Secure and interoperable electronic health record exchange using blockchain and ECDHE-based access control

Krishna Prasad Narasimha Rao, Selvan Chinnaiyan
School of Computer Science and Engineering, Reva University, Bengaluru, India

Article Info

Article history:

Received May 23, 2025
Revised Dec 28, 2025
Accepted Jan 10, 2026

Keywords:

Access control
Blockchain-based HER
Electronic health records
HFRP
Interplanetary file system
Patient privacy
Patient-centric health-care data management

ABSTRACT

Electronic health records (EHRs) act as comprehensive records of health-related transactions and essential resources of data in the healthcare sector. However, the integrity and security problems of EHR continue to be inflexible. The architecture of blockchain-enabled EHR addresses the issues of integrity efficiently. This paper developed the decentralized patient-centric healthcare data management (PCHDM) system using blockchain-enabled EHR architecture for addressing problems with access control, record privacy and data confidentiality. This framework places the patient at the control center, ensuring secure storage of EHR records and obtaining efficient data management through the integration of blockchain and interplanetary file system (IPFS). To prevent access by unauthorized users, the proposed elliptic curve Diffie-Hellman ephemeral (ECDHE) mechanism incorporates smart contract-enabled access control for managing EHR transactions and enforcing access strategies. This architecture incorporates hyperledger fabric endorsement policies (HFRP) to address scalability problems while preserving patient privacy and securing medical data. The developed method secures the EHR data and facilitates the data exchange across heterogeneous healthcare platforms, ensuring standard communication among different EHR systems. The architecture is assessed with parameters of time for block creation, the computational overhead of transaction with encryption key size and EHR upload and download time.

Corresponding Author:

Krishna Prasad Narasimha Rao
School of Computer Science and Engineering, Reva University
Bengaluru, India
Email: r20pcs09@cit.reva.edu.in

1. INTRODUCTION

Health data is generally stored in databases, which makes it vulnerable to theft and tampering [1]. Therefore, the healthcare data required to be saved electronically for removing issues to exchange the data and visualization of data between healthcare providers [2]. A huge amount of electronic health records (EHR) developed as digital healthcare process [3]. The rapid adoption of EHR demands unparalleled data security in healthcare industry [4]. Additionally, the limitations drawn by COVID-19 on remote process have an importance of security breaks, particularly in situations where confidential patient information is processed online for transmission [5]. Moreover, patients face risks due to the potential exposure of their personal health information [6]. The use of a patient's personal information for various secondary purposes without their consent significantly compromises patient privacy [7].

Apart from information security, patients are allowed to profit financially from sharing their health data. Therefore, system that ensures secure EHR storage and implements an approved retrieval algorithm with patient control and incentive mechanisms is the solution for these issues [8]. The blockchain-based EHR system ensures secure storage of patient data, while its smart contract-dependent method enables secure exchange of records between authenticated users [9]. The audit trail tracking transactions on the blockchain provides opportunities to incentivize data sharing for patients [10]. Though blockchain-based system offers high record storage, as well as offers expensive solutions [11]. Therefore, the blockchain-based system is developed with interplanetary file system (IPFS) for original storage records [12]. It is a cost-effective solution for EHR storage requirements but moreover suffers from the complexity of the algorithm of mapping data records for transactions [13].

Developing blockchain-based applications for patients and providers has the capability of mitigating interoperability barriers among commercial EHR systems. These applications enable patients to have complete control over their healthcare records, granting permission to providers to share data as needed [14], [15]. In this manuscript, integrated design of patient-centric, secure and interoperable EHR exchange framework. Particularly, developed a five-phase interoperability architecture which incorporates health level seven-fast healthcare resources (HL7-FHIR) standardization, smart contract-enabled registries and cross-chain data exchange by wrapper transactions. Moreover, integration of elliptic curve Diffie-Hellman ephemeral (ECDHE) with dynamic, role-based access control (RBAC) and session-level encryption introduced multi-layered security mechanism for real-time, consent-based EHR sharing.

Sonkamble *et al.* [16] suggested the decentralized patient-centered healthcare data management (PCHDM) along blockchain-enabled EHR for handling the challenges of access control, record privacy and confidentiality. For controlling unauthorized users, developed secure password authentication-enabled key exchange (SPAKE) introduced the smart contract-enabled access control for the transaction of EHR and access strategies. Díaz and Kaschel [17] presented the EHR management method depending on entities, and user roles and introduced hyperledger fabric in double-channel configuration. Here, presented prototype implemented in hyperledger fabric by single and double-channel configuration. The presented algorithm provides a solution like the hyperledger fabric platform, which provides an alternative for addressing scalability challenges and for preventing the privacy of the patient and the security of medical information. Mhamdi *et al.* [18] introduced the SEMRAchain device depending access control and smart contract algorithm. The access control mechanisms like RBAC and attribute-BAC (ABAC) were used in this approach. By using blockchain as secure distributed ledger and access control mechanism, the system gives stakeholders with transparency, credibility, immutability and trustworthiness.

Amanat *et al.* [19] introduced the architecture depended on blockchain technology which authenticated a user identity by proof of stake (POS) cryptographic mechanism and secure hash algorithm (SHA256) for securing the sharing of EHR between various electronic healthcare devices. Sammeta and Parthiban [20] implemented the hyperledger blockchain enabled secure medical data management with deep learning enabled diagnosis (HBESDM-DLD) method. Implemented method involved different phases like encryption, generation of optimum key, hyperledger blockchain-enabled secured data management and diagnosis. To enhance the effectiveness of a Simon algorithm, the group teaching optimization algorithm (GTOA) was employed to generate a best key of a Simon algorithm. Kaur *et al.* [21] presented a novel security framework that combined blockchain and software-defined network (SDN) algorithms, zero-trust (ZT) for addressing the issues in latency-sensitive healthcare environments. The presented method enhanced security by integrating an immutable transaction log, ensuring data integrity, and traceability, while supporting dynamic network configurations.

