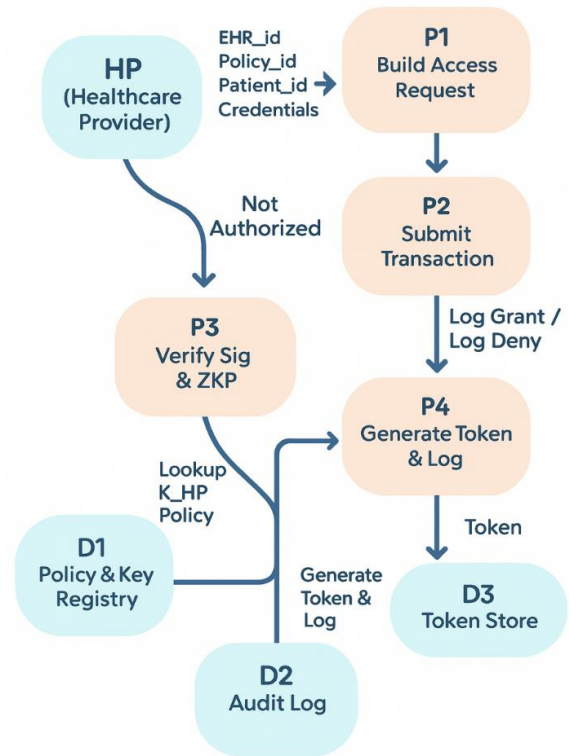


Figure 3.2 Level-1 Data Flow Diagram of the Privacy-Preserving Data Exchange (PPDE) Algorithm

The PPDE workflow which aligns with the data flow shown in Figure 3.2, proceeds as follows: newly generated EHR data is encrypted using asymmetric session key derived from ECC-based key agreement. The ciphertext is stored off-chain, while the corresponding hash, metadata, and policy identifier are anchored on-chain through a smart-contract transaction. When an authorized requester submits an access request, the PPDE smart contract verifies their identity and checks for policy compliance. It then issues a short-lived access token and releases the encrypted session key (or a re-encrypted key) through proxy re-encryption. Only those requesters who have valid cryptographic credentials and the right policy attributes can access the plaintext. By regularly re-evaluating policies and keys, PPDE maintains stable, fine-grained access control even as participants join or leave and as consent preference changes.

3.3 Simulation Evaluation

The proposed PPDE is evaluated through simulations that utilize a variety of performance metrics aimed at assessing the efficiency, responsiveness, and stability of the blockchain-enabled EHR system. The key metrics are as follows:

Transaction throughput: This refers to the number of application-level transactions (like EHR writes or authorized reads) that are successfully recorded on the ledger within a specific timeframe.

End-to-end transaction latency: This is the total time taken from when a client submits a transaction (or access request) to when that transaction is finally committed and visible to authorized users.

Successful access probability: This metric represents the ratio of access requests that are completed successfully and comply with policy, compared to the total number of access requests submitted in the network.

Packet Delivery Ratio (PDR): PDR is calculated as the ratio of PPDE-related messages that are successfully delivered (including requests, proofs, decisions, and tokens) to the total number sent. A high PDR signifies a reliable control plane, ensuring that access decisions and tokens are not lost, which is vital for maintaining continuity of care.

Energy Efficiency: This metric assesses the computational and communication overhead caused by the blockchain, ECC operations, and ZKP verification, particularly on resource-limited IoT gateways.

Ensuring data integrity: Check if any committed block or EHR transaction has been altered or does not pass the hash-chain verification.

Evaluating regulatory compliance: Map framework controls (like PPDE, RBAC, logging, consent management, and key management) with a checklist derived from relevant standards and regulations. Then, calculate the overall compliance level as a total score and highlight any controls that are not compliant.

Table 3.1 Simulation parameters and their values

Parameter	Value
Blockchain platform	Hyperledger Fabric
Consensus mechanism	Delegated Proof of Stake (DPoS) and sharding
Simulation tools	MATLAB, Hyperledger Caliper
Cryptographic techniques	AES, Zero-Knowledge Proofs (ZKP)
IoT device density	50, 100, 150, 200 devices
Network load	Low, Medium, High
Transaction latency	≤ 500 ms
Transaction throughput	≥ 1000 transactions per second
Frequency band	5 GHz
Energy efficiency	Monitored across nodes
Data storage	IPFS (off-chain storage)
Privacy metrics	Compliance with GDPR and HIPAA
Evaluation metrics	Scalability, privacy, resilience
Smart contract language	Go (chaincode)
Simulation time	60 minutes per scenario

Table 3.1 provides a summary of the key configuration parameters used to evaluate the proposed blockchain-enabled EHR framework. A permissioned network based on Hyperledger Fabric is set up, featuring smart contracts developed in Go chaincode and assessed using Hyperledger Caliper. For post-processing of performance logs, MATLAB is utilized. The system's cryptographic security is ensured through AES for data confidentiality and ZKP for privacy-preserving authorization, with data objects stored off-chain in IPFS, while only hashes and metadata are anchored on-chain. To stress-test the workload, the study varies the density of IoT devices (ranging from 50 to 200) and adjust network load levels (low, medium, high). Additionally, transaction arrival patterns is fine-tuned to determine if the system can sustain a target throughput of at least 1000 transactions per second, with end-to-end latency kept under 500 ms. Other parameters, such as the wireless frequency band, client concurrency, and simulation duration per scenario (60 minutes), help define the communication and temporal context for each run. The evaluation metrics reflect privacy and resilience

requirements, jointly assessing the regulatory compliance and robustness of the integrated PPDE mechanisms.

4. Privacy-Preserving Data Exchange (PPDE) Algorithm

4.1. Cryptographic and Access-Control Foundations of the Proposed Framework

This section formalizes the cryptographic and access-control foundations of the proposed framework, building directly on ECC and ZKP as specified in Objective (i).

4.1.1 Cryptographic Foundations for Data Integrity and Security

i. Hash Functions

Let $H(\cdot)$ be a collision-resistant hash function. For each EHR record:

$$H(EHR) = h \quad (4.1)$$

The blockchain stores h and metadata. Any change to the off-chain EHR content produces a different hash, enabling integrity verification.

ii. Elliptic Curve Cryptography (ECC)

Each entity i has private key k_i and public key $K_i = k_i G$, where G is a base point on elliptic curve $E(F_q)$.

Encryption and decryption are abstracted as:

$$\begin{aligned} E_k(M) \\ = C(\text{encryption of message } M \text{ with key } k) \end{aligned} \quad (4.2)$$

$$\begin{aligned} D_k(C) \\ = M(\text{decryption of ciphertext } C \text{ with key } k) \end{aligned} \quad (4.3)$$

Digital signatures use ECC-based algorithms (e.g. ECDSA), with correctness implying:

$$\text{Verify}_{K_i}(H(M), \sigma) = \text{true} \Rightarrow \sigma = \text{Sign}_{k_i}(H(M)) \quad (4.4)$$

iii. Zero-Knowledge Proofs (ZKP)

ZKPs allow a prover to show that a statement S is true (e.g. policy satisfied) without revealing the witness w . We denote:

$$\text{ZKP}(M) = P_{\text{verify}}(M) \quad (4.5)$$

indicating that verification succeeds if, and only if, the asserted predicate over hidden attributes holds.

4.1.2 Consensus Mechanisms for Blockchain Validation

Let the blockchain state be a sequence of blocks $b_1, b_2, \dots, b_n$, each containing a set of transactions T_j .

i. Proof of Work (PoW) (conceptual reference):

Nodes seek a nonce such that:

$$\text{hash}(\text{header} \parallel \text{nonce}) < \text{target}$$

ii. Proof of Stake (PoS) (or permissioned variant):

The probability of validator v_i producing the next block is:

$$P(v_i) = \frac{\text{stake}_i}{\sum_j \text{stake}_j} \quad (4.6)$$

In this context, a **permissioned, energy-efficient variant** (e.g. Raft) is used for the healthcare consortium.

