PRAGUE UNIVERSITY
OF ECONOMICS
AND BUSINESS

Acta Informatica Pragensia
2024, Volume 13, Issue 1, pp. 1–23
https://doi.org/10.18267/j.aip.225

Article Open Access

Blockchain-Based Framework for Privacy Preservation and Securing EHR with Patient-Centric Access Control

Reval Prabhu Puneeth [1,2], Govindaswamy Parthasarathy [1]

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

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

Abstract

The technological advancements in the field of E-healthcare have resulted in unprecedented generation of medical data which increases the risk of data security and privacy. Ensuring the privacy of Electronic Health Records (EHR) has become challenging due to outsourcing of healthcare information in the cloud. This increases the chance of data leakage to unauthorized users and affects the privacy and integrity of the user data. It requires a trustworthy central authority to protect the sensitive patient information from both internal and external attacks. This paper presents a blockchain based privacy preservation framework for securing EHR data. The proposed framework integrates the immutability and decentralized nature of blockchain with advanced cryptographic techniques to ensure the confidentiality, integrity and availability of EHR. The EHR data are stored in an InterPlanetary File System (IPFS) which is encrypted using a hybrid cryptographic algorithm. In addition, a novel smart contact based patient-centric access control is designed in this paper using a blockchain-based SHA-256 hashing algorithm to protect the privacy of patient data. The experimental results show that the proposed framework enables secure sharing of health information between network users with improved data privacy and security. Furthermore, the optimized search process reduces the time and space complexity compared to the traditional search process. Through the utilization of smart contracts, this framework enforces patient-centric access controls and allows patients to manage and authorize access to their medical data.

Keywords

Cryptography; Electronic health records; Encryption; Privacy; Patient-centric access control; Optimized search.

Citation: 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

Academic Editor: Michal Dolezel, Prague University of Economics and Business, Czech Republic

1 Introduction

With the increase in the significance of information and communication technology (ICT), the majority of healthcare organizations are shifting from traditional storage database to electronic health records (EHR). Patient data in EHR are stored in digitized form, which encompasses different types of medical information such as patient medical history, laboratory test reports and sensitive financial information (Kruse et al., 2017). The data stored in EHR are highly unstructured and the volume of EHR data increases on a daily basis due to the extensively conducted medical tests. The large-scale generation of medical data increases the dependency on centralized cloud servers which not only store large volumes of data but also allows users to access the information across the internet (Chenthara et al., 2019; Jin et al., 2019). The increasing implementations of advanced and smart healthcare systems have substantially increased the security risks associated with these systems. Since a majority of the medical data and patient information is highly sensitive and confidential, it is treacherous to depend on third party centralized servers for storage. Third party entities increase the security risks and can lead to attacks such as denial of service (DoS) or distributed denial of service (DDoS) attacks (John and Norman, 2019) and ransomware attacks, which have greater potential to breach the security protocols (Thamer & Alubady, 2021; Gopinath and Olmsted, 2022). Considering the susceptibility of medical data and patient information, it is crucial to secure the data by implementing a robust and efficient technique which can securely store and share the data across multiple stakeholders (Singh et al., 2021; Hathaliya & Tanwar, 2020; Awotunde et al., 2021). The emergence of blockchain technology has brought a significant transformation in various processes such as global supply chain management, decentralized information exchange, asset ledgers, financial transactions and healthcare security management (Rijanto, 2021; Yaqoob et al., 2021).

Blockchain is considered as a potential solution to overcome the drawbacks of centralized and distributed architecture in healthcare applications by introducing a patient-centric electronic healthcare system known as a patient-controlled electronic health record system (PCEHR) (Lee et al., 2022). In this system, patients are the consent providers and can share their private information with multiple stakeholders except in emergency conditions. Blockchain has a decentralized architecture that is immutable and can provide better security for different smart applications, including smart healthcare. Blockchain forms a peer-to-peer (P2P) network, which avoids the dependency on a centralized architecture and is characterized by its superior security performance and excellent attributes such as verification, authentication, decentralization and synchronization. Blockchain incorporates a series of time-stamped transactions called blocks, which are connected to each other to form a chain. The information stored in these blocks is secured using different core strategies such as identity and access management (Mikula & Jacobsen, 2018), key management (Pal et al., 2021), cryptography (Zhai et al., 2019), decentralization and consensus (Patel, 2019). These strategies make it difficult to access and tamper the data stored in the blockchain.