Selvaraj *et al.* [22] suggested the effective adaptive feature centric polynomial (AFCP) data security method. The suggested method is adapted to ensure security for all types of data. The suggested scheme categorized EHR data features into various classes depending on the significance identified from the data. The method enforced a healthy trust access restriction to restrict malicious access. Natarajan *et al.* [23] introduced the secured patient login credential system (PLCS) to EHR data exchange including block encryption with a symmetric and asymmetric mechanism for hospital servers and patients. Moreover, a quantum secure trust protocol (QSTP) was combined to improve trust and security among patients and hospitals, ensuring data security and confidentiality. Though existing HER management systems suffers from critical issues related to data privacy, unauthorized access, lack of patient control and limited interoperability across heterogeneous platforms. Traditional block chain solutions, beneficial in security and auditability still faces challenges in scalability, secure key exchange and effective off-chain data storage. Additionally, many existing algorithms lacks of unified framework that simultaneously ensures secure access control, patient-centric data ownership and seamless interoperability across multiple block chain networks.

The main objective of this manuscript is to develop the block chain-enabled, patient-centric EHR data exchange framework which combines ECDHE for secure key exchange, IPFS for scalable off-chain storage and hyperledger fabric for permissioned block chain access. The developed algorithm aims to ensure dynamic, RBAC by smart contracts, ensures patient authorization in every phase and enables secure and interoperable data sharing across different healthcare entities using HL7-FHIR standards and cross-chain communication protocols. The significant contributions of this manuscript are described as follows:

developed the blockchain-enabled EHR architecture along with on-chain transactions and off-chain storage. Developed ECDHE algorithm for secure smart-contract enabled access control for introduce the patient centrical control on EHR data. The hyperledger fabric endorsement policies (HFRP) rely on on-chain transactions, while an IPFS is used on off-chain storage of EHR data.

This paper is systemized as follows: section 2 gives details of a developed algorithm. Section 3 gives the results and discussion of the proposed model. The conclusion of this research is given in section 4.

2. PROPOSED METHOD

The rapid evolution of healthcare is driven by improved patient care services. The EHRs are numerically saved records containing healthcare relevance data. The healthcare information is simply shared over different healthcare providers because of EHR. This enhances health care by offering accurate health records (HR) in situations. However, device privacy and security protection are challenging to maintain. Blockchain has emerged as a practical technology that is expanding across various industries. Given the need on patient-centric systems and an integration of different systems, blockchain has significant potential in health information. This paper, primarily focuses on blockchain-enabled healthcare data management, emphasizing an exchange of EHR data among healthcare providers and research analyses. The developed method secures a EHR data and facilitates the data exchange across heterogeneous healthcare platforms, ensuring standard communication among different EHR systems. Figure 1 represents the process of blockchain-enabled data exchange for EHR.

Data owner is a patient and it contains ownership across its health data. It can be shared if required. The patient authorization is processed with the ECDHE access control mechanism by utilizing smart contracts. Patients are authorized to grant healthcare providers access to their EHRs, which are shared by providers with patient's permission. The hashes of HER and main attributes are saved on a blockchain and original data in a format of document is saved on IPFS. Therefore, the article aims to create patient-centric EHR system. The challenging problem is to ensure access control and data privacy which is accessed and shared. Developed solution prevents patient privacy on EHRs by the healthcare data-sharing process which involves the restriction of access and data encryption. Additionally, an in-depth analysis of privacy, information security and requirements of access control on blockchain-based security is conducted.

2.1. Data storage of electronic health record

The main aim is to develop an approach to store portions of EHR on blockchain, incorporating standards like HL7-FHIR data standard for blockchain-based data storage. This enabled us to keep track of data about the patient on HER which follows HL7-FHIR standard. Therefore, the HL7 gives a complete analysis of proper EHR handling. Patient centric health-care data management (PCDHM) is the developed solution for the issue. This system is developed using IPFS, a permissioned decentralized storage solution dependent on hyperledger fabric which saves health data with an owner's consent. The cryptographic public key encryption mechanism is taken for encrypting IPFS data for establishing the EHR blockchain device. In a health chain structure method, the Byzantine fault tolerance (BFT) is used for choosing and identifying blocks to include in a blockchain. Figure 1 represents the process of blockchain-based data exchange for EHR and the Figure 2 represents the architecture of interoperability process.

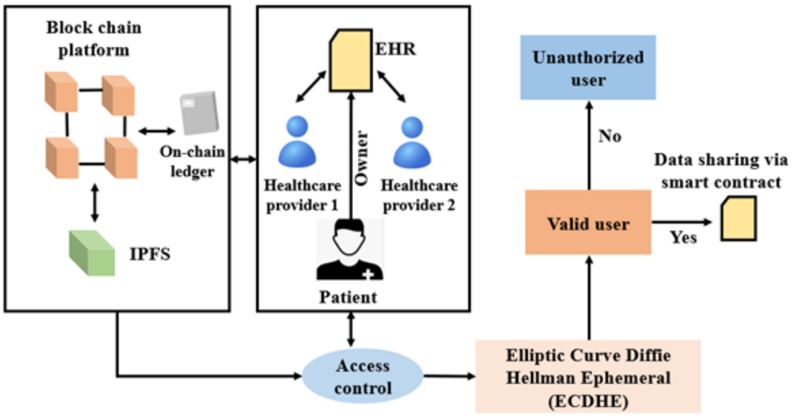

Figure 1. Process of blockchain-enabled data exchange for EHR

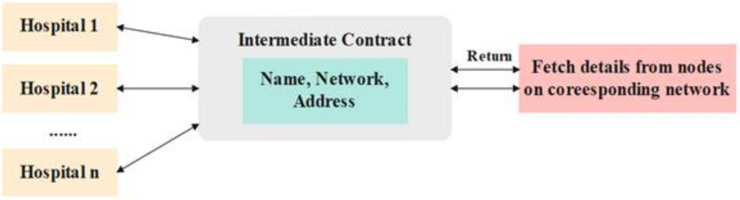

Figure 2. Architecture of interoperability

2.1.1. Interoperability structure

To obtain interoperability, the EHRs follow the general standard. The HL7-FHIR ensured that EHR data was structured and accessible across various blockchain platforms. The HL7-FHIR enables secure data queries and retrievals across hospitals. This ensures the compatibility among hyperledger fabric and other blockchain based health care systems [24], [25]. Figure 2 represents the architecture of the interoperability method. This includes the intermediate contract which includes a name, network and address of every hospital contract. While Hospital 1 needs access to information from Hospital 2, the following steps were followed.