4.1.3 Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC)

Access rights are formalized through RBAC and ABAC policies encoded in smart contracts.

RBAC

Let u be a user and r a role. Access decision:

$$\begin{aligned} \text{Access}(u, r) \\ = \{\text{Grant}, \text{if } u \text{ has role } r \text{ Deny}, \text{otherwise} \end{aligned} \quad (4.7)$$

ABAC

Let p be a patient, $time$ be the access time, and $conditions$ a set of attribute predicates.

$$\begin{aligned} \text{Access}(u, p, \text{time}, \text{conditions}) \\ = \{\text{Grant}, \text{if all conditions are satisfied Deny}, \text{otherwise} \end{aligned} \quad (4.8)$$

ZKPs ensure that satisfaction of conditions can be proven without revealing the attributes themselves.

4.2 Smart Contract Logic for EHR Access Control

Smart contracts encode the access-control rules as deterministic functions:

$$\begin{aligned} \text{If } \text{AccessRequest}(u, p, s, \pi) \text{ is valid} \\ \Rightarrow \text{Grant}(u, p) \end{aligned} \quad (4.9)$$

Validity requires:

- i. $\text{Verify}_{K_u}(H(\text{ART}), \sigma_u) = \text{true}$
- ii. $\text{ZKP_Verify}(s, \pi) = \text{true}$
- iii. Policy reference in s is active and not revoked by patient p .

The contract then creates an audit entry and triggers PPDE token generation.

4.3 Blockchain-Based EHR System Model

Let:

- i. denote the blockchain as an ordered set of blocks.
- ii. Each block b_j contains transactions including access requests and policy updates.
- iii. $A(u, p)$ denote an abstract access request from user u for patient p .

We write:

$$\begin{aligned} T = \{b_1, b_2, b_3, \dots, b_n\} A(u, p) = \text{SC_Logic}(u, p, s, \pi) \\ \in \{\text{Grant}, \text{Deny}\} \end{aligned} \quad (4.10)$$

The security of the framework follows from:

- i. Cryptographic guarantees of ECC and hash functions (confidentiality, integrity, authenticity).
- ii. Zero-knowledge properties of the ZKP scheme (completeness, soundness, zero-knowledge).
- iii. Consensus properties of the permissioned blockchain (liveness and safety).

Together, these ensure that only authorized, policy-compliant requests result in decryption capabilities, and all decisions are immutably recorded.

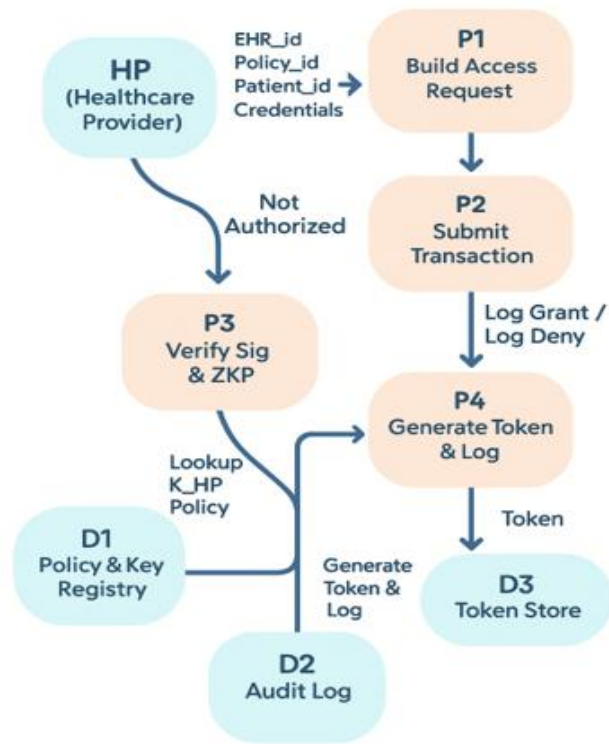


Figure 4.1: Level-1 Data Flow Diagram of the Privacy-Preserving Data Exchange (PPDE) Algorithm

Figure 4.1 breaks down the PPDE into four key processes: First, P1 takes the healthcare provider's input like EHR_id, policy_id, patient_id, and credentials and uses that information to create an access statement and a zero-knowledge proof (ZKP), and forms a signed access request transaction (TX_{req}). Next, P2 sends this

transaction (TX_{req}) over to the blockchain. In P3, the system checks the provider's signature and the ZKP against the registered policies and public keys stored in D1 (Policies & Keys). If any check fails, a deny event is recorded in D2 (Audit Log) and "Not authorized" is returned to the provider. However, if the check is successful, P4 steps in to generate a short-lived access token, records the grant decision in D2, saves the token in D3 (Token Store), and sends the token back to the provider. With this token, the provider can then access the corresponding encrypted EHR off-chain.

4.4 Privacy-Preserving Data Exchange (PPDE) Algorithm

In Algorithm 4.1, the healthcare provider (HP) first constructs an access request by forming a public statement (s) that specifies the target record, the applicable policy, and the patient identifier, then assembling a private witness (w) from its credentials and attributes. Using (s) and (w), HP generates a zero-knowledge proof (pi) that it satisfies the policy, builds the Access Request Tuple (ART = (s, pi)), and signs its hash with its ECC private key to obtain (sigma_{HP}). The resulting transaction (TX_{req}) = (ART, sigma_{HP}) is submitted to the access-control smart contract (AC-SC) on the blockchain, which first verifies the signature with HP's public key; if this fails, a deny event with reason "Invalid signature" is logged and the algorithm returns "Not authorized". If the signature is valid, AC-SC runs the ZKP verifier on ((s, pi)); failure at this stage leads to a deny log with reason "Policy not satisfied" and the same "Not authorized" outcome. Only when both checks succeed does AC-SC generate a short-lived access token bound to the EHR identifier, HP identity, and an expiry time, record a grant event in the audit log, and return this token, which HP can then use off-chain to obtain or unwrap the decryption key for the encrypted EHR.

Algorithm 4.1: Privacy-Preserving Data Exchange (PPDE)

Input: EHR_id, Patient P, Healthcare Provider HP

Output: Access token or denial

```

1: // Step 1 – Request Construction
2: HP prepares statement s = (EHR_id, policy_id, patient_id)
3: HP builds witness w from its credentials/attributes
4:  $\pi \leftarrow \text{ZKP\_Prove}(s, w)$  // Zero-knowledge proof of policy satisfaction
5:  $\text{ART} \leftarrow (s, \pi)$ 
6:  $\sigma_{\text{HP}} \leftarrow \text{Sign}_{\{k_{\text{HP}}\}}(H(\text{ART}))$ 
7: // Step 2 – Submission to Blockchain
8: Submit transaction  $\text{TX}_{\text{req}} = (\text{ART}, \sigma_{\text{HP}})$  to AC-SC
9: // Step 3 – On-chain Verification
10: AC-SC verifies signature: if  $\text{Verify}_{\{K_{\text{HP}}\}}(H(\text{ART}), \sigma_{\text{HP}}) = \text{false}$  then
11:   Log_Deny(HP, EHR_id, reason = "Invalid signature")
12:   return "Not authorized"
13: end if
14: if  $\text{ZKP\_Verify}(s, \pi) = \text{false}$  then
15:   Log_Deny(HP, EHR_id, reason = "Policy not satisfied")
  
```

```

16:   return "Not authorized"
17: end if
18: // Step 4 – Capability Generation
19: token ← Gen_Access_Token(EHR_id, HP_id, expiry_time)
20: Log_Grant(HP, EHR_id, token)
21: return token

```

4.5 Performance Evaluation of the PPDE Mechanisms

This section takes a closer look at how well the proposed Blockchain-Enhanced EHR Access Control system performs, especially focusing on the PPDE algorithm, ECC-based cryptography, and ZKP-based authorization. The aim here is to evaluate how effectively the framework ensures secure and privacy-preserving access to electronic health records (EHR) in real-world healthcare IoT scenarios. The assessment considers network throughput, end-to-end delay, packet delivery ratio (PDR), scalability, and energy efficiency, with emphasis on the extra cost introduced by blockchain, ECC, and ZKP verification.\

