Acta Informatica Pragensia
2026, Volume 15, Issue 1, 90–108
https://doi.org/10.18267/j.aip.290

VŠE / PRAGUE UNIVERSITY OF ECONOMICS AND BUSINESS

Article Open Access

Blockchain-Based Framework for Enhancing Interoperability and Security in EHR Exchange Using Lightweight ECC Proxy Re-Encryption

Devaramane Yogaraj Ashwini [1], **Reval Prabhu Puneeth** [2]

[1] Department of Humanities, NMAM Institute of Technology – affiliated to NITTE (Deemed to be University), Karkala, Karnataka, India
[2] Department of Computer Science and Engineering, NMAM Institute of Technology – affiliated to NITTE (Deemed to be University), Karkala, Karnataka, India

Corresponding author: Reval Prabhu Puneeth (puneeth.reval313@gmail.com)

Editorial Record

First submission received:
June 19, 2025

Revisions received:
August 12, 2025
September 16, 2025

Accepted for publication:
September 23, 2025

Academic Editor:
Zdenek Smutny
Prague University of Economics and Business, Czech Republic

This article was accepted for publication by the Academic Editor upon evaluation of the reviewers' comments.

How to cite this article:
Ashwini, D. Y., & Puneeth, R. P. (2026). Blockchain-Based Framework for Enhancing Interoperability and Security in EHR Exchange Using Lightweight ECC Proxy Re-Encryption. *Acta Informatica Pragensia*, 15(1), 90–108. https://doi.org/10.18267/j.aip.290

Abstract

Background: The sharing of electronic health records among hospitals is crucial for ensuring consistent patient treatment. However, the process remains challenging due to the existence of varied systems, privacy concerns and interoperability issues. It is often difficult to maintain an equilibrium of security, efficiency and compliance across all platforms.

Objective: The objective of this article is to develop a framework that enables secure, efficient and interoperable Electronic health records (EHR) sharing across healthcare systems.

Methods: The proposed work introduces a Lightweight elliptic curve cryptography proxy re-encryption (LWECC-PRE) framework that facilitates safe and distributed EHR exchange through Ethereum and Hyperledger Fabric blockchains. It integrates Hybrid elliptic curve proxy re-encryption (HEC-PRE) by combining elliptic curve cryptography with proxy re-encryption for giving healthcare providers the means to control access to confidential data. Besides, the design incorporates the Elliptic curve integrated encryption scheme (ECIES) for secure data encryption and the Elliptic curve digital signature algorithm (ECDSA) to verify the integrity and authenticity of data communications. It uses Interplanetary file system (IPFS) for secure peer-to-peer storage. The design supports asynchronous record sharing between blockchain networks through smart contracts and regulated re-encryption.

Results: The experimental results show that the framework minimizes computation overheads, preserves patient privacy and improves interoperability of distributed healthcare systems.

Conclusion: The proposed solution addresses key challenges in EHR sharing by providing a safe, secure, efficient and patient-centred solution to healthcare data exchange.

Index Terms

Electronic health record; EHR; Proxy re-encryption; PRE; Blockchain; Interoperability; Healthcare data security; Elliptic curve cryptography; ECC.

1 INTRODUCTION

Electronic health records (EHRs) are a digital version of patients' medical information such as the history of illnesses, treatment, medication, laboratory analyses, scan reports, allergies and other important medical details. For the benefit of patients, this digital information can be made available online by ensuring the individual's privacy and also maintaining confidentiality. Patient-centric access control helps patients have control over their medical information such that the data owner can decide about with whom the data can be shared.

However, these approaches should ensure that only authorized users based on their privileges can update real-time data to keep the data up-to date (Cobrado et al., 2024; Ali et al., 2025). Meanwhile, the EHR data need to be structured to ensure that patient data can be exchanged among multiple healthcare service providers. This helps patients obtain quick response, faster treatment, avoid redundant health checks and generally improve the healthcare outcomes (Ettaloui et al., 2024).

The blockchain technology that was initially introduced in 2009 by Satoshi Nakamoto is a root of cryptocurrencies and a bitcoin system. This decentralized system has characteristics such as immutability, data tamper-proofness, distribution of control, data security and secure access control management. Thanks to these, Blockchain 2.0 led to financial services and smart contracts. From 2012, Blockchain 3.0 was used to implement applications beyond the financial service industry and is used in government, health, media, the arts and justice. Blockchain proves to be the potential technology to address most stakeholder requirements in the field of healthcare. Thus, it has resulted in increasing numbers of research studies aiming to incorporate blockchain in EHRs (Sharma et al., 2025).

Blockchain is a promising technology to support interoperability, but it has a number of challenges and limitations as well. Firstly, one needs to analyse what kind of blockchain to use. An existing open-source blockchain can be used, or a new one has to be designed for the system. It is also necessary to find out whether it is public, private or managed by a group and whether to include smart contracts as part of the setup. Secondly, choosing the appropriate EHR standard for recording patient data is important. Since different organizations and countries follow different standards, it is necessary to either adopt a common approach or find a practical way to convert data into compatible versions to meet the need for interoperability (Anand et al., 2023; Shen et al., 2025).

Another issue to be considered is scalability. Usually. EHR data are large in size and saving them directly on the blockchain can be costly and slow to access. One way to deal with this is by using cloud storage along with the blockchain. In that case, however, the records will not be completely immutable, so other steps are needed to make sure that the data stay accurate and secure. It is also important to consider whether a third-party auditor should be part of the system. Should there be someone in the network who monitors the data and requests on the blockchain, or should all members have equal access? This is another point that needs to be looked into (Puneeth & Parthasarathy, 2023).

To deal with these challenges, researchers have designed different system architectures and software platforms that support blockchain-based EHRs with interoperability. They have also introduced various supporting features to handle specific problems. Most of these approaches start by making sure that all stakeholders use the same standards to record EHR data. Basic identity details, hash of the information and references of the information are stored on the blockchain, while larger medical records are saved in a cloud database. A link or reference to the cloud data is stored on the blockchain to help maintain its integrity. Access to this information is given only to authorized users through encryption. Smart contracts are used to manage and control these steps. With this setup, blockchain can be used effectively to store and manage EHRs while supporting interoperability (Sonkamble et al., 2024; Ferreira et al., 2024).

1.1 Blockchain-enabled interoperability for electronic health records

Interoperability is an important aspect of software systems. As per the IEEE definition, it refers to the ability of two or more systems to share information and use it effectively. In the healthcare field, organizations such as the NAHIT (National Alliance for Health Information Technology) have added to this idea by defining interoperability as the ability of software and IT systems to exchange data in a clear, accurate and efficient manner and also make use of those data when needed.

Interoperability plays an important role in EHR management for sharing and managing patient EHRs. As data are generated at different places such as lab, clinic, hospitals and even body sensors, all these store data separately in their own storage systems. To access these scattered data, all the stakeholders such as patients, doctors and hospitals are supposed to access the information in a faster way. Besides, interoperability helps reduce human error and enhances efficiency of healthcare services (Shen et al., 2025).

The healthcare data in a blockchain keep growing as new data are added; they are managed by the network users rather than a single entity. The major concern in implementing distributed applications in healthcare is addressing privacy and security needs, as multiple stakeholders are involved in sharing and managing sensitive medical information. Figure 1 shows that a blockchain-based solution helps securely share patient data between hospitals 1 to N, with a government authority in control. This provides assurance that patient data will not be compromised and that data exchange remains open and secure. Blockchain technology, along with a central manager, helps control access to the system and keeps it safe according to privacy regulations, while also achieving interoperability among hospitals.

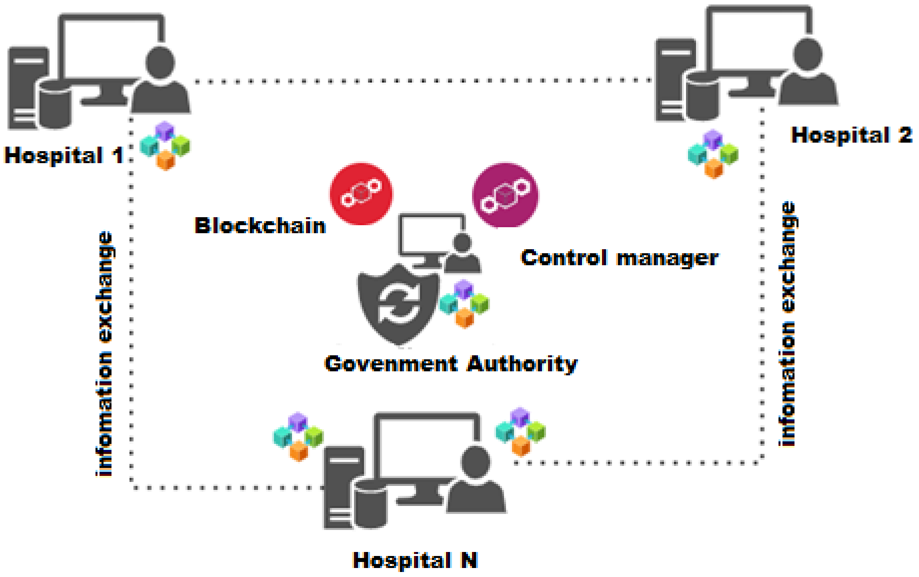


Figure 1. Blockchain-based secure interoperability framework for healthcare data exchange.

However, several challenges still exist, such as implementation difficulties, large volumes of medical data, scalability issues, differences between blockchains, storage concerns, security trade-offs and the absence of standard communication protocols, all of which make achieving full interoperability difficult. Moreover, differences in the structure of EHR-based blockchains such as how transactions are handled, the variety of standards followed and the methods used to send data continue to create new challenges in reaching effective interoperability (Ettaloui et al., 2024).

2 LITERATURE REVIEW

An interoperability framework provides a set of rules and guidelines that enable different systems to work together effectively. Jabbar et al. (2020) addressed interoperability difficulties in EHR systems by proposing a software architecture that uses both cloud and blockchain technologies, along with a trusted third-party auditor. The proposed approach includes two components: the health information centre (HIS) and the BiiMED blockchain. Cloud storage is used to address scalability issue and to speed up data access. However, the presence of a third-party auditor can also be seen as a weakness, as the auditor may approve or validate incorrect medical data in collaboration with stakeholders. There is also a risk of a single point of failure (Jabbar et al., 2020).