- Switch to in-between contract network.
- Retrieves network and address on Hospital 2.
- Switch to a network in Hospital 2.
- Retrieves components from a contract of Hospital 2.
- Return to an actual contract network and revert information. This procedure permits to security and control of data sharing among various contracts of the hospital.

2.1.2. Cross-chain interoperability

This method allowed the users to direct exchange assists among various blockchains without requiring intermediates. The wrapped tokens in a single blockchain are wrapped to develop the illustration in different blockchains and enable its utilization in various ecosystems. Individual blockchains called sidechains are integrated with the primary blockchain, allows defined tasks to be processed on a sidechain when maintaining integration with a primary chain. Smart contracts act as bridges among various blockchains, facilitating a transmission of information and assisting in their interactions. This platform is developed with attributes of cross-chain interoperability allows several blockchains to be integrated into huge networks. This interoperability enabled utilization of specialized attributes from various blockchains in the specified ecosystem. Assets move seamlessly among blockchains, enabling much more effective usage and trading. Interoperability supports the ease of congestion on one blockchain through distributes the transactions over multiple chains. This interoperability helps the collaboration among various projects and platforms. This interoperability plays an essential part in mitigating the drawbacks of isolated blockchains and developing the much interrelated and adaptable blockchain. Figure 3 represents the architecture of cross-chain interoperability process.

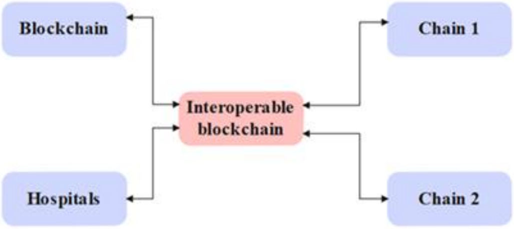

Figure 3. Architecture of cross-chain interoperability

The ecosystem of blockchain continues to validate, and solutions on cross-chain communication and information sharing are essential to obtain major spread adoption and fully realizing a significance on decentralized techniques. Figure 3 represents the architecture of cross-chain interoperability. Interoperability of the proposed blockchain-enabled EHR system, obtained by adopting the HL7-FHIR standards for ensuring data consistency and accessibility across different healthcare platforms. The interoperability structure of the system enables secure and structured queries among hospitals, ensuring that EHRs are handled consistently. Additionally, cross-chain interoperability allows direct data exchange among various blockchains without relying on intermediates, utilizing bridge smart contracts and wrapped tokens. This integration facilitates blockchain features, improves collaboration among healthcare providers and helps overcome network congestion. Hence, these mechanisms are much more adaptable and reliable for digital healthcare infrastructure. Interoperability in blockchain-enabled healthcare data exchange is significant for ensuring seamless communication among various entities like hospitals, diagnostic centers and insurance providers. This research introduced the five-stage interoperability framework which facilitates effective and secure data exchange among blockchain networks.

i) Stage 1: data standardization—in initial phase includes standardizing the patient data by HL7-FHIR framework, which enables structured and interpretable EHR. This ensured that various healthcare systems exchange and process data without compatibility problems.
ii) Stage 2: smart contract—enabled registry for interoperability-the interoperability smart contrast (ISC) is deployed to be considered as a registry that handles metadata of participating hospitals. Registry includes:
    - Hospital identifiers: blockchain addresses.
    - Smart contract IDs: to query the medical records.
    - Access parameters: for data retrieval requests. When Hospital 1 requests the patients' data from Hospital 2, ISC verifies credentials and forwards a request.
iii) Stage 3: secure request and retrieval process—after ISC verifies a request, the data exchange process is given as follows.
    - Hospital A sends the query to ISC with the patient ID and needed medical requests.
    - ISC forwards a request to the smart contract of Hospital 2.
    - Hospital 2 computes access control mechanisms for verifying the authenticity of requesters.
    - Whether verified, the requested EHR is encrypted and transmitted back to Hospital 1 through the blockchain network.
iv) Stage 4: cross-chain interoperability by wrapper transactions—where various blockchain networks are involved, the cross-chain communication protocol is utilized.
    - The requested data is hashed and locked in the origin blockchain.
    - The wrapped token represents data that is produced and sent to the desired blockchain.
    - Receiving hospital redeems a wrapped token to securely access the actual data.
v) Stage 5: secure data decryption and access—receiving an encrypted EHR, Hospital 1 decrypts data by ECDHE key exchange. This ensures end-to-end security and prevents unauthorized access.

2.2. Hyperledger fabric blockchain

In this paper, the user should register to utilize permission-relied hyperledger blockchain network. Mechanism of access control and model on hyperledger is utilized for managing the permission in the network. It is the distributed ledger solution framework, that offers great levels of robustness, adaptability, confidentiality, and scalability. This is supported through a modular structure. As an outcome, the closed blockchain is needed, that maintain the needed privacy. Hyperledger fabric helps multiple authorization layers, allowing information owners to control portion of its information is accessible. This makes a good choice on managing access on healthcare records. Smart contract negotiations followed rules on smart contract storage. Patient-centered healthcare data management access control using smart contract (PCHDMAC-SC) is a framework developed to chain code on a RBAC algorithm. Depending on pre-determined participants, the permissioned blockchain assigns hyperledger fabric for efficiently share health data without relying on one authority. Hyperledger fabric employs a BFT compromises protocol, enabling consensus without the need for native cryptocurrency. The IPFS objects are utilized to replicate through graph tree architecture called as Merkle directed acyclic, act as a state data source to a hyperledger blockchain. The off-chain and on-chain blockchains are designed to store HRs and use IPFS. The precise access control system is designed which uses the hyperledger blockchain and PCHDMAC-SC protocol for avoiding the attacking without patient permission.