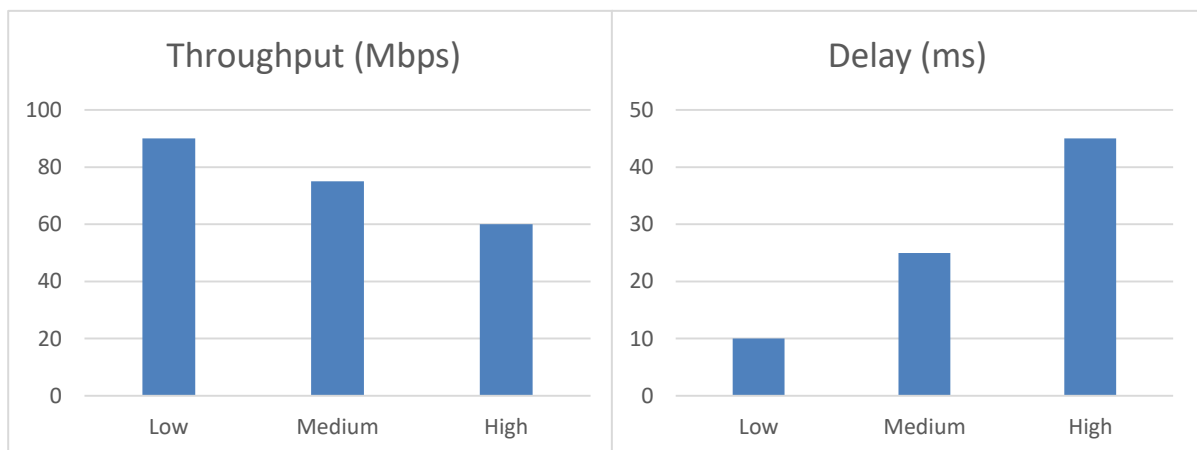
4.6 Results and Discussion

The proposed system demonstrates several key advantages over traditional centralized EHR access-control approaches. Network throughput remains higher as concurrent users increase, thanks to Fabric's Raft consensus enabling rapid block production and confirmation, coupled with efficient batching of PPDE requests; the modest per-transaction overhead from ECC and ZKP computations does not dominate throughput for the tested workloads. End-to-end delay stays within acceptable bounds for low to moderate traffic, with the main contributors being block confirmation and ZKP verification, and it grows gradually with higher traffic due to validator queuing, yet remains well below PoW-based healthcare blockchains; further reductions are achievable through tuning block size, interval, and off-chain proof aggregation. Packet delivery ratio is effectively unity across scenarios, as consensus replication and immutable audit logs mitigate the risk of lost or inconsistent access decisions that can plague centralized servers. Scalability is achieved through near-linear throughput growth until validator CPU becomes the bottleneck, with off-loading of raw EHR content to IPFS and

storing only hashes and control data on-chain preventing rapid ledger growth and preserving performance under high device densities. Energy efficiency benefits from using Raft over PoW, with most ECC and ZKP processing occurring at gateways and validators rather than constrained sensors; the resulting energy footprint per successful access is lower than PoW-based blockchains and comparable to optimized permissioned ledgers, while delivering stronger privacy guarantees via ZKPs.

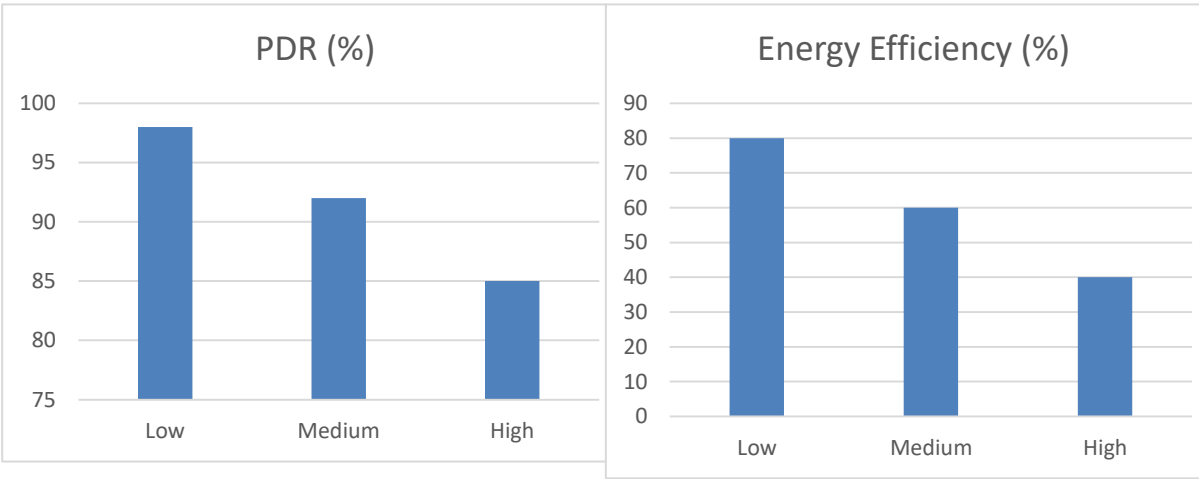
4.7 Comparison with Existing Systems

The proposed blockchain-enhanced EHR access-control framework is compared with traditional centralized EHR systems and representative blockchain-based healthcare solutions such as MedRec and Hyperledger Fabric. The study compares three approaches to EHR access control and finds that a blockchain-enabled design offers the best balance: centralized EHR access is easy to manage but creates a single point of failure, it is prone to insider misuse, and becomes less auditable and resilient as load grows; MedRec-style PoW systems give decentralization and tamper-resistant logs but suffer from high latency and energy use, making them unsuitable for interactive healthcare tasks, whereas a Hyperledger Fabric-based framework with Raft consensus delivers higher throughput, lower delay, and lower energy cost, with strong privacy when combined with PPDE and ZKPs; Hyperledger Fabric, especially when paired with off-chain storage and lightweight PPDE transactions, scales better for large IoT deployments and heavy request rates while still offering fine-grained, auditable access control comparable to Ethereum. Overall, integrating Fabric, ECC, and ZKPs within the PPDE framework provides a practical balance of security, privacy, performance, and energy efficiency for large-scale, blockchain-enabled EHR access control.



a: Network Throughput vs Traffic Level

b: End-to-End Delay vs Traffic Level



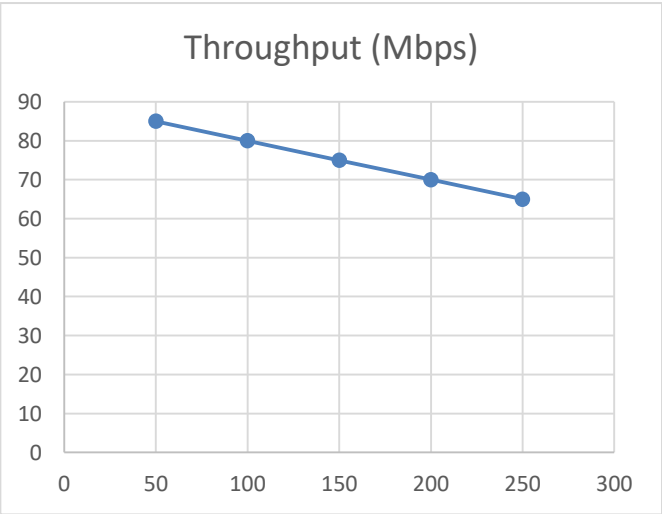
c: Packet Delivery Ratio (PDR) vs Traffic Level

d: Energy Efficiency vs Traffic Level

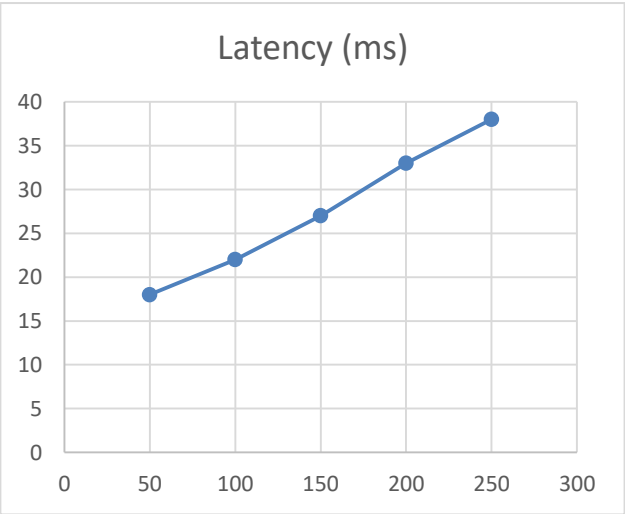
Figure 4.2: Performance of the proposed blockchain-enhanced EHR access-control system under varying traffic levels.