MedRec is a blockchain-based model developed to support interoperability between providers while giving patients control over their medical records. It uses the Ethereum blockchain, treating health records as assets managed through smart contracts and enabling patients to access data via a user interface (Reegu et al., 2023). FHIRchain (fast health interoperability resource chain) is another blockchain framework, following HL7 and FHIR standards for secure health data exchange. It allows metadata to be stored in a decentralized way without transferring the actual data. Encrypted reference pointers are used for identity verification and once authenticated, users can access data directly from the source (Anand & Sadhna, 2023).

The system known as Ancile proposes a blockchain solution to enhance safe interoperability aspects for stakeholders in the healthcare sector. The proposed solution uses smart contracts on Ethereum and the homomorphic encryption technique to ensure data privacy and authorized control. Despite being decentralized, there are nodes with higher authority, which may lead to single point failure or issues with control and reliability (George et al., 2024).

The aforesaid schemes MedRec, FHIRChain and Ancile work with standards such as HL7, HIPAA and DICOM to enhance data sharing among multiple healthcare service providers, make it more consistent and secure. This indicates the significance of developing blockchain-based solutions that are compatible with existing medical data standards to handle data more conveniently and reliably. To address the average delay in transferring data between blockchains, Hashim et al. (2022) proposed a transaction-based smart contract triggering system to support sharing of health records; however, scalability and security concerns were not considered in their communication protocol.

Yan et al. (2020) highlighted the security concerns associated with the distributed nature of the blockchain network. Data privacy and protection remain critical concerns as the system is prone to cyber-attackers. Ensuring consistent view of patient details across network is also considered as a problematic because of distributed data resources and potential conflicts in data updates. Scalability and performance issues persist as participants and data volume increase.

Rajput et al. (2021) developed permissioned blockchain-based access control framework using Hyperledger Fabric frameworks mainly to address privacy in personal health records (PHR) during emergencies. Latency and performance are the limitations of the proposed framework and they are inherent in hyperledger-based approaches. The present research aims to address the scalability issue and provide a more effective solution for PHRs within healthcare systems.

Semantha et al. (2023) proposed an interoperability framework named PbDinEHR, mainly focused on a privacy-by-design mechanism to address privacy challenges in EHRs. It was implemented using two permissioned Ethereum blockchain networks along with IPFS. The proposed technique lacks support for the right to be forgotten – a significant aspect defined in GDPR – and robust user access controls. The proposed framework approach is progressive resistance against data breaches.

Corbin et al. (2023) proposed a DEPLOYR framework, which enables quick deployment of clinical machine learning models into EMR systems primarily within Stanford Health Care in the USA. The frameworks supports the APIs of the FHIR standards to enable data exchange. In continuation to that, Mishra et al. (2023) proposed an API-led integration framework focused on using reusable APIs to securely and effectively share patient data among systems. It follows a multitier architecture designed for scalability and real-time communication to improve interoperability.

Sonkamble et al. (2024) proposed a framework based on hash lock and secure password key exchange (SPAKE method) for sharing patient information between two healthcare stakeholders. Although the system adopted an off-chain approach to handle scalability, their method faces limitations related to high gas costs, cross-chain transaction conflicts and lack of semantic interoperability. The secure password remained vulnerable to brute-force attacks and dictionary attacks.

Islam et al. (2025) developed a hybrid blockchain and fog computing model to ensure that there is low latency and fault tolerance in healthcare edge networks. Recent literature reviews outline the high levels of interoperability and privacy and compliance increases with the integration of blockchain and the FHIR standards (Ettaloui et al., 2024; Ferreira et al., 2024; Ahmad et al., 2024; Kunal et al., 2024).

In order to address the above limitations in interoperable healthcare networks, we propose a lightweight elliptic curve cryptography proxy re-encryption (LWECC-PRE) framework that uses an ECC integrated encryption scheme, along with IPFS, an optimized storage approach based on a hash table (Puneeth & Parthasarathy, 2023) that tackles the problem of scalability, security and interoperability. The main advantage of the proposed approach is that it enables asynchronous cross-chain interoperability of EHRs.

3 METHODOLOGY

In the present approach of LWECC-PRE, the system ensures secure and interoperable EHR exchange among blockchains. Existing approaches such as SPAKE (Sonkamble et al., 2024) are vulnerable to brute-force attacks as well as dictionary attacks. In contrast, the proposed approach addresses these weaknesses and data can be transferred securely without transmission of plaintext by using elliptic curve cryptography (ECC) and proxy re-encryption.

3.1 Secure access and proxy re-encryption

LWECC-PRE enables only privileged and authorised healthcare service providers to access patient data through a proxy that re-encrypts the data without requiring decryption. This mechanism of patient-centric access control was proposed by Puneeth and Parthasarathy (2024), with the help of public key cryptography, ECIES and ECDSA. It facilitates fine-grained access control deployed in the smart contracts to regulate decryption rights and enforce strict authorization.

3.2 Hybrid storage with IPFS

In order to overcome the storage restrictions of blockchain, the framework integrates a hybrid on-chain/off-chain model. Information such as metadata and access policies is on chain to permit auditing, whereas the actual EHRs are stored in a distributed interplanetary file system (IPFS). Every file has a unique hash value, maintaining integrity and providing efficient retrieval of files. The design is more appropriate to handle large data and is cost-effective compared to an on-chain approach. Additionally, it is scalable. Having secure storage and access controls, cross-chain interoperability within the framework can be achieved seamlessly between blockchain platforms (Keshta et al., 2023).

3.3 Cross-chain interoperability

Asynchronous cross-chain interactions between multiple blockchains are preferred over synchronous ones because, as the chains are loosely coupled, any node can start initiation without waiting for approval from others. Strategies such as event-driven or message-based techniques can aid the process. By a combination of proxy re-encryption and smart contracts, EHRs can be effectively shared between networks, such as Ethereum and Hyperledger Fabric, without the need for synchronization and/or trust between them.

3.4 Lightweight cryptography for efficiency

The security-to-key-size ratio of ECC is predominantly high. For instance, the Secp256k1 elliptic curve private key is just as secure as a 3072-bit RSA private key; the computational overheads are also low compared to RSA. For most attacks such as eavesdropping, impersonate attack, replay attack, DDoS attack, MITM attacks, ECC is considered the optimal solution. These characteristics render LWECC-PRE more suitable for internet of medical things and mobile applications, where resource efficiency is crucial. Additionally, the framework also eliminates the use of passwords that increase human error by improving the security stance.

3.5 System architecture and workflow

Figure 2 shows the design of the proposed architecture, which proposes a secure and efficient system to exchange cross-blockchain EHRs with elliptic curve proxy re-encryption (ECC-PRE), blockchain platforms (Ethereum and Hyperledger Fabric) and the interplanetary file system (IPFS).

The process begins with the application of the elliptic curve integrated encryption scheme (ECIES) to encrypt EHR information. The encrypted records are later saved at the IPFS off-chain storage, which is decentralized. The participating blockchain network maintains on-chain information that helps keep track of access privileges, permissions and metadata. Meanwhile, the elliptic curve digital signature algorithm (ECDSA) used to ensure authenticity and integrity of data in all the transactions.

Patients will be in full control of their data by having a protected interface where they can control the access to their data. If cross-chain sharing is needed, it is re-encrypted with ECC-PRE by the proxy server node. This proxy encrypts cipher texts compatible with the intended recipient without accessing the plaintext; this helps achieve confidentiality of data in the server nodes. The data that have been re-encrypted are sent to the intended recipient, who can decrypt them with a personal key. Smart contracts are associated with patient-centric access control (Puneeth & Parthasarathy, 2024).

This promotes transparency and accountability of blockchain networks. A sequence diagram of data sharing between two different blockchain platforms is shown in Figure 3.