2.3. Patient-centered healthcare data management system

This system architecture utilizes three peer nodes for developing the web apps for one organization, utilizing hyperledger creator user permission blockchain depended on hyperledger fabric. Organization utilizes three peer nodes; one acts as validation on the peer node and next act as ordering node to register stakeholders. Multi-peers access a similar data source in the system, which is achieved through IPFS to distribute data storage. Blockchain connectivity is supported by components like information certificate authority, smart contracts, the membership service provider (MSP) and ordered nodes. Multi peers distributed across different locations and machines to evaluate system scalability. This architecture enables smart contracts to access the ledger, with multiple peers distributed across different locations and machines to evaluate system scalability. These peer nodes are integrated into an application, utilizes smart contracts on updating a ledger. The system consists of three peer nodes peernode0 (PE0), peernode1 (PE1) and peernode2 (PE2) everyone maintaining copies on ledger and smart contracts. The one channel in hyperledger composer made the peer transmission feasible. This network develops the transaction and sends that to PE0, PE1, and PE2. The peer install chain nodes depended on transaction execution. For communication with peers, an application assigns chain codes while requesting or modifying a ledger. HR chain network enabled blocks in a blockchain for displaying the hash values as modified in history which made for a framework. Block in ledger, which corresponds to the patient's health record, majorly consists of transactions $WL_{tr(n)}$, present transaction is represented as $WL_{h(n)}$ and hash of past transactions is represented as $WL_{ph(n)}$. By using the $WL_{ToT(n)}$, block workload is determined, and its mathematical formula is given as (1). The EHR includes details like diagnosed disease, recommendation of a doctor, address, position, ID of the hospital, patient profile, further review notes, doctor name, medicine, and scan and test image reports. PCHDM considers a following stakeholder to account.

$$WL_{Tot(n)} = WL_{tr(n)} + WL_{ph(n)} + WL_{h(n)} \tag{1}$$

Record owner—HRs belong to patients. PCHDMAC-SC agreement is signed through the patient and saved on a hyperledger blockchain. Patients control access permission for viewing its healthcare reports by healthcare record chain networks, with each PCHDMAC-SC determining access based on its context.

Data uploader—for data uploaders. The primary responsibility is to upload patient health data by encrypting the clinical information of affected individuals and adding it to IPFS network. The initial transactions are then authorized on a blockchain.

Data users—parties interested in obtaining clinical or health information about patients, such as physicians, insurance companies, hospitals, and researchers are represented as data customers within the data user category. An access control mechanism is offered based on roles. This mechanism allows patients to provide access rights for data users through PCHSMAC-SC.

2.4. Data encryption

Cryptographic algorithms like paring-enabled cryptography, secure cryptography algorithms like proxy re-encryption and public key cryptography offer confidentiality and integrity for blockchain information. The patients and doctors have interaction when access its HRs, doctors give IPFS HRs and next request for accessing the records. This approach enables request-enabled, patient-centric view of records, rather than disclosing a patient's entire information. Session key S_k is encrypted and saved, enabling a patient-centric view of records on IPFS. This key is needed for retrieving records for particular session. Both a session key and encrypted patient-centric views are shared with patients and doctors. Perspective of patient-centric and S_k is decrypted through doctors to update patient HR. The patient is informed to follow an update of IPFS record. The view of patient-centric and S_k is automatically eliminated while HR is committed through a patient. HR access is proscribed for stakeholders till a consent of patient is provided. This method prevents patient privacy. Data hash value is safely saved on the hyperledger blockchain using smart chain code, which processes it in the system's back end. As an outcome, the ledger informs the patient after updating the records successfully.

2.5. Interplanetary file system

IPFS is decentralized storage protocol, employs a specific hash value, depending on the content of the file. This allows for the sharing and permanent storage of different file types using hash values. This process allows the users to identify their files. Moreover, data are effectively protected from saving twice, and that consumes storage space through utilizing a deduplication method on IPFS. Here, a IPFS is utilized for storing the EHR. This is the primary benefit of IPFS to access that instead of position-based addressing. The IPFA allows the distribution of large amounts of information without duplication, which minimizes storage needs and bandwidth costs. This enhances the download rates of records. The IPFS is the immutable storage mechanism and the hash value of IPFS can't be modified. Figure 4 represents the overall transaction of blockchain-enabled EHR data using IPFS.

2.6. Patient-centered healthcare data management access control-smart contract

Doctor requests the permission from patients to access the patient's IPFS HR. The RBAC permission either allows or denies the request for authorized users. After getting the permission of the patient, the doctor develops, and writes and reads the records of patients. Patient commits their record after the writing process to have permanent storage. Patient-centric HRs are accessed through various stakeholders like insurance agents, researchers, and pharmacists in healthcare chain architecture for sessions. Access is granted only if the ownership and object ID match a patient. HR of a patient is updated through laboratory technician with a consent doctor and patient. Hyperledger fabric blockchain manages access control, privacy agreements, and policies which are enforced through a certificate authority. Some settings are followed through the technique described as follows:

i) The identity on every stakeholder granted access is defined through an access control policy.

ii) Authorized value is employed through system for resources, action kinds, stakeholders, and environment features after obtaining patients' approval. There are three layers on privacy in the system:
   - Phase 1: only patients view its HR.
   - Phase 2: the authorized stakeholders have access for HR.
   - Phase 3: the authorized patient caretaker accesses the HR in the emergency.

Patients handle its information privacy through adjusting the privacy phase. Authorizing access before submitting it to authorized EHR users. The method is structured in tiers to accommodate changing conditions.