Figure 4.2, performance of the proposed blockchain-enhanced EHR access-control system under low, medium, and high traffic levels. Under low traffic, the system achieves about 90 Mbps throughput with ≈ 10 ms end-to-end delay, $\approx 98\%$ packet delivery ratio (PDR), and $\approx 80\%$ energy efficiency. As traffic increases to medium and high levels, throughput decreases to roughly 75 Mbps and 60 Mbps, while delay rises to ≈ 25 ms and 45 ms due to higher

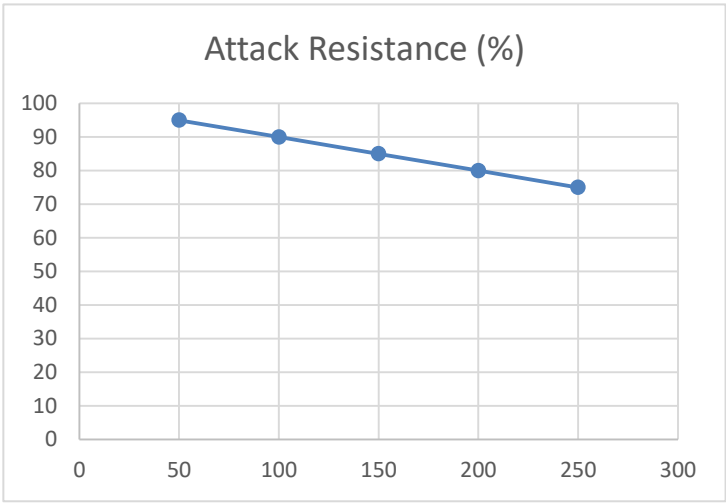
transaction and verification load. PDR remains above 85% across all scenarios, indicating robust reliability even under stress. Energy efficiency drops from $\approx 80\%$ to $\approx 60\%$ and $\approx 40\%$ as validator and gateway utilisation increases, but stays acceptable for IoT-centric deployments, confirming that the ECC+ZKP design and PPDE workflow do not impose prohibitive overheads at scale.



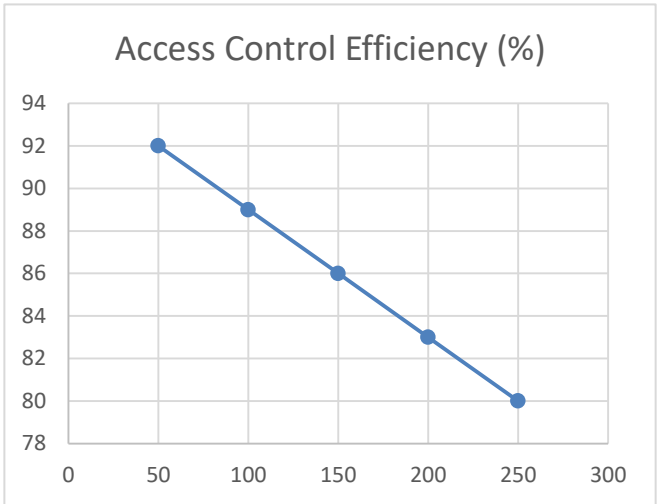
a: Scalability – Throughput vs Number of Devices



b: Scalability – Latency vs Number of Devices



c: Security – Attack Resistance vs Number of Devices

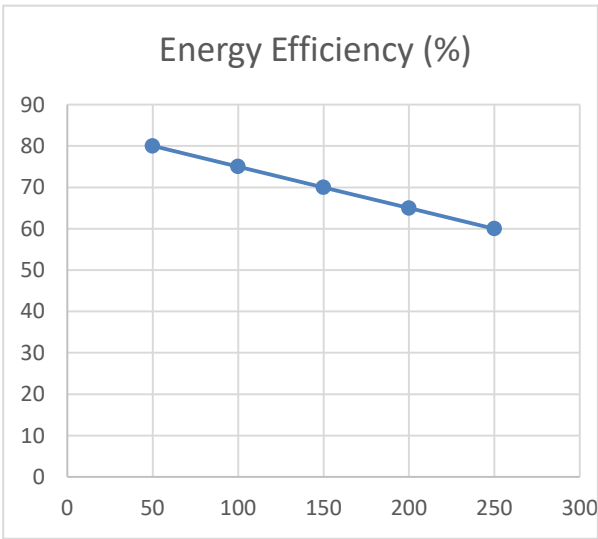


d: Security – Access Control Efficiency vs Number of Devices

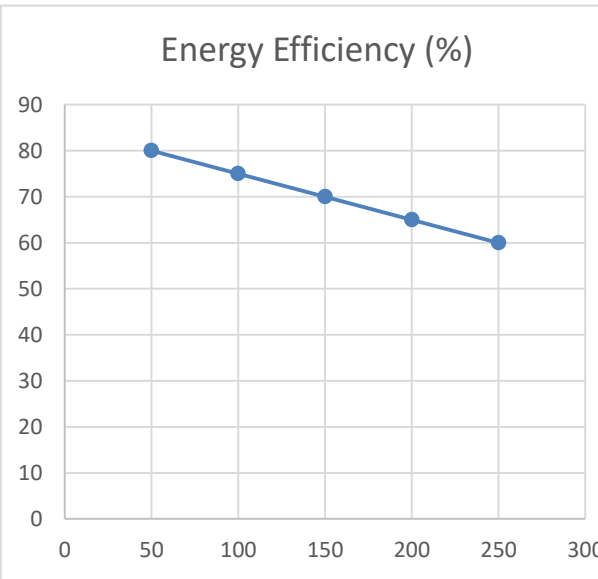
Figure 4.3: Scalability and security of the proposed blockchain-enhanced EHR access-control system as the number of IoT devices increases.

Figure 4.3, scalability and security of the proposed blockchain-enhanced EHR access-control system as the number of IoT devices increases from 50 to 250. Throughput declines gradually from about 85 Mbps to 65 Mbps while latency rises from roughly 18 ms to 38 ms, reflecting the extra consensus and smart-contract load as more PPDE transactions are processed but without abrupt degradation. On the security side, attack resistance decreases from

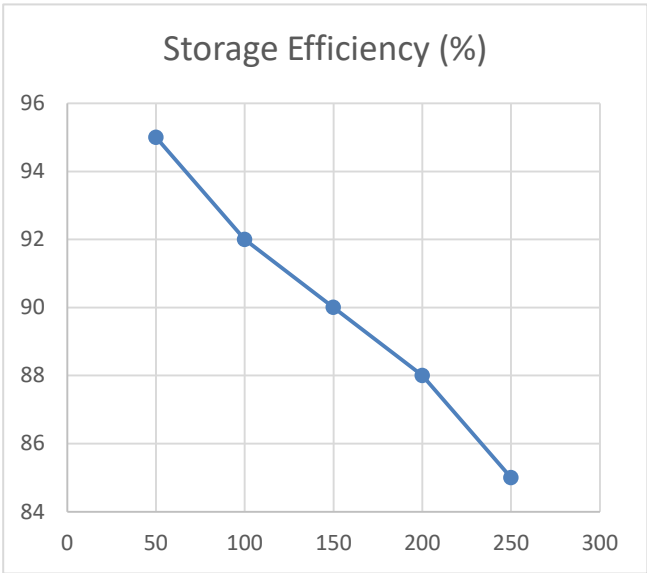
roughly 95% to 75% and access-control efficiency from about 92% to 80% as contention at validators and gateways increases, yet both metrics remain relatively high. These simulation results suggest that the ECC+ZKP-based design scales to higher device densities without catastrophic loss of performance, security, or access-control accuracy, although real deployments would still require empirical validation.