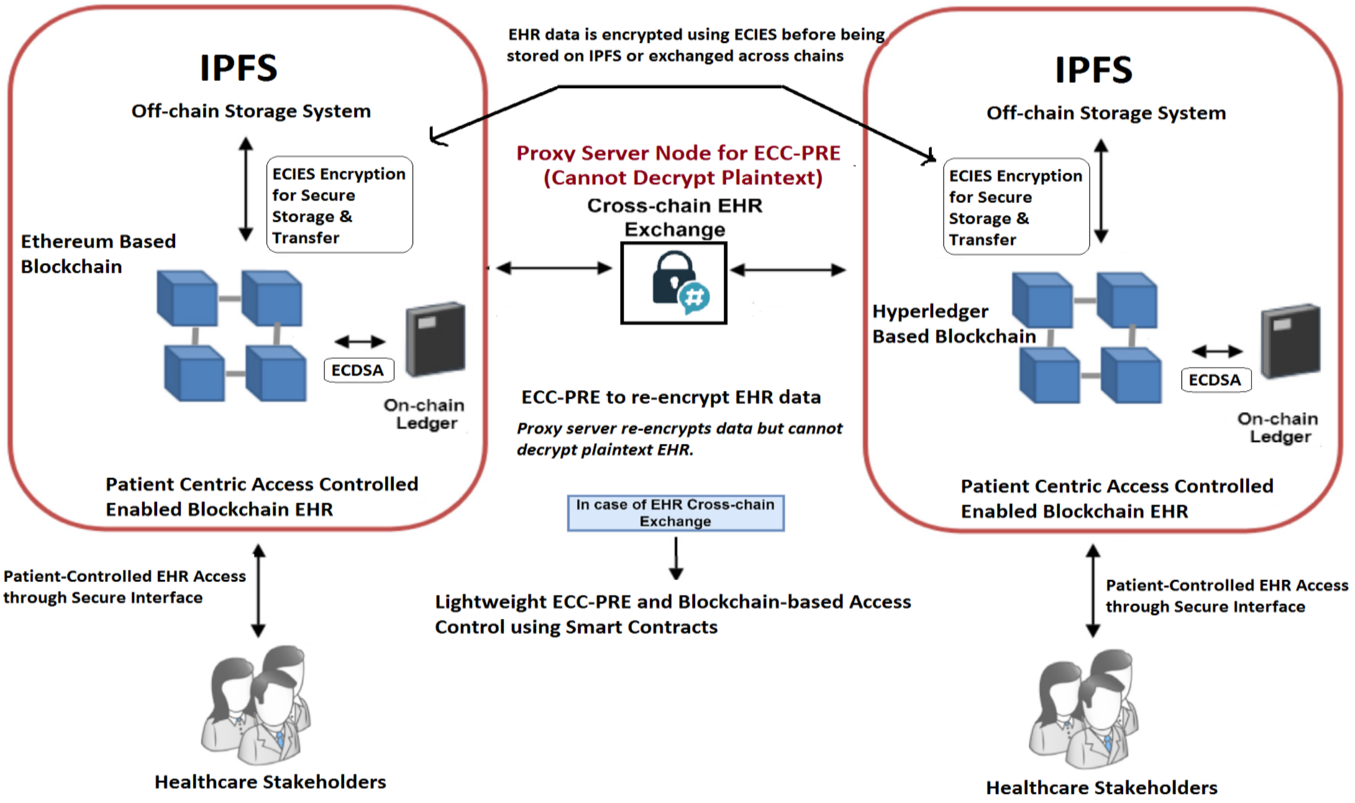

EHR data is encrypted using ECIES before being stored on IPFS or exchanged across chains
IPFS
Off-chain Storage System
ECIES Encryption for Secure Storage & Transfer
Ethereum Based Blockchain
ECDSA
On-chain Ledger
Patient Centric Access Controlled Enabled Blockchain EHR
Proxy Server Node for ECC-PRE (Cannot Decrypt Plaintext)
Cross-chain EHR Exchange
ECC-PRE to re-encrypt EHR data
Proxy server re-encrypts data but cannot decrypt plaintext EHR.
In case of EHR Cross-chain Exchange
Lightweight ECC-PRE and Blockchain-based Access Control using Smart Contracts
IPFS
Off-chain Storage System
ECIES Encryption for Secure Storage & Transfer
Hyperledger Based Blockchain
ECDSA
On-chain Ledger
Patient Centric Access Controlled Enabled Blockchain EHR
Patient-Controlled EHR Access through Secure Interface
Healthcare Stakeholders
Patient-Controlled EHR Access through Secure Interface
Healthcare Stakeholders

Figure 2. *Secure cross-chain exchange of electronic health records (EHR) using ECC-PRE and blockchain.*

The framework under consideration starts with the patient encrypting and securing their electronic health record (EHR) via ECIES and storing it in IPFS at a decentralized off-chain storage. The metadata and access control are then registered on the Ethereum blockchain through a smart contract, guaranteeing traceability and immutability. In the case of a doctor demanding access, Ethereum checks the doctor’s identity and permission with the smart contract. When verification of the request has been successful, the request is sent to a proxy server, which re-encrypts the data with ECC-PRE. This guarantees safe access delegation which does not reveal the actual data.

The proxy proceeds to give re-encryption reference information and metadata to Hyperledger Fabric. Once the request can be verified, Hyperledger keeps the reference in a secure form and grants access to the doctor. Based on the reference, the doctor accesses the encrypted EHR from IPFS; after retrieving it, the doctor uses their own private key to decrypt it. Ethereum and Hyperledger Fabric record these accesses to make their systems transparent and cross-chain consistent. Lastly, the patient retains access rights and has the right to audit permissions and revoke access at any given time via the Ethereum smart contract.

The following algorithms provide a description of the secure sharing of electronic health records (EHRs) using elliptic curve cryptography (ECC), proxy re-encryption (PRE) and smart contracts on a blockchain. The encryption, access control, re-encryption and decryption covered by these algorithms guarantee data confidentiality, integrity and controlled access and allow sharing secured data among several healthcare systems.

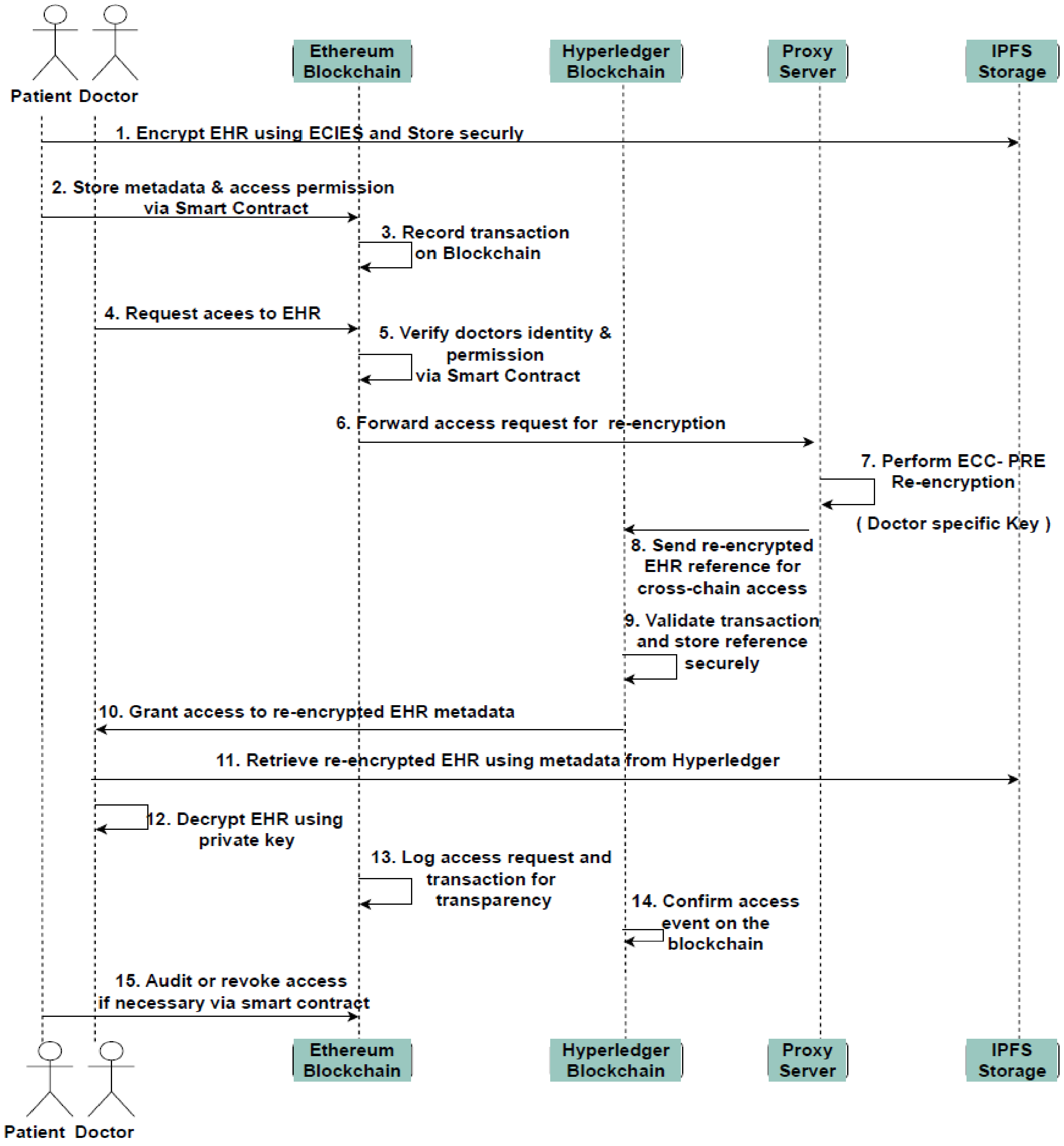

Patient
Doctor
Ethereum Blockchain
Hyperledger Blockchain
Proxy Server
IPFS Storage
1. Encrypt EHR using ECIES and Store securly
2. Store metadata & access permission via Smart Contract
3. Record transaction on Blockchain
4. Request acees to EHR
5. Verify doctors identity & permission via Smart Contract
6. Forward access request for re-encryption
7. Perform ECC- PRE Re-encryption
(Doctor specific Key)
8. Send re-encrypted EHR reference for cross-chain access
9. Validate transaction and store reference securely
10. Grant access to re-encrypted EHR metadata
11. Retrieve re-encrypted EHR using metadata from Hyperledger
12. Decrypt EHR using private key
13. Log access request and transaction for transparency
14. Confirm access event on the blockchain
15. Audit or revoke access if necessary via smart contract
Ethereum Blockchain
Hyperledger Blockchain
Proxy Server
IPFS Storage
Patient
Doctor

Figure 3. *Workflow of secure EHR re-encryption and access control via blockchain and proxy server.*

Algorithm 1. Secure patient data encryption and access control

Input: Medical record M, patient's private key sk_P, doctor's public key pk_D, proxy re-encryption key $rk_{P\to D}$

Output: Secure encrypted medical record C_P and controlled access for the doctor

Step 1. Key generation using ECC

To establish a secure communication, both the patient and doctor generate their respective key pairs using elliptic curve cryptography (ECC):

- The patient generates the key pair sk_P, pk_P: $pk_P = sk_P.G$
- The doctor generates the key pair sk_D, pk_D: $pk_D = sk_D.G$
- The proxy does not generate its own key pair but uses the re-encryption key $rk_{P\to D}$ for controlled access.

Step 2. Encryption using ECIES

To ensure confidentiality, the patient encrypts the medical record before storing it:

1. Generate a cryptographically secure random ephemeral key r from the set Z_q.

2. Compute shared secret using elliptic curve Diffie-Hellman (ECDH):

$$K = r\,.pk_P$$

3. Derive the AES encryption key from the shared secret using a secure cryptographic hash function H: $K_{AES} = H(K_x)$, Ensure that K_x is the shared secret generated in Step 2.

4. Encrypt the medical record M using the AES-GCM encryption mode (which provides both confidentiality and integrity/authentication):

$$C_P = AES - GCM(K_{AES}, M)$$

5. Store the encrypted medical record C_P on the IPFS and obtain the corresponding hash H_{IPFS}.

6. Store metadata including $H_{IPFS}, pk_P, access\ permissions$ on the blockchain to ensure immutable access control.

Step 3. Access request and authorization via smart contract

To prevent unauthorized access, doctors must request permission via a blockchain smart contract:

The doctor requests access by signing the transaction $Tx_{Request}$ using ECDSA:

$\sigma D = ECDSA - Sign\ (sk_D, Tx_{Request})$

If authorized, the smart contract triggers re-encryption to allow controlled data sharing.