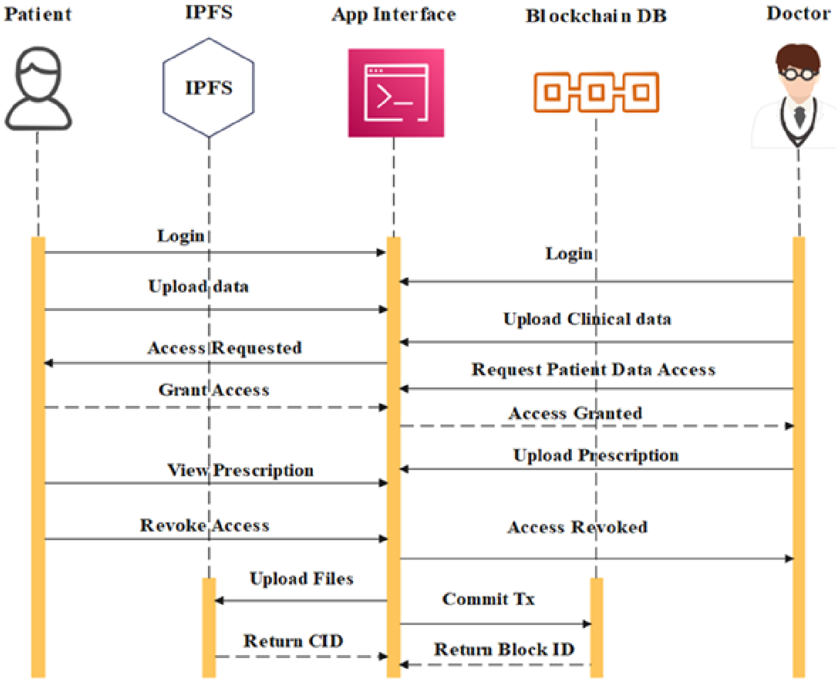

Figure 4. Overall transaction of blockchain-enabled EHR data using IPFS

2.7. Elliptic curve Diffie-Hellman ephemeral

ECDHE is a key exchange technique utilized between client and server, resulting in pre-defined secret shared by parties. In handshake, once client and server agree in cipher suite and curve to be used, both parties establish a common parameter domain. These include the following values.

- p is prima number represented on field F_p.
- a is curve equation parameter.
- $S(u, v)$ is base point coordinates.
- n is order of S, represented as a small integer on $ns = 0$.
- h is co-factor

The process of pre-defined secret arrangement is described as follows. Meanwhile, the ECDHE process is shown in Algorithm 1.

- Server selects random number $k(0 < k < n)$. Next, a server measures kS and send that to a client.
- Client selects random number $k'(0 < k' < n)$. Client measures $k'S$ and send that to a server.
- Client and server, after acquiring ephemeral information k and k', measures a secret of the pre-defined $P = kk'S = k'kS$

Algorithm 1. Process of ECDHE

i) When the valid user requests the access to patient's her, the secure key is established for encrypting the communication.

ii) The ECDHE enabled both the patient and healthcare provider for securely generate the shared secret key without transferring that across the network.

iii) After establishing the shared key, the EHR data is encrypted before the transmission.

iv) Whether the attacker intercepts encrypted data, it can't decrypt that without private keys.

v) Next, the smart contract verifies the user authorization before allowing access to HER data.

vi) Once the valid user is authenticated, ECDHE establishes the secured communication channel.

2.8. Access control and secure data sharing

The access control is the essential device for handling the EHR data and preventing its privacy and security. The rules and identifiers of smart contract are managed through blockchain-enabled controller that ensured pseudo within framework. Ethereum contains numerous features like capability for utilizing the smart contract. The blockchain smart contract supports the user in using its access privileges. As an outcome, the risk of revealing confidential medical information is minimized. The blockchain ensures that the EHRs can't modified arbitrarily. The transfer of secured data is carried out automatically through access permission of patients utilizing the smart contract blockchain. The signature algorithm ensured the secure data transfer. These decentralized system offers the protection of patient-centric privacy to segmentation of EHR information and causes accessed constraints. These devices implement key-enabled access control to secure transactions of EHR using ECDHE, with access restrictions defined in smart contract. EHRs are encrypted by a public key on patients and file sharing is handled through patients. Healthcare providers securely accessed EHRs from remote givers on demanding utilizing cloud computing, time variance, position. Secure medical source sharing which contains message authentication, is facilitated through private cloud environments. The developed system addresses the key threats like Sybil attacks are mitigated by using permissioned hyperledger fabric blockchain, where entire nodes are authenticated through MSP. Key compromise is handled by ECDHE protocol, that ensures forward secrecy through ephemeral key pairs for every session. Replay attacks are prevented through including timestamp validation in smart contracts, rejects reused or delayed messages. Algorithm for ECDHE protocol with smart contract-based access control, included the step-by-step algorithm as shown in Algorithm 2.

Algorithm 2. ECDHE protocol with smart contract-based access control

i) ECDHE key exchange algorithm—the generation of ephemeral key pairs by both parties, shared secret derivation, and encryption of EHR data.

ii) Smart contract access control flow—detailed how patient consent, role-based permissions and request validation are enforced by chain code on hyperledger fabric.

iii) Secure EHR Retrieval process—describes how encrypted data is retrieved from IPFS and decrypted by session key established through ECDHE.

3. EXPERIMENTAL ANALYSIS

The performance of the developed HFRP-ECDHE algorithm is simulated in a cloud environment with the required configuration of an i5 processor, 8 GB RAM and Windows 10 (64-bit). The uploading time, downloading time, execution time, computational overhead and throughput are the metrics considered to evaluate the performance of the developed HFRP-ECDHE algorithm. The evaluation and validation of HFRP-ECDHE algorithm is described as follows.