Since all the blocks in the chain are interconnected with each other, it is practically impossible to modify the data stored in the blocks without modifying other subsequent blocks. Among different security strategies available, cryptographic techniques are considered to be the most effective strategy for blockchain security. Cryptographic hash functions such as SHA-224, SHA-256 and SHA-512 are applied to the blockchain for achieving anonymity and immutability and making the blocks tamper-resistant (Guo & Yu, 2022). In addition, blockchain uses consensus algorithms to create and update the transactions and also employs smart contracts to validate the transactions (Bamakan et al., 2020; Garcia et al., 2022). Furthermore, blockchain overcomes problems associated with issues such as interoperability, scalability, integrity, security and privacy in healthcare applications and provides a secure yet robust architecture for medical systems. This research exploits the excellent attributes of blockchain to develop an efficient privacy-preserving framework for securing EHR data with an aim to achieve the patient-centric access control.

One of the major drawbacks in existing healthcare systems is that sensitive patient information is stored in centralized databases, which makes it vulnerable to security threats and attacks. It can be inferred from existing works that the centralized architecture increases security risks due to the dependency on the third party and requires a trusted authority for facilitating secure data exchange. Different types of attacks such as spoofing, eavesdropping, phishing, ransomware and Equifax attacks can affect the privacy and security of EHR (Naser et al., 2022). The information stored in EHR is highly unstructured with different formats and standards. This makes it difficult to share the data with other stakeholders and service providers. Hence, it is challenging to secure the EHR considering its dynamic nature (Keshta and Odeh, 2021).

Another important concern in EHR security is internal attacks caused by insiders or people with authorized credentials in the organization such as database administrators or key managers. These people may pose as attackers and are more dangerous than external attackers. Furthermore, when the patient record is deleted from the database, it is permanently lost from the system. Hence, there is a need to deploy a tamper-proof system which is only accessible to authorized entities. Conventional databases cannot address all these requirements and more advanced technologies should be explored with an emphasis on effective data sharing among multiple entities in the public domain.

In addition, it is crucial to protect the privacy of patient records by providing controlled access to patient records for different entities such as laboratories, physicians, etc. In existing systems, the patients do not have complete control over their EHR data, since the data are usually handled by service providers. Due to the increasing volume of healthcare data, it is challenging to store the data securely without affecting the scalability. Besides, the susceptibility of healthcare data makes it complicated to share the data among stakeholders in the public domain. Existing privacy-preserving techniques are not robust enough to provide foolproof security for EHR in the cloud. Despite the availability of different techniques for EHR security, there is a lack of an effective model which can protect the privacy and integrity of EHR data with patient-centric access control. These challenges and concerns motivate this research to employ blockchain for developing an efficient framework for securing EHR data. In this work, a blockchain-based patient preservation framework is designed to effectively share data and patient records with robust access control. The patient-centric framework proposed in this work overcomes most of the challenges and complexities associated with traditional access control mechanisms and record search processes by implementing a distributed platform.

The main contributions of this study can be summarized as follows:

- This paper designs and develops a novel patient-centric security approach to improve privacy of patient medical information.
- An off-chain storage approach is implemented for storing EHR data.
- A hybrid cryptographic technique comprising the advanced encryption standard (AES), elliptic curve integrated encryption scheme (ECIES) and elliptic curve digital signature algorithm (ECDSA) is employed in this research to achieve privacy preservation and secure EHR sharing.
- A novel and optimized search approach is presented in this paper to extract relevant records, which improves the computation time of the blockchain model.
- The performance of the proposed approach is validated by comparing it with existing schemes in terms of data privacy, integration, user authentication, confidentiality, scalability, access control and optimized search process.

The rest of the paper is organized as follows: Section 2 reviews the related works on security of EHR data using blockchain technologies. Section 3 discusses the proposed methodology and system architecture for developing a robust blockchain-based privacy preservation framework for securing EHR data. Section 4 provides a brief explanation of the patient-centric access control mechanism and implementation of smart contracts for optimized search. Section 5 presents the experimental results and performance evaluation and Section 6 concludes the paper with prominent research observations.