a: Energy Efficiency vs Number of Devices



b: Data Storage Cost vs Number of Devices



C: Storage Efficiency vs Number of Devices

Figure 4.4: Energy and storage behaviour of the proposed blockchain-enhanced EHR access-control system as the number of IoT devices increases

Figure 4.4, energy and storage behaviour of the proposed blockchain-enhanced EHR access-control system as the number of IoT devices increases. Energy efficiency declines from about 80% to 60% as devices grow from 50 to 250, reflecting the extra cryptographic and consensus workload at gateways and validator nodes, but remains relatively high, consistent with the use of Raft and lightweight ECC/ZKP primitives. The average storage cost per

device falls from roughly \$50 to \$30 as fixed blockchain and IPFS overheads are amortised over more nodes and off-chain deduplication becomes more effective. Storage efficiency decreases slightly from about 95% to 85% because a larger share of total capacity is consumed by hashes, metadata, and replicated audit logs, yet it stays high enough to support long-term EHR retention using IPFS with on-chain anchoring.

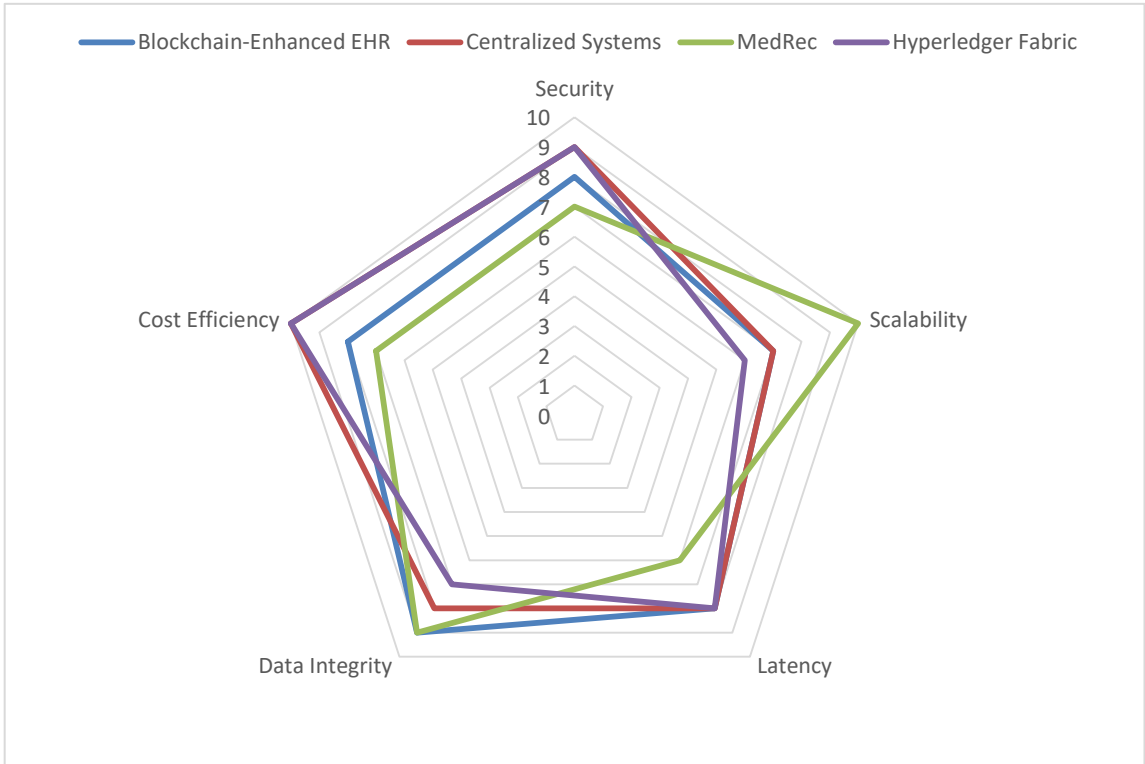


Figure 4.5: Normalized comparison of the proposed Blockchain-Enhanced EHR access-control framework with centralized EHR systems, MedRec, and Hyperledger Fabric across five criteria (higher is better).

Figure 4.5, normalized comparison (0–10 scale) of the proposed blockchain-enhanced EHR access-control framework with centralized EHR systems, MedRec, and Hyperledger Fabric across security, scalability, latency, data integrity, and cost efficiency. The proposed design matches or slightly exceeds the baselines on security and data integrity, and achieves higher cost efficiency than MedRec and Fabric by combining Raft consensus with off-chain storage. Its scalability surpasses centralized systems and Fabric, while MedRec retains an edge in raw scalability at the expense of higher latency and cost. Latency for the proposed framework remains comparable to centralized and Fabric deployments and markedly lower than PoW-based MedRec. Overall, the radar plot suggests that the ECC+ZKP-enabled, Fabric-backed architecture offers a more balanced trade-off across all five criteria, although these scores are derived from simulations and should ultimately be confirmed by empirical measurements.

5. Conclusion

This work presented the design and analysis of the Privacy-Preserving Data Exchange (PPDE) algorithm, which serves as the backbone for ensuring secure, fine-grained access to blockchain-based Electronic Health Records (EHRs) within a diverse IoT landscape. The framework effectively distinguishes between the off-chain data plane where ECC-encrypted EHR content is stored in distributed repositories or IPFS, and the on-chain control plane, which stores access-control smart contracts that manage EHR hashes, policy references, and audit logs, while also verifying ECC signatures and ZKP-based authorization proofs. Algorithm 4.1 lays out the PPDE workflow, guiding everything from request creation and identity/policy verification to the issuance of short-lived capability tokens instead of raw decryption keys. This approach enhances confidentiality and traceability while minimizing long-term key exposure. The cryptographic and access-control elements are built on hash functions, ECC, ZKPs, and RBAC/ABAC policies integrated into smart contracts, all operating over a permissioned Fabric-style consensus designed for consortium healthcare environments. Performance evaluations through simulations indicate that this framework can handle high throughput, maintain low to moderate end-to-end delays, achieve near-unity Packet Delivery Ratios (PDR), and keep energy consumption within acceptable limits, all while scaling effectively with the number of IoT devices. It even outperforms centralized servers, MedRec-style Proof of Work systems, and Hyperledger Fabric baselines across various security and efficiency metrics. However, it is important to note that these findings are based on controlled workloads and synthetic traffic; real-world validation in hospital settings is still needed to confirm these gains. Overall, the PPDE framework fulfills the primary goal of this research by establishing a cryptographically secure, auditable, and scalable access-control layer for EHR sharing in IoT-enabled healthcare consortia.