In proposed HFRP-ECDHE system, key sizes are varied to evaluate its impact on computational overhead and execution. Encryption key length is considered form 16, 64, 128, 256, and 512 bits. Experimental results show that as the key size increases, both computational overhead and execution time also increases due to high complexity involves in encryption and key exchange processes. Table 1 represents the evaluation of computation overhead, execution time and throughput using different key encryption algorithms. Here, the existing algorithms like ECDH, elliptic curve integrated encryption scheme (ECIES) and DHE are simulated based on proposed HFRP-ECDHE simulation parameters. Figure 5 represents an upload time and download time when an information size varied from 20 to 100 MB. While data size maximizes, upload and download time increases. But, a rate of rise in download time is greater than upload time when a block size is increased.

Figure 6 represents computational time with various key sizes. The evaluation is done based on various key sizes like 16, 64, 128, 256, and 512 bits, time consumed for encrypting the record and uploading that into blockchain. This is clear that the computational time increased when key length was increased. However, it needs additional computation time, as longer keys provide higher security against attacks.

Figure 7 represents the execution time with various key sizes. The evaluation is done based on various key sizes like 16, 64, 128, 256 and 512 bits, the time consumed for executing the whole process. This is clear that the execution time increased when the key length was increased.

Figure 8 the uploading and downloading time of IPFS EHR data is represented. It includes the size of data and the uploading and downloading duration of EHR data. Here, the data size is varied from 20 to 100 MB. As shown in Figure 9, as data size of EHR maximizes, time required for upload and download data also maximizes. Figure 9 shows that the transaction throughput is represented which is how many transactions is validated and processed per second. The blockchain batch transaction throughput outcomes are observed under multi-endorsement policies and sent rates of transactions. As the sent rate of blockchain batch transaction increases, mean throughput also increases for 1-of-any, 2-of-any and 3-of-any endorsement policies. From the Figure 6, mean transaction throughput minimizes while the blockchain system maximizes the amount of peers in the endorsement process.

Figure 10 shows the performance of the developed HFRP-ECDHE algorithm is evaluated with different conventional algorithms in terms of computation overhead (ms), execution time (s), and throughput (tps). The conventional mechanisms like elliptic curve cryptography (ECC), rivest Shamir Adleman (RSA) and blowfish in terms of computation overhead (ms), execution time (s), and throughput (tps). Compared to conventional algorithms, the developed HFRP-ECDHE algorithm obtained high throughput and consumed less execution time and computational overhead.

Table 1. Evaluation of HFRP-ECDHE with different encryption algorithms

Metrics	Methods	File size in MB		
		20	30	40
Computation overhead (ms)	ECDH	1.9	2.0	2.5
	ECIES	1.3	1.5	1.9
	DHE	0.9	1.1	1.4
	Proposed HFRP-ECDHE	0.4	0.7	0.9
Execution time (s)	ECDH	36	39	43
	ECIES	32	35	38
	DHE	27	29	34
	Proposed HFRP-ECDHE	22	26	31
Throughput (tps)	ECDH	26	30	35
	ECIES	22	27	31
	DHE	18	23	28
	Proposed HFRP-ECDHE	15	19	23