2 Related Works

This section starts with a brief overview of the current literature on privacy preservation techniques and medical data storage approaches adopted by other researchers. Paul et al. (2023) pointed out the growing volume of medical data, conventional centralized data storage servers and the use of databases failing to meet the privacy and security requirements of healthcare organization, as further discussed in the other articles (Cerchione et al., 2023; Gupta et al., 2023), thus increasing the risk of data leakage. To overcome the limitations of these conventional data storage techniques and to strengthen the security of sensitive medical data, recent research works have emphasized the application of blockchain to achieve effective privacy preservation and secure exchange of medical data among multiple entities (Escorcia et al., 2023; Luong & Park, 2023; Singh et al., 2022). The study presented by Sharma et al. (2023a) designed a secure proposed application (PA) using blockchain for generating, maintaining and validating health certificates. The PA connects blockchain with different modules of healthcare systems such as doctors, patients and hospitals in an IoT network for verifying the authenticity of medical certificates. Improved data confidentiality with better access control is achieved through smart contracts, which strengthens the security compared to other techniques. A similar approach for privacy preservation using a blockchain-based distributed application (DA) was implemented by Sharma et al. (2023b) for creating and maintaining medical certificates. The DA acts as an interface between different medical entities and blockchain for issuing medical certificates. The security of these certificates is ensured using smart contracts and the efficiency of the DA is validated in terms of latency, response time and operational costs.

Nath et al. (2023) classified different privacy-improving methods and evaluated their effectiveness in terms of achieving confidentiality. In addition, they identified potential security threats, issues and concerns related to IoT-based medical applications. They modified the traditional expensive blockchain to make it appropriate for resource-constrained IoT devices which depend on the distributed nature and other security attributes of the system. These requirements are satisfied using advanced cryptographic techniques.

Ghayvat et al. (2022) integrated blockchain with a confidentiality and privacy (CP) technique to design a novel approach known as CP-BDHCA which is operated in two stages. In the first stage, an elliptic curve cryptography (ECC)-based digital signature (HCA-ECC) scheme is implemented to achieve a secure communication between different healthcare organizations using a secure session key. In the second stage, a two-step authentication scheme is implemented which combines two cryptographic techniques namely Rivest-Shamir-Adleman (RSA) and Advanced Encryption Standard(AES) for safeguarding the system against potential threats. An authentication-based encryption approach is proposed by Joe and Raj (2021) to secure sharing of medical image data. A searchable encryption algorithm is implemented for secure data sharing with improved traceability and resistance to data tampering using blockchain technology. The proposed approach overcomes the limitations of existing blockchain networks such as high power consumption and storage requirements. The authentication approach is resilient to attacks such as keyword guessing attacks along with privacy protection, verification and authorization. Considering these factors, the study states that it requires advanced methods to provide better security for data senders. A blockchain-based privacy preservation approach for medical image fusion is proposed by Xiang et al. (2023). The model is designed using an integrated model combining a convolutional neural network and an inception network, which are used along with the consensus mechanism of blockchain. The proposed approach provides theoretical analysis about security and privacy requirements, and validates it practically through implementation. However, the need for secure and effective encryption methods and appropriate consensus protocols is still defiant.

A brief review of blockchain-based security solutions for IoT-based healthcare system was presented by Raj and Prakash (2023). The efficacy of blockchain is analysed in terms of different aspects such as data integrity, secure data sharing, distributed EHR, access control, etc. Important security issues in IoT-based healthcare system are discussed and different challenges related to blockchain implementation are highlighted, which provides a better insight for the researchers to obtain detailed information about the security of IoT-based healthcare systems. Zhu et al. (2023) discussed recent technologies such as ledger databases having provided an efficient way to build a secure database system which supports verified data processing. Though the ledger database system provides tamper-evidence with high performance, these systems employ different trust assumptions and depend on a centralized service provider and a trusted entity to identify whether the server data are tampered with or not. A deep reinforcement learning-aware blockchain-based task scheduling (DRLBTS) framework was proposed by Lakhan et al. (2023) to overcome drawbacks associated with issues such as security and a complex processing approach. The proposed approach effectively provides security and task scheduling for healthcare applications. However, the proposed approach is not tested for real-time applications.