References

- [1] V. Nehra, A. K. Sharma, and R. K. Tripathi, *Blockchain Implementation for Internet of Things Applications*, no. March. 2020. doi: 10.1016/B978-0-12-819816-2.00005-8.
- [2] S. Rathore, J. H. Park, and H. Chang, “Deep Learning and Blockchain-Empowered Security Framework for Intelligent 5G-Enabled IoT,” *IEEE Access*, vol. 9, pp. 90075–90083, 2021, doi: 10.1109/ACCESS.2021.3077069.
- [3] Bhawana, S. Kumar, R. S. Rathore, M. Mahmud, O. Kaiwartya, and J. Lloret, “BEST—Blockchain-Enabled Secure and Trusted Public Emergency Services for Smart Cities Environment,” *Sensors*, vol. 22, no. 15, pp. 1–25, 2022, doi: 10.3390/s22155733.
- [4] J. Ren, J. Li, H. Liu, and T. Qin, “Task offloading strategy with emergency handling and blockchain security in SDN-empowered and fog-assisted healthcare IoT,” *Tsinghua Sci. Technol.*, vol. 27, no. 4, pp. 760–776, 2022, doi: 10.26599/TST.2021.9010046.
- [5] J. Almalki *et al.*, “Enabling Blockchain with IoMT Devices for Healthcare,” *Inf.*, vol. 13, no. 10, pp. 1–23, 2022, doi: 10.3390/info13100448.
- [6] C. V. N. U. Bharathi Murthy and M. Lawanya Shri, “Secure Sharing Architecture of Personal Healthcare Data Using Private Permissioned Blockchain for Telemedicine,” *IEEE Access*, vol. PP, p. 1, 2024, doi: 10.1109/ACCESS.2024.3436075.
- [7] A. A. Dar, M. Z. Alam, A. Ahmad, F. A. Reegu, and S. A. Rahin, “Blockchain Framework for Secure COVID-19 Pandemic Data Handling and Protection,” *Comput. Intell. Neurosci.*, vol. 2022, 2022, doi: 10.1155/2022/7025485.
- [8] A. Gohar, S. AbdelGaber, and M. Salah, “A proposed patient-centric healthcare framework for better Semantic interoperability using Blockchain,” ... *J. Comput. Sci.* ..., vol. 19, no. 11, 2021, [Online]. Available: https://www.academia.edu/download/78685573/04_Paper_01112111_IJCSIS_Camera_Ready_pp26_35.pdf
- [9] B. Abotsi, E. Agbemaflle, and E. Ayimey, “Positive Outcomes and Challenges of Electronic Health Record Systems: A Case of a Ghanaian Hospital,” *J. Heal. Informatics Africa*, vol. 11, no. 1, pp. 10–21, 2024, doi: 10.12856/JHIA-2024-v11-i1-457.
- [10] L. Ismail and H. Materwala, “Blockchain paradigm for healthcare: Performance evaluation,” *Symmetry (Basel)*, vol. 12, no. 8, 2020, doi: 10.3390/SYM12081200.
- [11] S. Alam *et al.*, “A blockchain-enabled framework for mhealth systems,” *Sustain.*, vol. 12, no. 15, pp. 255–267, 2021, doi: 10.1007/978-981-15-8711-5_13.
- [12] R. G. Sonkamble, A. M. Bongale, S. Phansalkar, A. Sharma, and S. Rajput, “Secure Data Transmission of Electronic Health Records Using Blockchain Technology,” *Electron.*, vol. 12, no. 4, 2023, doi: 10.3390/electronics12041015.
- [13] A. Ali, B. A. S. Al-rimy, A. A. Almazroi, F. S. Alsubaei, A. A. Almazroi, and F. Saeed, “Securing Secrets in Cyber-Physical Systems: A Cutting-Edge Privacy Approach with Consortium Blockchain,” *Sensors*, vol. 23, no. 16, Aug. 2023, doi: 10.3390/s23167162.
- [14] H. B. Mahajan *et al.*, “Integration of Healthcare 4.0 and blockchain into secure cloud-based electronic health records systems,” *Appl. Nanosci.*, vol. 13, no. 3, pp. 2329–

- 2342, Mar. 2023, doi: 10.1007/s13204-021-02164-0.
- [15] S. Fugkeaw, L. Wirz, and L. Hak, "Secure and Lightweight Blockchain-Enabled Access Control for Fog-Assisted IoT Cloud Based Electronic Medical Records Sharing," *IEEE Access*, vol. 11, pp. 62998–63012, 2023, doi: 10.1109/ACCESS.2023.3288332.
- [16] A. Rahman *et al.*, "Internet of medical things and blockchain-enabled patient-centric agent through SDN for remote patient monitoring in 5G network," *Sci. Rep.*, vol. 14, no. 1, pp. 1–19, 2024, doi: 10.1038/s41598-024-55662-w.
- [17] P. Tzavaras, E. Karamanoli, S. Stelios, and K. Sgantzios, "Optimizing Data Governance : Policies and Processes for Data Management in Public Administration and Large Organizations," no. February, 2024, doi: 10.33422/6th.icrbmf.2023.09.105.
- [18] M. Uddin *et al.*, "Hyperledger fabric blockchain: Secure and efficient solution for electronic health records," *Comput. Mater. Contin.*, vol. 68, no. 2, pp. 2377–2397, 2021, doi: 10.32604/cmc.2021.015354.
- [19] D. Gadiraju, R. McMaster, S. Azam, and D. Khazanchi, "BIONIB: Blockchain-based IoT using Novelty Index in BridgeHealth Monitoring," *arXiv (Cornell Univ.)*, pp. 1–10, 2024.
- [20] S. K. Dwivedi, R. Amin, and S. Vollala, "Blockchain based secured information sharing protocol in supply chain management system with key distribution mechanism," *J. Inf. Secur. Appl.*, vol. 54, 2020, doi: 10.1016/j.jisa.2020.102554.
- [21] B. S. Egala, A. K. Pradhan, V. Badarla, and S. P. Mohanty, "Fortified-Chain: A Blockchain-Based Framework for Security and Privacy-Assured Internet of Medical Things with Effective Access Control," *IEEE Internet Things J.*, vol. 8, no. 14, pp. 11717–11731, 2021, doi: 10.1109/JIOT.2021.3058946.
- [22] B. S. Egala, A. K. Pradhan, V. R. Badarla, and S. P. Mohanty, "Fortified-Chain: A Blockchain Based Framework for Security and Privacy Assured Internet of Medical Things with Effective Access Control."
- [23] F. A. Reegu *et al.*, "Blockchain-Based Framework for Interoperable Electronic Health Records for an Improved Healthcare System," *Sustain.*, vol. 15, no. 8, 2023, doi: 10.3390/su15086337.
- [24] H. Tian *et al.*, "Enabling Cross-Chain Transactions: A Decentralized Cryptocurrency Exchange Protocol," *IEEE Trans. Inf. Forensics Secur.*, vol. 16, pp. 3928–3941, 2021, doi: 10.1109/TIFS.2021.3096124.
- [25] K. H. Yeh, G. Y. Yang, C. Butpheng, L. F. Lee, and Y. H. Liu, "A Secure Interoperability Management Scheme for Cross-Blockchain Transactions," *Symmetry (Basel)*, vol. 14, no. 12, pp. 1–19, 2022, doi: 10.3390/sym14122473.
- [26] N. R. Pradhan *et al.*, "A Novel Blockchain-Based Healthcare System Design and Performance Benchmarking on a Multi-Hosted Testbed," *Sensors*, vol. 22, no. 9, pp. 1–20, 2022, doi: 10.3390/s22093449.
- [27] U. Zaman, Imran, F. Mehmood, N. Iqbal, J. Kim, and M. Ibrahim, "Towards Secure and Intelligent Internet of Health Things: A Survey of Enabling Technologies and Applications," Jun. 01, 2022, *MDPI*. doi: 10.3390/electronics11121893.
- [28] R. Bhan, R. Pamula, P. Faruki, and J. Gajrani, *Blockchain-enabled secure and efficient data sharing scheme for trust management in healthcare smartphone network*, vol. 79, no. 14. Springer US, 2023. doi: 10.1007/s11227-023-05272-6.
- [29] T. Saikumari and G. V. Sudha, "An Improved Congestion Handling in Blockchain Secured Cloud Based Healthcare System," *Int. J. Intell. Eng. Syst.*, vol. 17, no. 2, pp. 453–463, 2024, doi: 10.22266/ijies2024.0430.37.
- [30] R. K. Bhaskar and B. Kumaraswamy, "Internet of Things (IoT) Based Modern Healthcare Systems with Nano-Integrated Wearable Biosensor Devices," vol. 1, pp. 882–887, 2024.
- [31] J. B. Madavarapu, S. Nachiyappan, S. Rajarajeswari, and N. Anusha, "Hot Watch : IOT based Wearable Health Monitoring System," *IEEE Sens. J.*, vol. PP, no. Xx, p. 1, 2024, doi: 10.1109/JSEN.2024.3424348.
- [32] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Blockchain for Secure EHRs Sharing of Mobile Cloud Based E-Health Systems," *IEEE Access*, vol. 7, pp. 66792–66806, 2019, doi: 10.1109/ACCESS.2019.2917555.
- [33] M. Roy and M. Singh, "Analytical Study of Blockchain Enabled Security Enhancement Methods for Healthcare Data," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 1131, no. 1, p. 012002, Apr. 2021, doi: 10.1088/1757-899x/1131/1/012002.
- [34] K. Miyachi and T. K. Mackey, "hOCBS: A privacy-preserving blockchain framework for healthcare data leveraging an on-chain and off-chain system design," *Inf. Process. Manag.*, vol. 58, no. 3, May 2021, doi: 10.1016/j.ipm.2021.102535.
- [35] S. Alam *et al.*, "An Overview of Blockchain and IoT Integration for Secure and Reliable Health Records Monitoring," *Sustain.*, vol. 15, no. 7, pp. 1–20, 2023, doi: 10.3390/su15075660.
- [36] A. El Azzaoui, H. Chen, S. H. Kim, Y. Pan, and J. H. Park, "Blockchain-Based Distributed Information Hiding Framework for Data Privacy Preserving in Medical Supply Chain Systems," *Sensors*, vol. 22, no. 4, Feb. 2022, doi: 10.3390/s22041371.
- [37] W. A. N. A. Al-Nbhany, A. T. Zahary, and A. A. Al-Shargabi, "Blockchain-IoT Healthcare Applications and Trends: A Review," *IEEE Access*, vol. 12, no. December 2023, pp. 4178–4212, 2024, doi: 10.1109/ACCESS.2023.3349187.
- [38] M. Saad, M. R. Bhutta, J. Kim, and T. S. Chung, "A Framework for Enhancing Privacy and Anonymity in