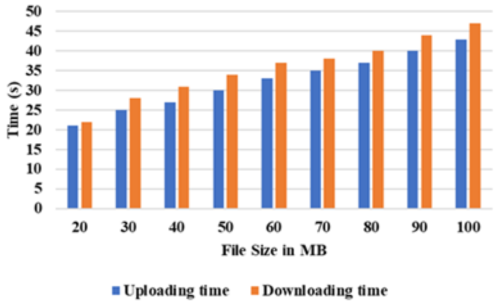

Figure 5. Uploading and downloading time

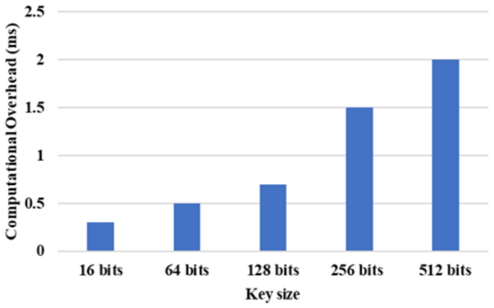

Figure 6. Key size vs computational overhead

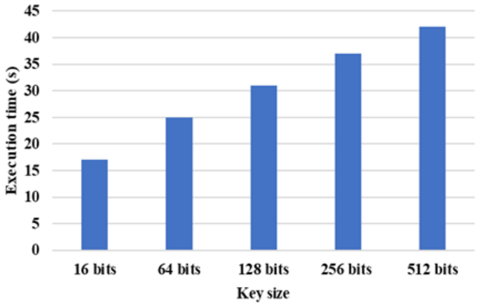

Figure 7. Key size vs execution time

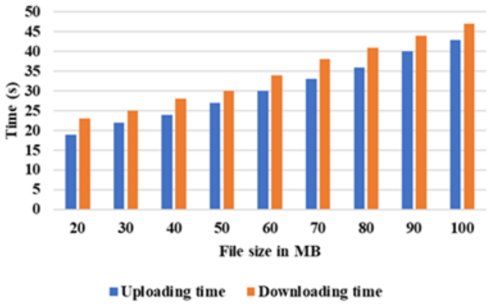

Figure 8. IPFS uploading and downloading of EHR data

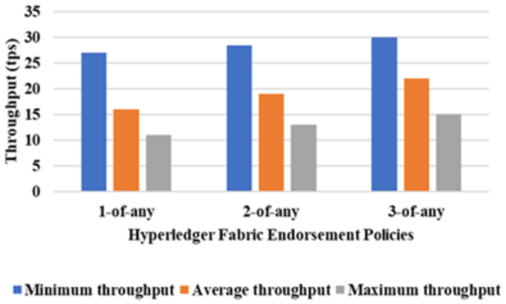

Figure 9. Performance of throughput

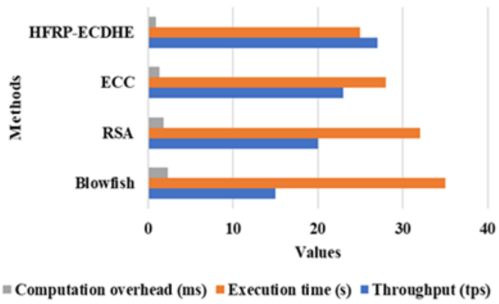

Figure 10. Evaluation with existing algorithms

3.1. Comparative analysis

In this section, the performance of the developed HFRP-ECDHE algorithm is simulated based on existing algorithms and compared to it. The existing algorithms like SPAKE [16] and scalable blockchain based EHR management [17] with different performance metrics are compared in this section. Table 2 shows the performance of the developed HFRP-ECDHE algorithm is compared with SPAKE [16] method with metrics of uploading and downloading time by varying the file size from 20 to 40 MB. Table 3 shows the performance of the developed HFRP-ECDHE algorithm is compared with the SPAKE [16] method with metrics of computational overhead by considering key sizes of 16, 64, 128, 256 and 512 bits. Table 4 shows the performance of the developed HFRP-ECDHE algorithm with metrics of latency and throughput in terms of successful transactions per specified sent rate.

Table 2. Comparison with SPAKE [16] in terms of uploading and downloading time

Metrics	Methods	File size in MB		
		20	30	40
Uploading time	SPAKE [16]	18	20	27
	Proposed HFRP-ECDHE	15	17	21
Downloading time	SPAKE [16]	20	22	32
	Proposed HFRP-ECDHE	17	20	26

Table 3. Comparison with SPAKE [16] in terms of computational overhead

Methods	Computational overhead (ms)				
	16 bits	64 bits	128 bits	256 bits	512 bits
SPAKE [16]	0.6	0.8	0.9	1.5	2.4
Proposed HFRP-ECDHE	0.4	0.6	0.7	1.1	2.0

Table 4. Comparison with scalable blockchain based EHR management [17] in terms of latency and throughput

Metrics	Methods	Successful transactions per specified sent rate			
		997	1000	1000	1000
Latency (s)	Scalable blockchain based EHR management [17]	0.15	0.17	0.24	0.44
	Proposed HFRP-ECDHE	0.12	0.15	0.19	0.35
Throughput (tps)	Scalable blockchain based EHR management [17]	25.0	50.0	94.4	186.2
	Proposed HFRP-ECDHE	28.0	37.2	78.3	123.7

4. CONCLUSION

The blockchain is a significant technology to deploy the digital health-care system because that addresses the issues with access control for EHR data. By utilizing IPFS, this article developed a PCHDM-DL system, which manages access to EHR data. Blockchain smart contracts assist users by utilizing their access rights. By, the ECDHE technique is proposed to secure the transactions of EHR data. The architecture enables access control for patient-centric EHRs using the ECDHE encryption technique. It is evaluated with metrics of time for block creation, the computational overhead of transaction with encryption key size and upload and download time for EHR size. Developed method secures the EHR data and facilitates the data exchange across heterogeneous healthcare platforms, ensuring standard communication among different EHR systems. The proposed architecture resulted in secure EHR transactions that are managed through the RBAC mechanism for data owners (patients). The cross-chain EHR exchange, demonstrates functions of smart contract-based registries and wrapped token mechanisms between two hyperledger fabric networks. Moreover, provided the quantitative results shows latency and data consistency in cross-chain data transfer scenarios by simulated hospital nodes. In future work, the framework traces EHR data based on user requests and personal behavior, enabling user classification based on their interactions and behavioral patterns.

FUNDING INFORMATION

Authors state no funding involved.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Krishna Prasad Narasimha Rao	✓	✓	✓		✓			✓	✓					✓
Selvan Chinnaiyan				✓		✓	✓			✓	✓	✓	✓	

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

The authors declare no conflict of interest.

DATA AVAILABILITY

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

REFERENCES

[1] J.-S. Lee, C.-J. Chew, J.-Y. Liu, Y.-C. Chen, and K.-Y. Tsai, "Medical blockchain: data sharing and privacy preserving of EHR based on smart contract," *Journal of Information Security and Applications*, vol. 65, Mar. 2022, doi: 10.1016/j.jisa.2022.103117.

[2] F. A. Reegu *et al.*, "Blockchain-based framework for interoperable electronic health records for an improved healthcare system," *Sustainability*, vol. 15, no. 8, Apr. 2023, doi: 10.3390/su15086337.

[3] J. K. Oladele *et al.*, "BEHeDaS: a blockchain electronic health data system for secure medical records exchange," *Journal of Computing Theories and Applications*, vol. 1, no. 3, pp. 231–242, Jan. 2024, doi: 10.62411/jcta.9509.

[4] E. A. Mantey, C. Zhou, S. R. Srividhya, S. K. Jain, and B. Sundaravadivazhagan, "Integrated blockchain-deep learning approach for analyzing the electronic health records recommender system," *Frontiers in Public Health*, vol. 10, May 2022, doi: 10.3389/fpubh.2022.905265.

[5] P. Pawar, N. Parolia, S. Shinde, T. O. Edoh, and M. Singh, "eHealthChain—a blockchain-based personal health information management system," *Annals of Telecommunications*, vol. 77, no. 1–2, pp. 33–45, Feb. 2022, doi: 10.1007/s12243-021-00868-6.

[6] 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, pp. 85777–85791, 2022, doi: 10.1109/ACCESS.2022.3198094.

[7] A. Abbas, R. Alroobaea, M. Krichen, S. Rubaiee, S. Vimal, and F. M. Almansour, "Blockchain-assisted secured data management framework for health information analysis based on internet of medical things," *Personal and Ubiquitous Computing*, vol. 28, no. 1, pp. 59–72, Feb. 2024, doi: 10.1007/s00779-021-01583-8.

[8] H. N. Alsuqaih, W. Hamdan, H. Elmessiry, and H. Abulkasim, "An efficient privacy-preserving control mechanism based on blockchain for E-health applications," *Alexandria Engineering Journal*, vol. 73, pp. 159–172, Jul. 2023, doi: 10.1016/j.aej.2023.04.037.