Step 4. Proxy re-encryption

Compute the re-encryption key: $rk_{\{P\to D\}} = sk_P^{-1}.pk_D$

The proxy transforms the ciphertext C_P into C_D without decrypting:

$$C_D = \text{ReEncrypt}\ (C_P, rk_{P\to D})$$

The re-encrypted ciphertext C_D is sent to the doctor.

Step 5. Decryption by the doctor

Once authorized, the doctor decrypts the medical record:

1. Compute shared secret:

$$K' = sk_D\,.R$$

2. Derive AES decryption key:

$$K_{AES} = H(K'_x)$$

3. Decrypt medical record:

$$M = \text{AES} - \text{GCM}^{-1}(K_{AES}, C_D)$$

Step 6. Verify data integrity and authentication

To ensure data integrity and authenticity:

The smart contract verifies the doctor's signature and the transaction using ECDSA:

$$ECDSA - Verify\left(pk_P, Tx_{Request}, \sigma_P\right)$$

Any tampering attempt invalidates the cryptographic signature, ensuring trust.

This algorithm ensures secure patient data exchange by encrypting medical records, enforcing access control via smart contracts and utilizing proxy re-encryption for authorized data sharing.

Algorithm 2. Secure inter-hospital patient data exchange

Input: Patient medical record M, hospital H_1's private key sk_{H_1}, hospital H_2's public key pk_{H_2}, proxy re-encryption key $rk_{H_1 \rightarrow H_2}$
Output: Secure encrypted medical record C_{H_1} and controlled access to H_2

Step 1. Key generation

To facilitate secure data exchange, each hospital generates key pairs:

- Hospital H_1 generates the key pair sk_{H_1}, pk_{H_1}: $pk_{\{H_1\}} = sk_{H_1}.G$
- Hospital H_2 generates the key pair sk_{H_2}, pk_{H_2}: $pk_{H_2} = sk_{H_2}.G$

The proxy uses $rk_{H_1 \rightarrow H_2}$ to mediate access without exposing private keys.

Step 2. Batch data encryption and storage

Each hospital encrypts medical records using ECIES:

1. Compute shared secret: $K = r . pk_{H_1}$
2. Derive AES encryption key: $K_{AES} = H(K_x)$
3. Encrypt M using AES-GCM for confidentiality: $C_{H_1} = AES - GCM(K_{AES}, M)$
4. Store C_{H_1} on IPFS and obtain hash H_{IPFS}. Store metadata on the blockchain to ensure traceability.

Step 3. Batch data retrieval for a doctor from multiple hospitals

Input: Doctor's public key pk_D, re-encryption keys $rk_{Hi \rightarrow D}$ from multiple hospitals *Hi*
Output: Aggregated encrypted medical records from multiple hospitals

1. Doctor submits a single access request to the smart contract.
2. Smart contract verifies authorization and triggers batch re-encryption.
3. Proxy computes re-encryption keys for all hospitals: $rk_{Hi \rightarrow D} = sk_P^{-1}.pk_D$
4. Proxy re-encrypts all records:
$$C_D = \frac{n}{i = 1} \text{ReEncrypt } (C_H, rk_{Hi \rightarrow D})$$
5. Doctor downloads and decrypts all re-encrypted medical records in one step.

This above algorithm supports both single and multiple-hospital exchanges efficiently, reducing communication overheads while ensuring security and privacy.

Algorithm 3. Smart contract for access control using ECDSA

A blockchain smart contract manages authorization:

1. Doctor requests access by signing transaction $Tx_{Request}$ using $ECDSA$.
2. If authorized, then the smart contract triggers re-encryption.
3. Proxy computes re-encryption: $K' = rk_{\{P \rightarrow D\}} * R$.
4. Doctor retrieves H_{IPFS} from the blockchain, downloads C_P and decrypts.

The smart contract automates the process of access control, ensuring secure and transparent authorization for patient data retrieval using message digest.

The above algorithms constitute an overall secure decentralized EHR exchange solution. The combination of ECC, PRE and smart contracts fills important gaps in solutions to data privacy, access control and interoperability, and is computationally efficient. The method guarantees that the solutions are applied in health practice, even within limited- resource systems.

3.6 Security analysis

The proposed HEC-PRE framework has a well-deduced security analysis with mathematically proven claims about its security properties. The ability of the framework to provide a correct proxy re-encryption process, resistance to impersonation and reply attacks as well as protection against collusion and assurance of the authenticity of a transaction is established below.

Theorem 1. Proxy cannot decrypt medical data

Statement: The re-encryption process carried out by the proxy server is such that no one can decrypt the medical information that is exchanged between parties.

Proof: Let us suppose that a patient encrypts their medical information and sends it to a physician. Let the patient's encryption key pair be (sk_P, pk_P) and the doctor's key pair be (sk_D, pk_D). The proxy re-encryption key is computed as:

$$rk_{P \to D} = sk_P^{-1} \cdot pk_D$$

The encrypted data are represented as $C_P = \text{ECIES}(pk_P, M)$,

where the shared secret is derived as:

$$K = r \cdot pk_P = r \cdot (sk_P \cdot G)$$
$$K_{ECIES} = H(K_x)$$

The proxy having only $rk_{P \to D}$ and C_P, cannot derive the shared secret K since it does not posses sk_P. This ensures that the proxy cannot decrypt the data.

Theorem 2. Data integrity with blockchain and ECDSA

Statement: The integrity of medical data is ensured through blockchain transaction logging and digital signatures using ECDSA.

Proof: Each transaction $T_i$related to medical data access is signed by the corresponding entity using their private key sk_i, forming a digital signature:

$$S_i = Sign\big(sk_i, H(T_i)\big)$$

The blockchain stores (T_i, S_i), ensuring that:

- if T_i is modified, the hash $H(T_i)$ changes, rendering S_i invalid. This prevents unauthorized alterations.
- Non-repudiation is ensured as S_i is verifiable using the public key pk_i, confirming identity of the signer.

Thus, the use of ECDSA guarantees data integrity and accountability in the system.

Theorem 3. Secure proxy re-encryption

Statement: The proxy re-encryption process securely transfers access from the patient to the doctor without revealing the plaintext data.

Proof: Assume that the patient encrypts data using pk_P resulting in cipher text C_P. When the proxy re-encrypts the ciphertext for the doctor, the transmission follows:

$$C_D = ReEncrypt(rk_{P \to D}, C_P)$$

The doctor, possessing sk_D, can then decrypt the message as follows:

$$K = sk_D \cdot R = sk_D \cdot (r \cdot G)$$
$$K_{ECIES} = H(K_x)$$
$$M = ECIES^{-1}(K_{ECIES}, C_D)$$

The proxy cannot compute K or K_{ECIES}, without sk_D, and therefore cannot access the plaintext. This ensures access delegation without data exposure.

Theorem 4. Proof of data exchange confirmation

Statement: The exchange of encrypted medical data between two hospitals is cryptographically confirmed and protected against unauthorized access.

Proof: Consider a system where Hospital H_1 encrypts patient data M using ECIES and stores them on an interplanetary file system. When Hospital H_2requests access, the process follows these steps:

1. Hospital H_1 encrypts M using ECIES:

$$C_{H1} = Encrypt(pk_{H1}, M)$$

The IPFS hash H_{IPFS} is recorded on the blockchain.

2. Hospital H_2 submits a digitally signed request T_{H2} to the blockchain.

3. The proxy computes the re-encryption key:

$$rk_{H1 \to H2} = sk_{H1}^{-1} \cdot pk_{H2}$$

The proxy re-encrypts the ciphertext:

$$C_{H2} = ReEncrypt(rk_{H1 \to H2}, C_{H1})$$

4. Hospital H_2 decrypts H_2 using its private key sk_{H2}.

In addition to the individual security properties established in the previous theorems, the formal proof below will show that the HEC-PRE system is highly robust in the context of an assortment of possible real-world security threats, such as insider misuse, MITM attacks, smart contract vulnerabilities and more.

Theorem 5. System-wide security assurance of HEC-PRE against insider threats, smart contract exploits and MITM attacks

Statement: The proposed approach uses ECIES, PRE, and smart contracts to perform access control. Provided that (i) ECIES offers good confidentiality even against chosen ciphertext attacks, (ii) ECDSA ensures that signatures are not forged and (iii) smart contracts to enforce roles and permissions, insider misuse, MITM attacks on proxy nodes and attempts at gaining unauthorized access via smart contract loopholes can all be effectively mitigated.

Proof: Suppose that a patient encrypts a medical data M as:

$$C_P = ECIES\,(pk_P,\ M)$$

The proxy generates a re-encryption key $rk_{P \rightarrow D} = sk_P^{-1} \cdot pk_D$ and re-encrypts C_P to obtain C_D.

A malicious insider or proxy with access to $rk_{P \rightarrow D}$, C_P and C_D, but without sk_D, cannot derive the plaintext *M*, since the session key is calculated as:

$$K = sk_D \cdot (r \cdot G), K_{ECIES} = H(K_x)$$

$$M = ECIES^{-1}\,(K_{ECIES}, C_D)$$

Without knowledge of sk_D, the attacker cannot compute K, so the confidentiality is guaranteed despite the existence of insider attacks or breached proxy servers.

Each access request transaction T_i is signed using the private key sk_i of the requesting party:

$$S_i = Sign\big(sk_i, H(T_i)\big)$$

The smart contract verifies both the signature and the role:

$$Verify\big(pk_i, S_i, H(T_i)\big) \wedge Role(pk_i) = R_i \Rightarrow Access_{Granted}$$

Due to security of ECDSA, attackers are unable to forge S_i without possession of sk_i. Moreover, properly implemented smart contract logic ensures strict role-based access, preventing unauthorized access privilege escalation or bypass.

All the access demands and re-encryption transactions are present in the blockchain and this implies a reliable history of data swaps. Moreover, unauthorized individuals are not able to decipher the information as the re-encryption key does not reveal the plain-text information. This ensures the safety of inter-hospital data sharing as well as traceability. Collectively, the above theorems indicate that the HEC-PRE model is robust and has the capability of facilitating secure, traceable and efficient exchange of EHR in decentralized health systems.