It can be inferred from existing literature that privacy preservation of medical data and secure exchange of information among different entities is still a challenging task, especially when data are shared with third-party entities involving smart contracts. It can also be observed that few research works have focused only on security and privacy along with secure data sharing and there is a great need for investigations focusing on issues such as data availability and patient-centric approaches with optimized search processes. These issues are the exact concerns of this paper. In addition, this research also identifies some prominent research gaps, which are as follows:

- Cloud-based electronic health record sharing schemes have been used extensively to share patient records among various healthcare organizations. However, centralized cloud architecture might pose a significant threat to patients' privacy and security.
- Patient access is considered another limitation in the EHR process**,** wherein patients do not have immediate access to their complete EHR. In addition, providers do not need to ask for patient consent to share information for a patient's general care in the case of transfers. In other words, a patient is not always aware about who is accessing their health records.
- The encryption methods used in some of the blockchain-based security models are not effective and scalable to support large-scale and real-time medical data.
- Issues such as scheduling and offloading tasks are often associated with high energy consumption. Several studies (Mohammed et al., 2023; Lakhan et al., 2022a; Lakhan et al., 2022b; Lakhan et al., 2022c) have addressed these issues using neural networks and federated learning and fog computing techniques. However, there is an incessant need to explore more on the implementation of these techniques for providing controlled access to patient records.

This study aims to address these research gaps by designing a patient-centric access control approach with an optimized search mechanism. A brief description of the proposed framework is discussed in the next section.

3 Overview of Proposed Framework

The present study designs and implements a privacy preservation approach using blockchain with an emphasis on patient-centric access control. The proposed framework consists of different modules such as cryptography for data encryption and authentication, off-chain storage for storing EHR data, hashing algorithm, smart contracts for access control and optimized search. The system architecture of the patient-centric approach is discussed in the section below.

3.1 System architecture

The blockchain is designed as a P2P network and does not provide access for unauthorized entities. The system architecture of the proposed approach is shown in Figure 1. The system architecture illustrates different functional modules of the proposed blockchain-based patient-centric architecture for privacy preservation, each represented using a rectangular box. A public blockchain known as Ethereum is used as a common data sharing platform for connecting different entities such as EHR users (hospitals, doctors) with EHR owners. The nodes in the blockchain store the data of each patient using off-chain storage known as the InterPlanetary File System (IPFS), and the data are encrypted using a cryptographic technique. In the proposed architecture, the access control is realized using smart contracts, which help in strengthening the security and maintaining user data privacy. The proposed architecture is composed of four modules. The first module is related to EHR management wherein patients, doctors and hospital administrators are considered to be EHR users. This module enables the participation of different hospitals and allows patients to share their EHR data. The second module is the blockchain platform which can create decentralized, immutable EHR whose data are stored in the IPFS. The third module is related to the registration of EHR owners, wherein the owner can register themselves by providing details such as EHR ID, access list and private key details. The EHR data are encrypted using an encryption key and digital signature, which is further verified and decrypted by the EHR users. The fourth module is related to access control, wherein the access control list provided by the EHR owner is verified using smart contracts. This module enables the modification of access control lists and provides better access privileges.