[9] M. Ndzimakhwe, A. Telukdarie, I. Munien, A. Vermeulen, U. K. C.-Okonkwo, and S. P. Philbin, "A framework for user-focused electronic health record system leveraging hyperledger fabric," *Information*, vol. 14, no. 1, Jan. 2023, doi: 10.3390/info14010051.

[10] K. Shuaib, J. Abdella, F. Sallabi, and M. A. Serhani, "Secure decentralized electronic health records sharing system based on blockchains," *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 8, pp. 5045–5058, Sep. 2022, doi: 10.1016/j.jksuci.2021.05.002.

[11] K. Azbeg, O. Ouchetto, and S. J. Andaloussi, "BlockMedCare: a healthcare system based on IoT, blockchain and IPFS for data management security," *Egyptian Informatics Journal*, vol. 23, no. 2, pp. 329–343, Jul. 2022, doi: 10.1016/j.eij.2022.02.004.

[12] M. Maher, I. Khan, and V. Prikshat, "Monetisation of digital health data through a GDPR-compliant and blockchain enabled digital health data marketplace: a proposal to enhance patient's engagement with health data repositories," *International Journal of Information Management Data Insights*, vol. 3, no. 1, Apr. 2023, doi: 10.1016/j.jjimei.2023.100159.

[13] Z. Pang, Y. Yao, Q. Li, X. Zhang, and J. Zhang, "Electronic health records sharing model based on blockchain with checkable state PBFT consensus algorithm," *IEEE Access*, vol. 10, pp. 87803–87815, 2022, doi: 10.1109/ACCESS.2022.3186682.

[14] G. Verma, "Blockchain-based privacy preservation framework for healthcare data in cloud environment," *Journal of Experimental & Theoretical Artificial Intelligence*, vol. 36, no. 1, pp. 147–160, Jan. 2024, doi: 10.1080/0952813X.2022.2135611.

[15] R. Johari, V. Kumar, K. Gupta, and D. P. Vidyarthi, "BLOSOM: blockchain technology for security of medical records," *ICT Express*, vol. 8, no. 1, pp. 56–60, Mar. 2022, doi: 10.1016/j.icte.2021.06.002.

[16] R. G. Sonkamble, A. M. Bongale, S. Phansalkar, A. Sharma, and S. Rajput, "Secure data transmission of electronic health records using blockchain technology," *Electronics*, vol. 12, no. 4, Feb. 2023, doi: 10.3390/electronics12041015.

[17] Á. Díaz and H. Kaschel, "Scalable electronic health record management system using a dual-channel blockchain hyperledger fabric," *Systems*, vol. 11, no. 7, Jul. 2023, doi: 10.3390/systems11070346.

[18] H. Mhamdi, M. Ayadi, A. Ksibi, A. Al-Rasheed, B. O. Soufiene, and S. Hedi, "SEMRAchain: a secure electronic medical record based on blockchain technology," *Electronics*, vol. 11, no. 21, Nov. 2022, doi: 10.3390/electronics11213617.

[19] A. Amanat, M. Rizwan, C. Maple, Y. B. Zikria, A. S. Almadhor, and S. W. Kim, "Blockchain and cloud computing-based secure electronic healthcare records storage and sharing," *Frontiers in Public Health*, vol. 10, Jul. 2022, doi: 10.3389/fpubh.2022.938707.

[20] N. Sammeta and L. Parthiban, "Hyperledger blockchain enabled secure medical record management with deep learning-based diagnosis model," *Complex & Intelligent Systems*, vol. 8, no. 1, pp. 625–640, Feb. 2022, doi: 10.1007/s40747-021-00549-w.

[21] N. Kaur *et al.*, "Securing fog computing in healthcare with a zero-trust approach and blockchain," *EURASIP Journal on Wireless Communications and Networking*, vol. 2025, no. 1, Feb. 2025, doi: 10.1186/s13638-025-02431-6.

[22] D. Selvaraj, J. J. Jasmine, R. Ramani, D. Dhinakaran, and G. Prabaharan, "AFCP data security model for EHR data using blockchain," *Journal of Cybersecurity and Information Management*, vol. 15, no. 1, pp. 22–33, 2025, doi: 10.54216/JCIM.150103.

[23] M. Natarajan, A. Bharathi, C. S. Varun, and S. Selvarajan, "Quantum secure patient login credential system using blockchain for electronic health record sharing framework," *Scientific Reports*, vol. 15, no. 1, Feb. 2025, doi: 10.1038/s41598-025-86658-9.

[24] S. Alsaedi, X. Gao, and T. Gojobori, "Beyond digital twins: the role of foundation models in enhancing the interpretability of multiomics modalities in precision medicine," *FEBS Open Bio*, vol. 15, no. 8, pp. 1192–1208, 2025, doi: 10.1002/2211-5463.70003.

[25] O. K. A., "Leveraging machine learning for predictive models in healthcare to enhance patient outcome management," *International Research Journal of Modernization in Engineering Technology and Science*, vol. 7, no. 1, pp. 1465–1482, 2025, doi: 10.56726/IRJMETS66198.

BIOGRAPHIES OF AUTHORS

Krishna Prasad Narasimha Rao is currently working as a software engineer at Niveus Solutions, Udupi. He completed his M.Tech. in Computer Science and Engineering from NMAMIT in the year 2012. He is currently pursuing his Ph.D. at Reva University, Bengaluru, India. His area of interest includes blockchain and cloud computing. He can be contacted at email: r20pcs09@cit.reva.edu.in.

Selvan Chinnaiyan is currently professor at the Reva University, he has teaching experience of more than 18 years in the areas of mobile and optical communication. He obtained his Ph.D. in University of Mysore and ME in IISC, Bangalore and participated in several high-profile conferences. His research area of interest includes mobile computing and data science. He can be contacted at email: dr.selvan.c@gmail.com.