4 RESULTS AND DISCUSSION

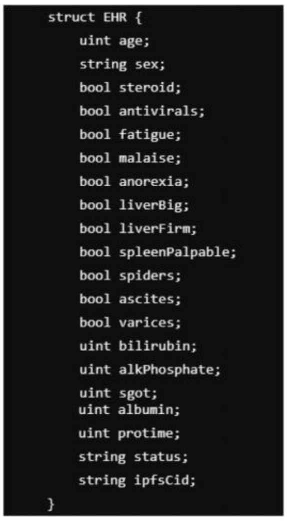
4.1 Method validation

Hepatitis is a severe health problem that is experienced by millions globally. We rely on a hepatitis dataset to prove the validity of our suggested approach on secure exchange of electronic health records (EHRs) between Ethereum and Hyperledger Fabric blockchains. The data sample comprises 155 patient records and 19 attributes, including age, sex, bilirubin levels, antiviral drug therapies, liver firmness, the use of steroids, ascites, prothrombin time, hypersomnia and other important medical health indicators. It was found that the results obtained in terms of the performance of the secure EHR exchange process between Ethereum and Hyperledger Fabric could be assessed based on the gathered data.

In the case of the Ethereum-based EHR blockchain, the testing system is examined on the Holesky test network, due to the fact that Sepolia is deprecated. The use of smart contracts was accomplished with Truffle (v5.11.5) and MetaMask (v11.11.4) was used to communicate with the blockchain. On its Hyperledger Fabric counterpart, a secured enterprise level network was configured with four peer nodes, each committed to the transactions, and one ordering node in charge of consensus. Docker (v18.06.3), Go (v1.13) and Python (v3.9) were chosen to create the network so that it could guarantee the security and optimal data exchange across multiple chains.

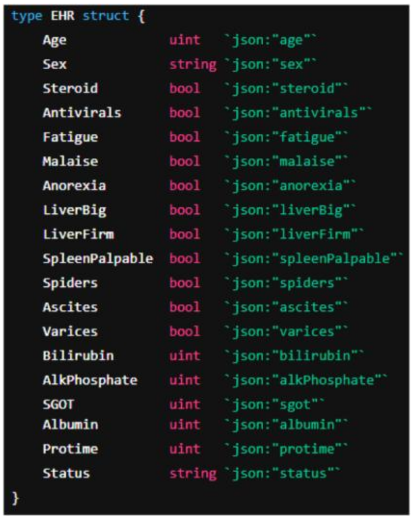
To ensure that the proposed framework maps to the HL7 FHIR standard, the framework incorporates a data transformation model that converts heterogeneous EHR formats into standard FHIR-compliant resources using a structured JSON encoding. This ensures seamless data exchange between multiple healthcare networks. The use of IPFS and metadata in the blockchain is also integrated in a way that it maps onto IHE profiles such as XDS.b (cross-enterprise document sharing), ensuring secure document referencing, verification of information integrity and patient-centric access control.

A configuration of the test environment provided hardware resources that realized maximum benefit of cryptographic and blockchain activities: a vPro processor that has a clock speed of 3.8 GHz, 32 GB RAM, a 512 GB SSD and an 8-core dedicated GPU to perform accelerated encryption and confirmation of transactions. To assure a continuous stream of data, the connection should be stable; 6 Mbps to 1 Gbps should be available. Ethereum and Hyperledger Fabric employ a structured format for managing EHRs. Figures 4–7 show the structure of the dataset attributes in each blockchain system.



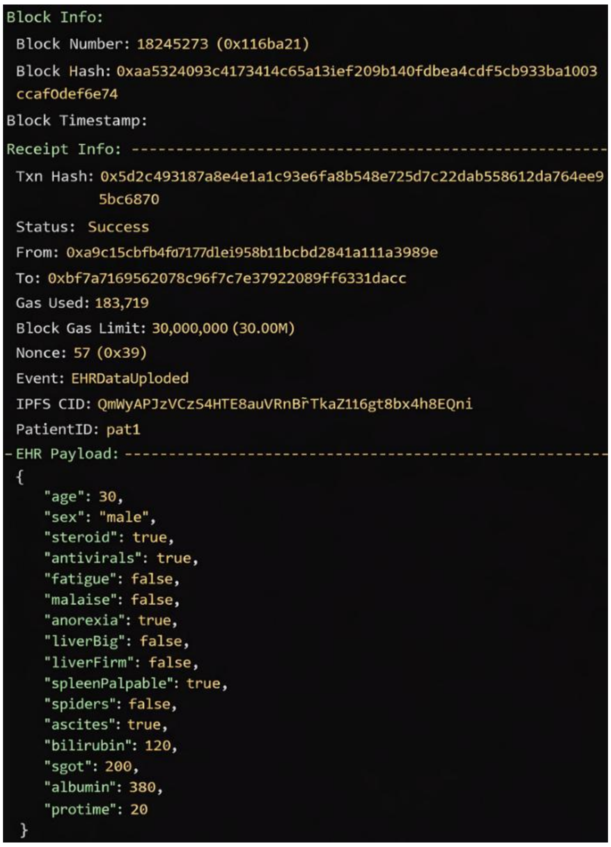
```
    struct EHR {
        uint age;
        string sex;
        bool steroid;
        bool antivirals;
        bool fatigue;
        bool malaise;
        bool anorexia;
        bool liverBig;
        bool liverFirm;
        bool spleenPalpable;
        bool spiders;
        bool ascites;
        bool varices;
        uint bilirubin;
        uint alkPhosphate;
        uint sgot;
        uint albumin;
        uint protime;
        string status;
        string ipfsCid;
    }
```

Figure 4. *Dataset attributes organized for Ethereum.*



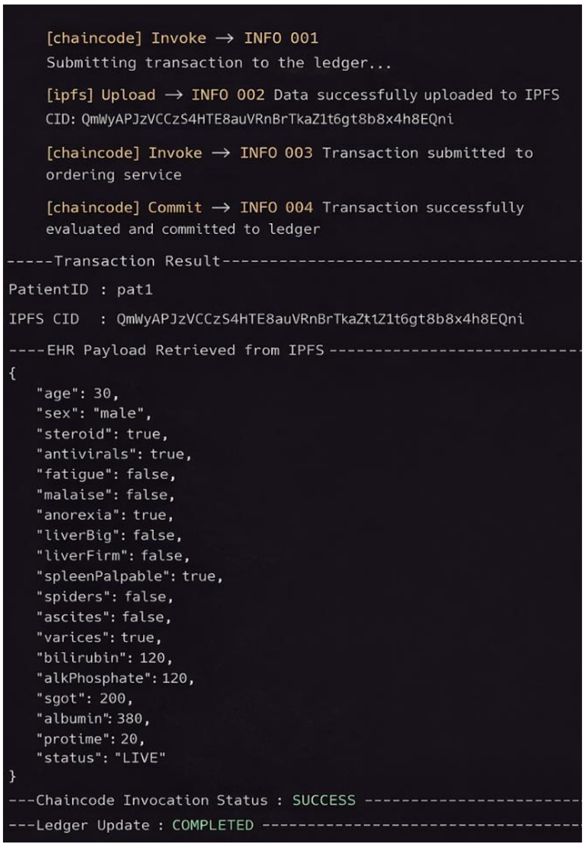
```
type EHR struct {
    Age             uint   `json:"age"`
    Sex             string `json:"sex"`
    Steroid         bool   `json:"steroid"`
    Antivirals      bool   `json:"antivirals"`
    Fatigue         bool   `json:"fatigue"`
    Malaise         bool   `json:"malaise"`
    Anorexia        bool   `json:"anorexia"`
    LiverBig        bool   `json:"liverBig"`
    LiverFirm       bool   `json:"liverFirm"`
    SpleenPalpable  bool   `json:"spleenPalpable"`
    Spiders         bool   `json:"spiders"`
    Ascites         bool   `json:"ascites"`
    Varices         bool   `json:"varices"`
    Bilirubin       uint   `json:"bilirubin"`
    AlkPhosphate    uint   `json:"alkPhosphate"`
    SGOT            uint   `json:"sgot"`
    Albumin         uint   `json:"albumin"`
    Protime         uint   `json:"protime"`
    Status          string `json:"status"`
}
```

Figure 5. *Dataset attributes organized for Hyperledger.*



```
Block Info:
 Block Number: 18245273 (0x116ba21)
 Block Hash: 0xaa5324093c4173414c65a13ief209b140fdbea4cdf5cb933ba1003
 ccaf0def6e74
Block Timestamp:
Receipt Info: ----------------------------------------------------
 Txn Hash: 0x5d2c493187a8e4e1a1c93e6fa8b548e725d7c22dab558612da764ee9
           5bc6870
 Status:  Success
 From: 0xa9c15cbfb4fd7177d1ei958b11bcbd2841a111a3989e
 To: 0xbf7a7169562078c96f7c7e37922089ff6331dacc
 Gas Used: 183,719
 Block Gas Limit: 30,000,000 (30.00M)
 Nonce: 57 (0x39)
 Event: EHRDataUploded
 IPFS CID: QmWyAPJzVCzS4HTE8auVRnBȓTkaZ116gt8bx4h8EQni
 PatientID: pat1
-EHR Payload: ----------------------------------------------------
 {
    "age": 30,
    "sex": "male",
    "steroid": true,
    "antivirals": true,
    "fatigue": false,
    "malaise": false,
    "anorexia": true,
    "liverBig": false,
    "liverFirm": false,
    "spleenPalpable": true,
    "spiders": false,
    "ascites": true,
    "bilirubin": 120,
    "sgot": 200,
    "albumin": 380,
    "protime": 20
 }
```

Figure 6. *Patient data access on Ethereum blockchain.*



```
    [chaincode] Invoke → INFO 001
    Submitting transaction to the ledger...
    [ipfs] Upload → INFO 002 Data successfully uploaded to IPFS
    CID: QmWyAPJzVCCzS4HTE8auVRnBrTkaZ1t6gt8b8x4h8EQni
    [chaincode] Invoke → INFO 003 Transaction submitted to
    ordering service
    [chaincode] Commit → INFO 004 Transaction successfully
    evaluated and committed to ledger
-----Transaction Result--------------------------------------
PatientID  : pat1
IPFS CID   : QmWyAPJzVCCzS4HTE8auVRnBrTkaZt1Z1t6gt8b8x4h8EQni
----EHR Payload Retrieved from IPFS --------------------------
{
   "age": 30,
   "sex": "male",
   "steroid": true,
   "antivirals": true,
   "fatigue": false,
   "malaise": false,
   "anorexia": true,
   "liverBig": false,
   "liverFirm": false,
   "spleenPalpable": true,
   "spiders": false,
   "ascites": false,
   "varices": true,
   "bilirubin": 120,
   "alkPhosphate": 120,
   "sgot": 200,
   "albumin": 380,
   "protime": 20,
   "status": "LIVE"
}
---Chaincode Invocation Status : SUCCESS ---------------------
---Ledger Update : COMPLETED ---------------------------------
```

Figure 7. *Patient data access on Hyperledger Fabric blockchain.*

4.2 Dataset source

The hepatitis dataset utilized in the research was downloaded through the UCI (1983) machine learning dataset[1]. These data are under the Creative Commons license in version 4.0 international (CC BY 4.0), where sharing and adaptation of the data is permitted with proper crediting. The dataset can act as a reference guide to measure the proposed secure and interoperable EHR exchange framework.