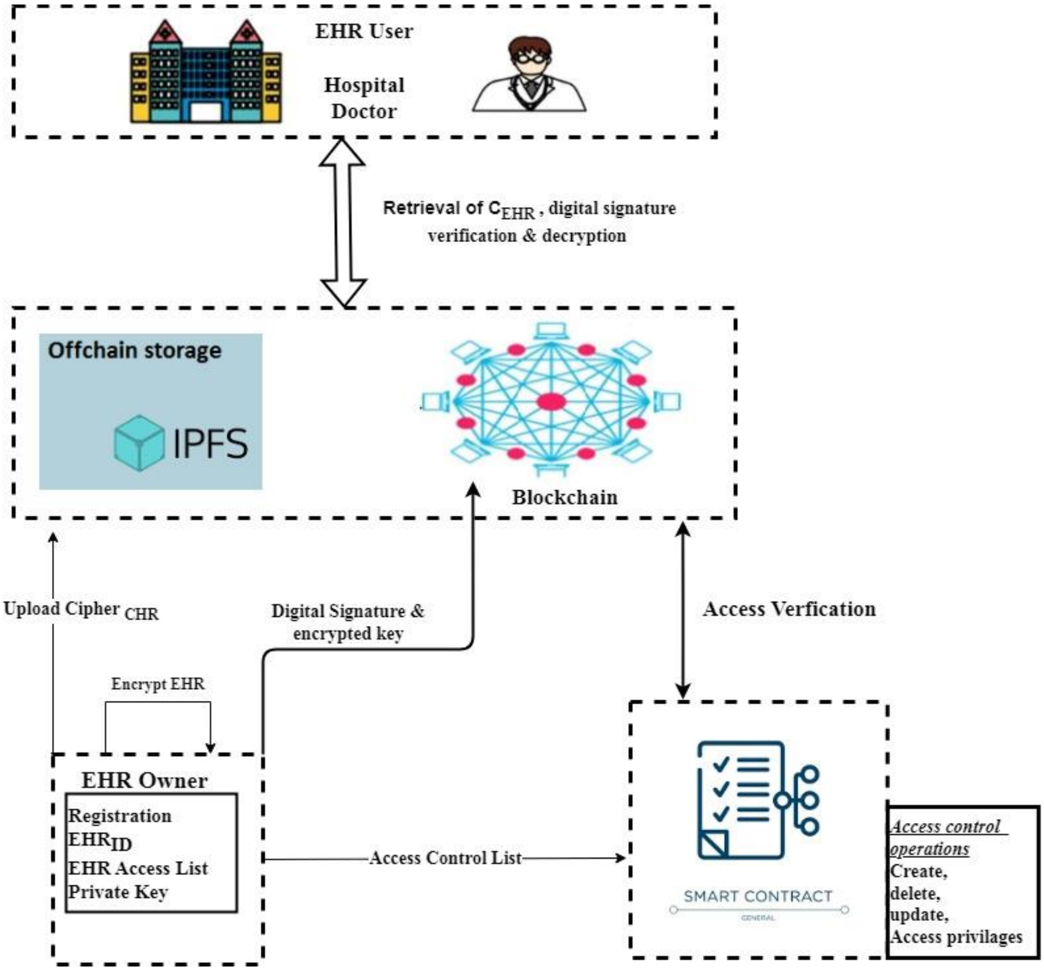


Figure 1. *Patient-centric access control architecture for privacy preservation.*

3.2 Cryptography using hybrid encryption

A hybrid cryptographic technique is employed in this study for securing the EHR data. The hybrid cryptography combines both symmetric and asymmetric cryptography. Symmetric cryptographic methods use the same key for encrypting and decrypting the data and this key is called a private key. On the other hand asymmetric techniques use different keys for encryption and decryption and this key is called a public key.

However, asymmetric techniques require a complex mathematical computation which makes them less efficient compared to symmetric key cryptosystems. In addition, the high costs of encrypting long messages using public keys restricts its adaptability in most cryptographic applications. To overcome this problem, this research employs a hybrid cryptographic approach, which combines both asymmetric and symmetric techniques. The integration of both these techniques greatly reduces the encryption duration compared to implementation of asymmetric methods alone. Moreover, exploitation of arbitrary keys, particularly in the case of symmetric encryption, solves the session-key distribution issue. Additionally, it strengthens the encryption technique. The hybrid cryptosystem is designed using two separate cryptographic techniques, namely, a key encapsulation mechanism using a public key, and a data encapsulation scheme using a private key. The techniques and steps involved in the hybrid encryption process are discussed below.

3.2.1 Data encryption using AES

The AES is one of the widely used cryptographic algorithms because of its high computational speed and better storage requirements. In addition, the AES has a shorter encryption time with faster response and simple design compared to other techniques (Puneeth & Parthasarthy, 2023; Sharma & Chopra, 2017). The block length of the AES is 128 bits and it uses three block ciphers namely 128, 192 or 256 bits. During encryption, an initial key is added to the input which is preceded by 9 rounds of normal rounds and completes the process with a transformed final stage. There are several processing rounds based on the block sizes; for instance, the AES takes 10 rounds for the 128-bit key and 12 and 14 rounds for the 192-bit key and the 256-bit key respectively. The steps involved the encryption process of the AES algorithm are as follows:

- ***Key Expansion:*** In this stage, a Rijndael's key schedule is employed for calculating the round key using a cipher key.
- ***Initial Round:*** An Add round key with a bitwise XOR operation is used for combining the bytes of each state with the obtained round key.
- ***Different Processing Rounds:*** Here, the processing is performed using sub bytes, shift rows and mix columns. In sub bytes, each byte is substituted with another byte according to the lookup table. The shifting of rows is also termed a transposition step, wherein each row is shifted in a cyclic manner for a desired number of times. In the mix column stage, four bytes of each column will be aggregated to form a state matrix.
- ***Final Round:*** Similar to the processing rounds, the final round will have three rounds, namely sub bytes, shift rows and add round key. However, there is no mixing of columns in the final round.