- Blockchain-Enabled IoT Devices,” *Comput. Mater. Contin.*, vol. 78, no. 3, pp. 4263–4282, 2024, doi: 10.32604/cmc.2024.047132.
- [39] F. Ullah *et al.*, “Blockchain-enabled EHR access auditing: Enhancing healthcare data security,” *Heliyon*, vol. 10, no. 16, p. e34407, 2024, doi: 10.1016/j.heliyon.2024.e34407.
- [40] Y. Xu, H. Y. Chong, and M. Chi, “A Review of Smart Contracts Applications in Various Industries: A Procurement Perspective,” *Adv. Civ. Eng.*, vol. 2021, 2021, doi: 10.1155/2021/5530755.
- [41] M. Tahir, M. Sardaraz, S. Muhammad, and M. S. Khan, “A lightweight authentication and authorization framework for blockchain-enabled IoT network in health-informatics,” *Sustain.*, vol. 12, no. 17, 2020, doi: 10.3390/SU12176960.
- [42] M. S. Islam, M. A. Bin Aamedeen, M. A. Rahman, H. Ajra, and Z. B. Ismail, “Healthcare-Chain: Blockchain-Enabled Decentralized Trustworthy System in Healthcare Management Industry 4.0 with Cyber Safeguard,” *Computers*, vol. 12, no. 2, 2023, doi: 10.3390/computers12020046.
- [43] R. Xu, Y. Chen, E. Blasch, and G. Chen, “BlendCAC: A smart contract enabled decentralized capability-based access control mechanism for the IoT,” *Computers*, vol. 7, no. 3, pp. 1–27, 2018, doi: 10.3390/computers7030039.
- [44] Chioma Anthonia Okolo, Oloruntoba Babawarun, and Tolulope Oyinlola Olorunsogo, “Mobile Health (Mhealth) Innovations for Public Health Feedback: a Global Perspective,” *Int. Med. Sci. Res. J.*, vol. 4, no. 3, pp. 235–246, 2024, doi: 10.51594/imsrj.v4i3.915.
- [45] M. A. Rahman, M. Shamim Hossain, M. S. Islam, N. A. Alrajeh, and G. Muhammad, “Secure and provenance enhanced internet of health things framework: A blockchain managed federated learning approach,” *IEEE Access*, vol. 8, pp. 205071–205087, 2020, doi: 10.1109/ACCESS.2020.3037474.
- [46] I. Chakour, C. Daoui, M. Baslam, B. Sainz-De-Abajo, and B. Garcia-Zapirain, “Strategic Bandwidth Allocation for QoS in IoT Gateway: Predicting Future Needs Based on IoT Device Habits,” *IEEE Access*, vol. 12, no. December 2023, pp. 6590–6603, 2024, doi: 10.1109/ACCESS.2024.3351111.
- [47] K. Zala, H. K. Thakkar, R. Jadeja, P. Singh, K. Kotecha, and M. Shukla, “PRMS: Design and Development of Patients’ E-Healthcare Records Management System for Privacy Preservation in Third Party Cloud Platforms,” *IEEE Access*, vol. 10, no. June, pp. 85777–85791, 2022, doi: 10.1109/ACCESS.2022.3198094.
- [48] M. J. Baucas, P. Spachos, and K. N. Plataniotis, “Federated Learning and Blockchain-Enabled Fog-IoT Platform for Wearables in Predictive Healthcare,” *IEEE Trans. Comput. Soc. Syst.*, vol. 10, no. 4, pp. 1732–1741, 2023, doi: 10.1109/TCSS.2023.3235950.
- [49] K. Seol, Y. G. Kim, E. Lee, Y. D. Seo, and D. K. Baik, “Privacy-preserving attribute-based access control model for XML-based electronic health record system,” *IEEE Access*, vol. 6, pp. 9114–9128, 2018, doi: 10.1109/ACCESS.2018.2800288.
- [50] J. Enare Abang, H. Takruri, R. Al-Zaidi, and M. Al-Khalidi, “Latency performance modelling in hyperledger fabric blockchain: Challenges and directions with an IoT perspective,” *Internet of Things (Netherlands)*, vol. 26, no. April, p. 101217, 2024, doi: 10.1016/j.iot.2024.101217.
- [51] P. Rani, S. Verma, S. P. Yadav, B. K. Rai, M. S. Naruka, and D. Kumar, “Simulation of the Lightweight Blockchain Technique Based on Privacy and Security for Healthcare Data for the Cloud System,” *Int. J. E-Health Med. Commun.*, vol. 13, no. 4, 2022, doi: 10.4018/IJEHMC.309436.
- [52] A. Ali *et al.*, “An Industrial IoT-Based Blockchain-Enabled Secure Searchable Neural Network,” *Sensors*, vol. 22, no. 2, 2022.
- [53] Z. Mahmood and V. Jusas, “Blockchain-Enabled: Multi-Layered Security Federated Learning Platform for Preserving Data Privacy,” *Electron.*, vol. 11, no. 10, 2022, doi: 10.3390/electronics11101624.
- [54] X. Yang and K. Zhang, “A Fair and Trusted Trading Scheme for Medical Data Based on Smart Contracts,” *Comput. Mater. Contin.*, vol. 78, no. 2, pp. 1843–1859, 2024, doi: 10.32604/cmc.2023.047660.
- [55] A. Ali *et al.*, “An Industrial IoT-Based Blockchain-Enabled Secure Searchable Encryption Approach for Healthcare Systems Using Neural Network,” *Sensors*, vol. 22, no. 2, Jan. 2022, doi: 10.3390/s22020572.
- [56] S. H. Alsamhi *et al.*, “Federated Learning Meets Blockchain in Decentralized Data Sharing: Healthcare Use Case,” *IEEE Internet Things J.*, vol. 11, no. 11, pp. 19602–19615, 2024, doi: 10.1109/JIOT.2024.3367249.
- [57] A. K. Jakhar, M. Singh, R. Sharma, W. Viriyasitavat, G. Dhiman, and S. Goel, “A blockchain-based privacy-preserving and access-control framework for electronic health records management,” *Multimed. Tools Appl.*, pp. 0–26, 2024, doi: 10.1007/s11042-024-18827-3.
- [58] S. K. Rana *et al.*, “Blockchain Technology and Artificial Intelligence Based Decentralized Access Control Model to Enable Secure Interoperability for Healthcare,” *Sustain.*, vol. 14, no. 15, 2022, doi: 10.3390/su14159471.
- [59] P. Chinnasamy, A. Albakri, M. Khan, A. A. Raja, A. Kiran, and J. C. Babu, “Smart Contract-Enabled Secure Sharing of Health Data for a Mobile Cloud-Based E-Health System,” *Appl. Sci.*, vol. 13, no. 6, 2023, doi: 10.3390/app13063970.
- [60] L. Hang and D. H. Kim, “Design and implementation of an integrated iot blockchain platform for sensing data integrity,” *Sensors (Switzerland)*, vol. 19, no. 10, 2019, doi: 10.3390/s19102228.
- [61] S. Chenthar, K. Ahmed, H. Wang, F. Whittaker, and Z. Chen, *Healthchain: A novel framework on privacy preservation of electronic health records using blockchain*