4.3 Cross-chain performance evaluation

To check the performance of the proposed cross-chain EHR exchange framework, we considered the impact on the transaction speed and reliability as the cross-chain communication rate between Ethereum and Hyperledger Fabric blockchain becomes higher. Cross-chain transactions are also critical in providing the ability of one isolated blockchain to interact with another. Here we analyse the results for cross-chain interaction between the two blockchain networks and the rate of effects on the system performance and reliability with increasing rates of cross-chain interaction.

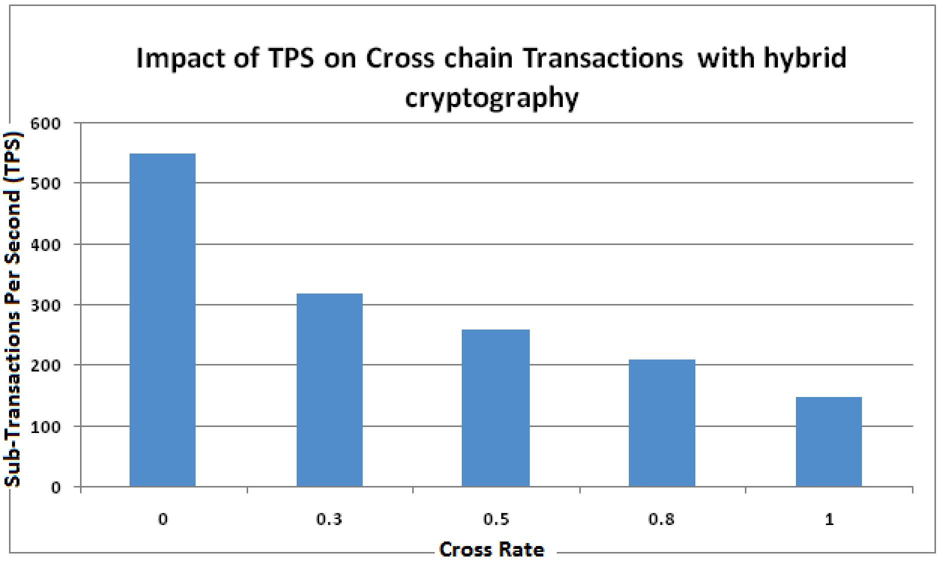


Figure 8. *Effect of cross rate on transaction processing speed (TPS).*

Cross rate is the share of transactions that involves interaction between both Ethereum and Hyperledger Fabric blockchains. The results in Figure 8 show the impact on TPS with the growth of the percentage of cross-chain transactions. A cross rate of 0.0 implies that all the transactions take place in only one blockchain, whereas a cross rate of 1.0 implies that all the transactions are in both blockchains. Figure 9 extends on this analysis adding success rate and cross conflict rate; this offers a comprehensive perspective on how the system is performing as more cross-chain transactions are conducted.

In case each transaction is represented in its own blockchain (cross rate = 0.0), the system will be at its optimal when it comes to a processing time at around 500 TPS. However, with increasing percentage of cross-chain transactions (cross rates = 0.3, 0.5, 0.8 and 1.0), the TPS decreases gradually down to about 130 TPS in the case of 100% percent cross-chain activity. This performance degradation is due to the extra cryptographic operation, validation checks, inter-network communication needed to coordinate cross-chain.

In the proposed approach, when more cross-chain transactions are performed, the system performance with respect to TPS begins to decrease. This is mainly due to additional validations and coordinating operations between the two blockchains. Meanwhile, when the success rate falls, it results in increased delays and operational challenges. Moreover, the conflict rate is higher, which demonstrates that when two or more blockchains take part, there is a higher likelihood of discrepancies or malfunctions.

[1] See, https://doi.org/10.24432/C5Q59J.

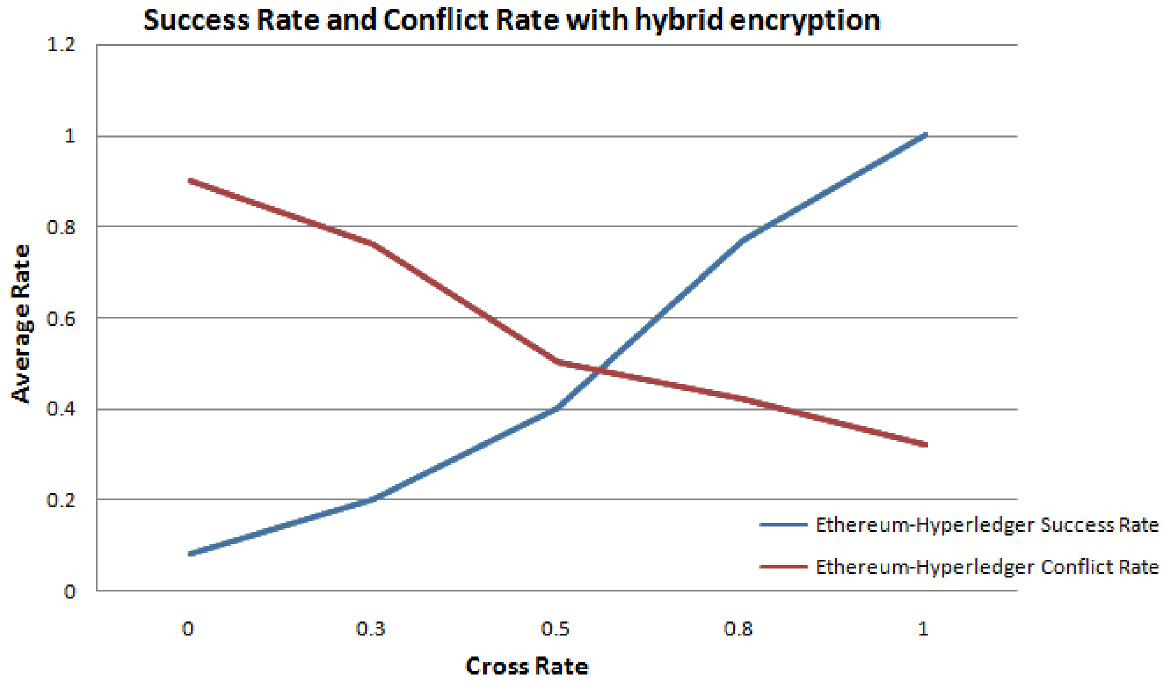


Figure 9. *Impact on TPS, success rate and cross conflict rate.*

4.4 Scalability evaluation

Based on the verification against large medical data, the scalability analysis verifies the behaviour of the LWECC-PRE framework when the size of the dataset under analysis expands from 155 to 2000 records. With increasing dataset size, TPS in Ethereum and Hyperledger Fabric decreases, which shows that larger datasets pose an additional load to the system. Moreover, although the success rate is not significantly changed, the cross conflict rate gets higher, indicating the growing complexity of the management process of the cross-chain transactions, as shown in Figure 10. These findings indicate that, even though the framework is optimized on smaller datasets, it will require some optimizations to achieve better performance on larger datasets.

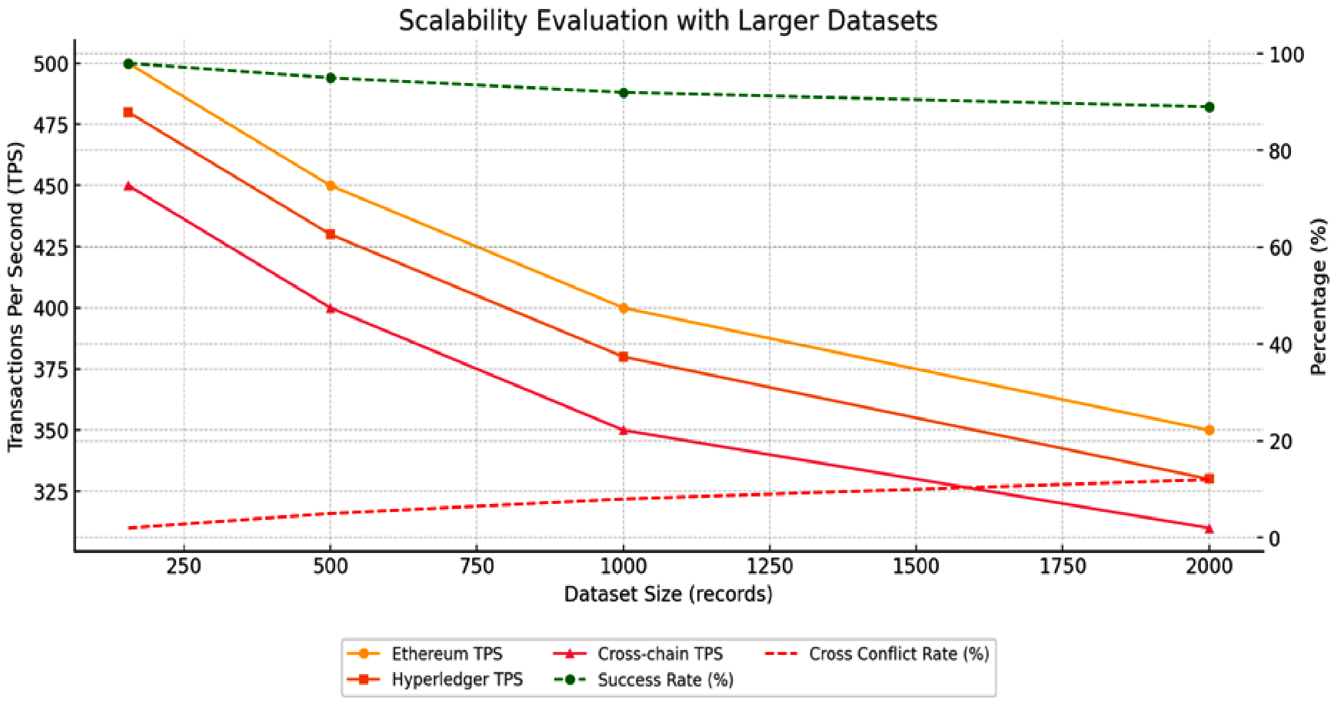


Figure 10. *Scalability evaluation of LWECC-PRE framework across increasing data sizes.*

Based on the above results and discussion, the performance degradation in the proposed approach can be addressed by following some enhancements such as parallelization of cryptographic operations, batch processing of transactions, catching and prefetching and adaptive rate control approaches. These can be considered to improve both scalability and responsiveness without compromising system security. These suggested approaches can be considered in future implementations.