- technology, vol. 15, no. 12 December. 2020. doi: 10.1371/journal.pone.0243043.
- [62] K. Hasan, M. J. M. Chowdhury, K. Biswas, K. Ahmed, M. S. Islam, and M. Usman, "A blockchain-based secure data-sharing framework for Software Defined Wireless Body Area Networks," *Comput. Networks*, vol. 211, 2022, doi: 10.1016/j.comnet.2022.109004.
- [63] M. Kumar *et al.*, "BBNSF: Blockchain-Based Novel Secure Framework Using RP2-RSA and ASR-ANN Technique for IoT Enabled Healthcare Systems," *Sensors*, vol. 22, no. 23, 2022, doi: 10.3390/s22239448.
- [64] L. Nkenyereye, S. M. Riazul Islam, M. Hossain, M. Abdullah-Al-Wadud, and A. Alamri, "Blockchain-Enabled EHR Framework for Internet of Medical Things," *Comput. Mater. Contin.*, vol. 67, no. 1, pp. 211–221, 2021, doi: 10.32604/cmc.2021.013796.
- [65] B. Saravana Balaji, P. Vishnu Raja, A. Nayyar, P. Sanjeevikumar, and S. Pandiyan, "Enhancement of security and handling the inconspicuousness in IoT using a simple size extensible blockchain," *Energies*, vol. 13, no. 7, 2020, doi: 10.3390/en13071795.
- [66] M. Mohammadi, R. Javan, M. Beheshti-Atashgah, and M. R. Aref, "SCALHEALTH: Scalable Blockchain Integration for Secure IoT Healthcare Systems," pp. 1–8, 2024, [Online]. Available: <http://arxiv.org/abs/2403.08068>
- [67] S. Shukla, B. Sachdeva, A. Sharma, R. Sharma, and S. Tomar, "A Blockchain-based Smart Contract System for Healthcare Management," *14th Int. Conf. Adv. Comput. Control. Telecommun. Technol. ACT 2023*, vol. 2023-June, pp. 2262–2268, 2023.
- [68] S. H. Kembo, P. Mpofu, B. T. Mukorera, and S. Jacques, "Blockchain-secured health wearables in smart homes utilising raspberry pi web of things gateways," *Proc. Int. Conf. Ind. Eng. Oper. Manag.*, vol. 59, pp. 2269–2280, 2020.
- [69] N. Kiyavitskaya *et al.*, "Automating the Extraction of Rights and Obligations for Regulatory Compliance," pp. 1–14.
- [70] A. Johannsen, D. Kant, and R. Creutzburg, "Measuring IT security, compliance and data governance within small and medium-sized IT enterprises," *IS T Int. Symp. Electron. Imaging Sci. Technol.*, vol. 2020, no. 3, pp. 1–11, 2020, doi: 10.2352/ISSN.2470-1173.2020.3.MOBMU-252.
- [71] M. Darshan, M. Amet, G. Srivastava, and J. Crichigno, "An Architecture That Enables Cross-Chain Interoperability for Next-Gen Blockchain Systems," *IEEE Internet Things J.*, vol. 10, no. 20, pp. 18282–18291, 2023, doi: 10.1109/JIOT.2023.3279693.
- [72] M. Abubakar, H. Ali, B. Ghaleb, I. Wadhaj, and W. J. Buchanan, "An Overview of Blockchain-Based IoT Architectures and Designs," *Lect. Notes Networks Syst.*, vol. 584 LNNS, no. February, pp. 596–605, 2023, doi: 10.1007/978-3-031-25274-7_52.
- [73] S. Duggineni, "Impact of Controls on Data Integrity and Information Systems," vol. 13, no. November 2020, pp. 29–35, 2023, doi: 10.5923/j.scit.20231302.04.
- [74] A. K. Jakhar, M. Singh, R. Sharma, and A. Sharma, "A Blockchain-based Privacy-preserving and Access-control Framework for Electronic Health Records Management," Sep. 21, 2022. doi: 10.21203/rs.3.rs-2048551/v1.
- [75] R. K. Mishra, R. K. Yadav, and P. Nath, "Blockchain-based Decentralized Authorization Technique for Data Sharing in the Internet of Things," *2021 5th Int. Conf. Inf. Syst. Comput. Networks, ISCON 2021*, no. February, 2021, doi: 10.1109/ISCON52037.2021.9702297.
- [76] A. M. Tawfik, A. Al-Ahwal, A. S. T. Eldien, and H. H. Zayed, "ACHealthChain blockchain framework for access control and privacy preservation in healthcare," *Sci. Rep.*, vol. 15, no. 1, 2025, doi: 10.1038/s41598-025-00757-1.
- [77] H. Aldawood and G. Skinner, "Contemporary Cyber Security Social Engineering Solutions , Measures , Policies , Tools and Applications : A Critical Appraisal," no. 10, pp. 1–15, 2019.
- [78] Y. Ding, Y. Zhang, B. Qin, Q. Wang, Z. Yang, and W. Shi, "A Scalable Cross-Chain Access Control and Identity Authentication Scheme," *Sensors*, vol. 23, no. 4, pp. 1–18, 2023, doi: 10.3390/s23042000.
- [79] P. Zhang, M. A. Walker, J. White, D. C. Schmidt, and G. Lenz, "Metrics for assessing blockchain-based healthcare decentralized apps," *2017 IEEE 19th Int. Conf. e-Health Networking, Appl. Serv. Heal. 2017*, vol. 2017-Decem, pp. 1–4, 2017, doi: 10.1109/HealthCom.2017.8210842.
- [80] S. Smetanin, A. Ometov, M. Komarov, P. Masek, and Y. Koucheryavy, "Blockchain evaluation approaches: State-of-the-art and future perspective," *Sensors (Switzerland)*, vol. 20, no. 12, pp. 1–20, 2020, doi: 10.3390/s20123358.
- [81] J. Almasizadeh and M. Abdollahi Azgomi, "Mean privacy: A metric for security of computer systems," *Comput. Commun.*, vol. 52, pp. 47–59, 2014, doi: 10.1016/j.comcom.2014.06.009.
- [82] I. Wagner and D. Eckhoff, "Technical privacy metrics: A systematic survey," *ACM Comput. Surv.*, vol. 51, no. 3, pp. 1–45, 2018, doi: 10.1145/3168389.
- [83] P. Pawar, N. Parolia, S. Shinde, T. O. Edoh, and M. Singh, "eHealthChain—a blockchain-based personal health information management system," *Ann. des Telecommun. Telecommun.*, vol. 77, no. 1–2, pp. 33–45, 2022, doi: 10.1007/s12243-021-00868-6.