4.5 Execution time analysis of cross-blockchain transactions

The proposed method evaluates the average execution time (ET) of client queries on the Ethereum blockchain (B1). As shown in Figure 11, the first transaction takes longer due to the initial connection setup with Hyperledger (B2). However, once the connection between Ethereum and Hyperledger is established, the execution time for subsequent transactions decreases significantly, demonstrating the efficiency of the system after the initial setup.

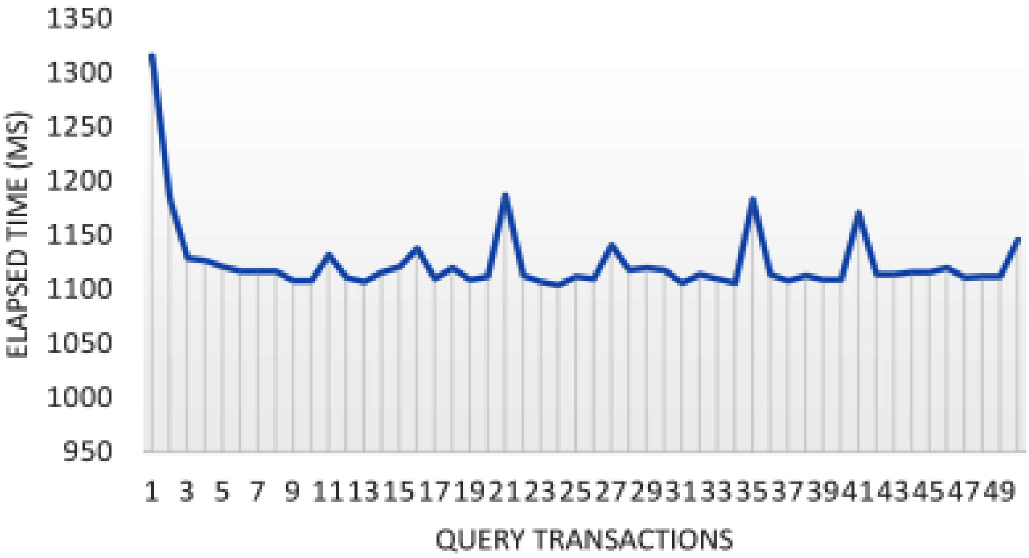


Figure 11. *B1 elapsed time for query transactions.*

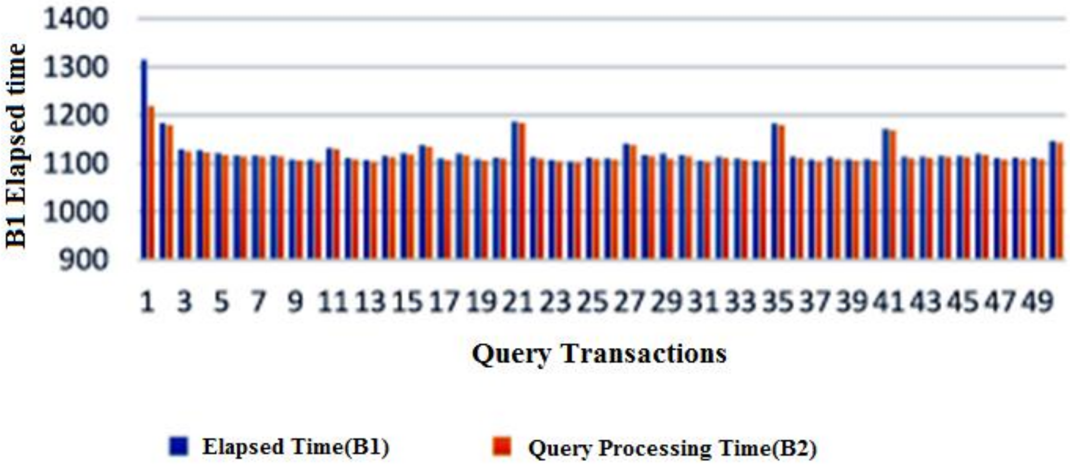


Figure 12. *B1 elapsed time versus B2 query processing time.*

A comparative analysis of Ethereum (B1) and Hyperledger (B2) reveals that B1 execution time is influenced by B2 query processing time (QT). When a client submits a request to Ethereum (B1), it triggers a query to Hyperledger (B2) and waits for the response. Figure 12 illustrates how the B2 nodes process the query in time *t* and send back the requested data to B1. As a result, the total execution time (ET) for Ethereum (B1) is directly affected by the query processing time (QT) of Hyperledger (B2), as highlighted in the corresponding equation.

4.6 Real-world deployment considerations

The current implementation focuses on architectural validation and controlled experimental evaluation. The real-world deployment considerations for healthcare applications are as follows.

Integration with hospital information systems (HIS): As the framework supports standard healthcare interoperability formats such as HL7 FHIR and DICOM, it can be integrated with widely used EHR systems via RESTful APIs.

Patient-centric access control: Via a web-based or mobile dashboard, patients can view, grant or revoke access to their medical data.

Compliance audits and privacy regulations: Blockchain logs keep track of every access and modification request, which supports regulatory audits and traceability as required under global / local health data privacy acts. Smart contracts and proxy re-encryption are used to enforce consent policies so that both access and its compliance is verifiable.

The proposed model is compared with other existing alternatives for EHR privacy preservation and interoperability between the nodes. The results above and in Table 1 highlight the merits of the framework.

Table 1. *Comparative analysis of proposed framework.*

Features	Sonkamble et al. (2024)	Mauricio et al. (2023)	Reegu et al. (2023)	Proposed LWECC-PRE
Encryption time (ms) (2MB of data)	20.3	-	-	12.4
Decryption time (ms) (2MB of data)	22.1	-	-	14.2
Storage overheads (%)	18%	21%	25%	10.3%
Computation costs	Medium (SPAK+ dual chain sync)	Medium	Higher (complex standards)	Low (hash table + ECC)
Interoperability	Yes (Ethereum ↔ Hyperledger)	Yes (FHIR- based clinics)	Yes (multi-standard)	Yes (cross-chain)
Security features	SPAKE + hash locking	FHIR HL7 + smart contracts	Smart contracts + metadata pointers	ECC + proxy re-encryption + IPFS
Throughput (transaction in sec)	120	60-70	90	140
Privacy preservation	Moderate (session-based)	Moderate (smart contract + patient-managed)	Strong (role based + fine-grained access control)	Strong (patient-centric and No plaintext sharing)

4.7 Discussion and future work

Although the proposed framework enables secure sharing of EHRs between Hyperledger Fabric and Ethereum in terms of hybrid elliptic curve proxy re-encryption (HEC-PRE), there are challenges which have not been overcome yet. Scalability still has to be improved; latency also arises in the process of cross-chain transaction since it has to be encrypted and validated; this might reduce the success rate of a transaction. Another issue is security risks, especially in cases of smart contracts. Such contracts need continuous monitoring and auditing to determine weak points. The complexity of implementing a hybrid blockchain system also implies that adequate knowledge of cryptography is critical and lack of it (even in small-scale settings) may lead to inefficiency.

Zero-knowledge proofs (ZKPs) are considered an emerging type of privacy-preserving cryptographic tools and have a promising potential in both healthcare and blockchain (Saroop, 2024). We did not consider these due to the computational complexity and performance overheads. Researchers can consider ZKPs in the case of access verification without identity disclosure and privacy-enhanced audit mechanisms especially where there are federated or public blockchain layers.

Future attempts should put an emphasis on efficiency of encryption, reduced transaction costs and shorter conflict resolution. Moreover, implementing machine learning to identify anomalies and adopting zero-knowledge proofs to enhance privacy may provide the system with superscale capacity, better security and cost-effectiveness in real-life applications in the healthcare field.

5 CONCLUSION

We proposed a secure and efficient method for exchanging EHRs across healthcare service providers, based upon an implementation of an LWECC-PRE mechanism. This approach uses ECIES as an encryption algorithm and ECDSA taking the role of an integrity verifier, ensuring robust protection of patient data while maintaining lightweight design that is suitable for resource-constrained real-world implementation.

One of the major strengths of the suggested model is its support for interoperability, accomplished by using a proxy re-encryption approach without disclosing any sensitive information to intermediaries. Such functionalities are necessary to develop connected healthcare networks in which sharing information in real time would make a huge difference to patient outcomes.

The framework results highlight its strong performance in speed and security, ideal for contemporary healthcare systems, which comprise distributed systems, mobile devices and cloud-based storage. The combination of blockchain and IPFS ensures tamper-proof logs and verifiable proof of data exchange, which is essential for generating trust, auditing and compliance assurance. This paper certainly demonstrates that achieving interoperability and security in balance is achievable – two objectives in healthcare IT that often cannot coexist. Future work will focus on real-life integration, while alignment with standards such as HL7 FHIR and enhancement of consent and identity management can further facilitate further trust and usability.

ABBREVIATIONS, NOTATIONS AND SYMBOLS

Abbreviation	**Full form**
ABE	Attribute-based encryption
AES	Advanced encryption standard
AES-GCM	AES in Galois/counter mode (authenticated encryption)
AI	Artificial intelligence
B1	Ethereum blockchain network
B2	Hyperledger Fabric blockchain network
DApp	Decentralized application
DICOM	Digital imaging and communications in medicine
ECC	Elliptic curve cryptography
ECDH	Elliptic curve Diffie-Hellman
ECIES	Elliptic curve integrated encryption scheme
ECDSA	Elliptic curve digital signature algorithm
EHR	Electronic health record
ET	Execution time
FHIR	Fast healthcare interoperability resources
GCM	Galois/counter mode
HE	Homomorphic encryption
HEC-PRE	Hybrid elliptic curve proxy re-encryption
HIPAA	Health Insurance Portability and Accountability Act
HL7	Health level 7
IoMT	Internet of medical things
IPFS	Interplanetary file system
LWECC-PRE	Lightweight elliptic curve cryptography proxy re-encryption
PHR	Personal health record
PRE	Proxy re-encryption

Abbreviation	Full form
QT	Query time
RSA	Rivest–Shamir–Adleman algorithm
TPS	Transactions per second
UCI	University of California, Irvine

Symbol/Notation	Meaning
sk_P, pk_P	Private key and public key of patient
sk_D, pk_D	Private key and public key of doctor
sk_i, pk_i	Private and public keys of *entity i*
T_i	Transaction *i* on the blockchain
S_i	ECDSA digital signature of transaction T_i
$rk_{\{P \to D\}}$	Re-encryption key from patient to doctor
C_P, C_D	Ciphertexts under patient's and doctor's public keys respectively
K	Shared secret derived via ECDH
$K_{\{ECIES\}}$	Key derived via hash function H(K_x) for ECIES
r	Ephemeral random scalar (for ECIES)
G	Base point on elliptic curve
M	Medical record / plaintext message
$H(\cdot)$	Secure cryptographic hash function
$Encrypt(\quad), Decrypt(\quad)$	Symmetric encryption and decryption operations
$ReEncrypt(\quad)$	Proxy re-encryption operation
ECIES^{-1}()	ECIES decryption operation
Sign(), Verify()	ECDSA signature and verification functions

ADDITIONAL INFORMATION AND DECLARATIONS

Conflict of Interests: The authors declare no conflict of interest.

Author Contributions: D.Y.A: Writing – Reviewing and Editing, Validation, Conceptualization, Project administration. R.P.P.: Conceptualization, Software, Writing – Original draft preparation, Conceptualization, Project administration.

Statement on the Use of Artificial Intelligence Tools: The authors declare that they didn't use artificial intelligence tools for text or other media generation in this article.

Data Availability: The data that support the findings of this study are available from the corresponding author. The used dataset is accessible on https://doi.org/10.24432/C5Q59J.

REFERENCES

Ahmad, H. F., Alhassan, F. M., Haque, A. & Shafqat, S. (2025). A Secure Architecture for Interoperable Personal Health Records (PHR) Based on Blockchain and FHIR. *Journal of Pioneering Medical Sciences*, 14(2), 42–48. https://doi.org/10.47310/jpms2025140207

Ali, A. A., Gunavathie, M. A., Srinivasan, V., Aruna, M., Chennappan, R., & Matheena, M. (2025). Securing electronic health records using blockchain-enabled federated learning for IoT-based smart healthcare. *Clinical eHealth*, 8, 125–133. https://doi.org/10.1016/j.ceh.2025.04.002

Anand, G., & Sadhna, D. (2023). Electronic health record interoperability using FHIR and blockchain: A bibliometric analysis and future perspective. *Perspectives in Clinical Research*, 14(4), 161–166. https://doi.org/10.4103/picr.picr_272_22

Cobrado, U. N., Sharief, S., Regahal, N. G., Zepka, E., Mamauag, M., & Velasco, L. C. (2024). Access control solutions in electronic health record systems: A systematic review. *Informatics in Medicine Unlocked*, 49, 101552. https://doi.org/10.1016/j.imu.2024.101552

Corbin, C. K., Maclay, R., Acharya, A., Mony, S., Punnathanam Thapa, R. S., Kotecha, N., Shah, N. H., & Chen, J. (2023). DEPLOYR: A technical framework for deploying custom real-time machine learning models into the electronic medical record. *Journal of the American Medical Informatics Association*, 30(10), 1532–1542. https://doi.org/10.1093/jamia/ocad114

Ettaloui, N., Arezki, S., & Gadi, T. (2024). Blockchain-based electronic health record: Systematic literature review. *Health & Biomedical Engineering*, 2, Article 4734288. https://doi.org/10.1155/hbe2/4734288

Ferreira, J. C., Elvas, L. B., Correia, R., & Mascarenhas, M. (2024). Enhancing EHR interoperability and security through distributed ledger technology: A review. *Healthcare*, 12(19), 1967. https://doi.org/10.3390/healthcare12191967

George, A., George, J., & Jenkins, J. (2024). Potential effects that health apps on mobile devices may have on patient privacy and confidentiality. *E-Health Telecommunication Systems and Networks*, 13, 23–44. https://doi.org/10.4236/etsn.2024.133003

Hashim, F., Shuaib, K., & Sallabi, F. (2022). Connected Blockchain Federations for Sharing Electronic Health Records. *Cryptography*, 6(3), Article 47. https://doi.org/10.3390/cryptography6030047

Islam, U., Alatawi, M. N., Alqazzaz, A., Alamro, S., Shah, B., & Moreira, F. (2025). A hybrid fog-edge computing architecture for real-time health monitoring in IoMT systems with optimized latency and threat resilience. *Scientific Reports*, 15(1), 25655. https://doi.org/10.1038/s41598-025-09696-3

Jabbar, R., Fetais, N., Krichen, M., & Barkaoui, K. (2020). Blockchain technology for healthcare: Enhancing shared electronic health record interoperability and integrity. In *Proceedings of the 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT),* (pp. 310–317). IEEE. https://doi.org/10.1109/ICIoT48696.2020.9089570

Keshta, I., Aoudni, Y., Sandhu, M., Singh, A., Xalikovich, P. A., Rizwan, A., Soni, M., & Lalar, S. (2023). Blockchain aware proxy re-encryption algorithm-based data sharing scheme. *Physical Communication*, 58, 102048. https://doi.org/10.1016/j.phycom.2023.102048

Kunal, S., Gandhi, P., Rathod, D., Amin, R., & Sharma, S. (2024). Securing patient data in the healthcare industry: A blockchain-driven protocol with advanced encryption. *Journal of Education and Health Promotion*, 13(1), 94. https://doi.org/10.4103/jehp.jehp_984_23

Mishra, R., Kaur, I., Sahu, S., Saxena, S., Malsa, N., & Narwaria, M. (2023). Establishing three layer architecture to improve interoperability in Medicare using smart and strategic API led integration. *SoftwareX*, 22, 101376. https://doi.org/10.1016/j.softx.2023.101376

Mauricio, D., Llanos-Colchado, P. C., Cutipa-Salazar, L. S., Castañeda, P., Chuquimbalqui-Maslucán, R., Rojas-Mezarina, L. ., & Castillo-Sequera, J. L. (2024). Electronic Health Record Interoperability System in Peru Using Blockchain. *International Journal of Online and Biomedical Engineering*, 20(3), 136–153. https://doi.org/10.3991/ijoe.v20i03.44507

Puneeth, R.P., & Parthasarathy, G. (2023). Survey on Security and Interoperability of Electronic Health Record Sharing Using Blockchain Technology. *Acta Informatica Pragensia*, 12(1), 160–178. https://doi.org/10.18267/j.aip.187

Puneeth, R.P., & Parthasarathy, G. (2024). Blockchain-Based Framework for Privacy Preservation and Securing EHR with Patient-Centric Access Control. *Acta Informatica Pragensia*, 13(1), 1–23. https://doi.org/10.18267/j.aip.225

Rajput, A. R., Li, Q., & Ahvanooey, M. T. (2021). A blockchain-based secret-data sharing framework for personal health records in emergency condition. *Healthcare*, 9(2), 206. https://doi.org/10.3390/healthcare9020206

Reegu, F. A., Abas, H., Gulzar, Y., Xin, Q., Alwan, A. A., Jabbari, A., Sonkamble, R. G., & Dziyauddin, R. A. (2023). Blockchain-based framework for interoperable electronic health records for an improved healthcare system. *Sustainability*, 15(15), 6337. https://doi.org/10.3390/su15086337

Saroop, S. (2024). Blockchain-based zero-knowledge proofs for data privacy: Explore the application of blockchain technology in facilitating privacy-preserving transactions through zero-knowledge proofs and analyze their effectiveness in protecting sensitive data. In *Proceedings of the 5th International Conference on Information Management & Machine Intelligence (ICIMMI '23*), (Article 158, pp. 1–8). ACM. https://doi.org/10.1145/3647444.3652463

Semantha, F. H., Azam, S., Shanmugam, B., & Yeo, K. C. (2023). 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*, 12(2), Article 36. https://doi.org/10.3390/jsan12020036

Sharma, P., Kumar, T., & Tyagi, S. S. (2025). A blockchain-based secure framework for interoperability of patient data in electronic health records (EHR). *Fusion: Practice and Applications*, 19(1), 23–37. https://doi.org/10.54216/FPA.190103

Shen, Y., Yu, J., Zhou, J., & Hu, G. (2025). Twenty-five years of evolution and hurdles in electronic health records and interoperability in medical research: Comprehensive review. *Journal of Medical Internet Research*, 27, e59024. https://doi.org/10.2196/59024

Sonkamble, R. G., Bongale, A. M., Phansalkar, S., & Dharrao, D. S. (2024). A secure interoperable method for electronic health records exchange on cross platform blockchain network. *MethodsX*, 13, 103002. https://doi.org/10.1016/j.mex.2024.103002

UCI. (1983). Hepatitis [Dataset]. UCI Machine Learning Repository. https://doi.org/10.24432/C5Q59J

Yan, X., Wu, Q., & Sun, Y. (2020). A homomorphic encryption and privacy protection method based on blockchain and edge computing. *Wireless Communications and Mobile Computing*, 2020, Article ID 8832341. https://doi.org/10.1155/2020/8832341

Acta Informatica Pragensia is published by the Prague University of Economics and Business, Czech Republic | eISSN: 1805-4951