While decrypting the data, the processing rounds remain the same but an inverse operation of the processing round will be performed. For example, in encryption if it is sub bytes, then during decryption, an inverse sub byte will be executed. Similarly for the other two operations, an inverse operation exists. When applied to encrypting EHR data, the data are encrypted as follows:

- The AES algorithm copies and divides an input array of 16 bytes into a matrix of 4 x 4, called state.
- A XOR operation is performed on the obtained state (input EHR data) using the initial 128 bits of the cipher key.
- Further, the EHR data are subjected to different processing rounds and the output obtained from the last round is considered the encrypted EHR data.

The encryption process of AES using a 128-bit key is shown in Figure 2.

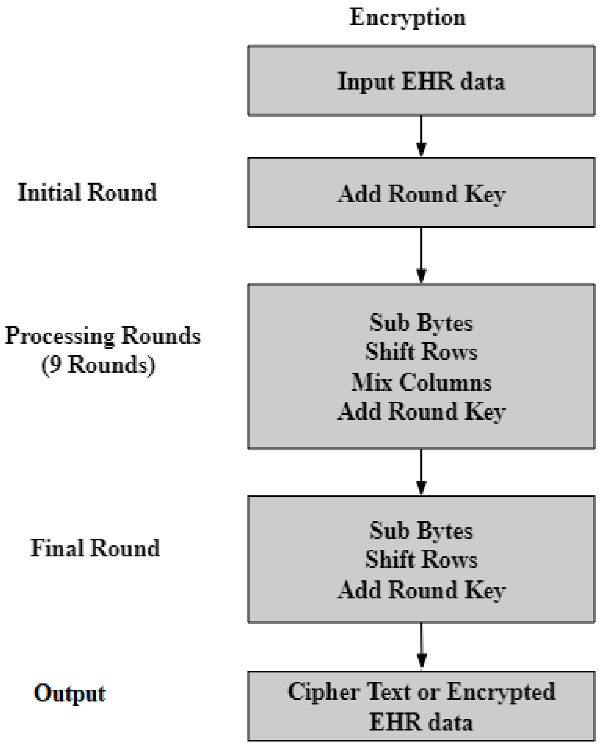


Figure 2. *AES encryption process.*

3.2.2 Key encryption using ECIES

An ECIES is a public-key based encryption technique which combines an ECC-based asymmetric cryptography with a symmetric cipher for encrypting the data. In general, it is challenging to implement public key methods considering the complexity of the design process. The ECC uses a smaller key size for ensuring secure key generation and authentication and transmitting the keys with a lesser bandwidth across a network (Velmurugadass et al., 2021). The ECIES uses an encryption and decryption process wherein plaintext is encrypted and is converted into cipher text and the user will decrypt the encrypted information. During encryption, the data are mapped to a particular point on the elliptic curve and then the point is converted into the message type and the mapped data are evaluated using the elliptic curve equation. The data are encrypted using a private key and the corresponding cipher text is decrypted later using an appropriate public key.

The ECIES algorithm selects a point on an elliptic curve G and a private key is generated by selecting a random number. This number is considered the gradient of the line between x and y coordinates. On the curve, a point X is selected as a private key. An elliptic curve is generally represented by Equation (1).

$$E_P(a, b): y^2 = x^3 + ax + b \tag{1}$$

Where x and y are the variables and a and b are defined as the constants for an elliptic curve with the discriminant $\triangle = -16\ (4a^3 + 27b^2)$ where $\triangle \neq 0$. Considering x and y to be the elliptic curve coordinates, the curve equation is now modified as follows:

$$y^2 \bmod p = (x^3 + ax + b) \bmod p \tag{2}$$

Here, p is considered an integer set. These integers are used to set the points on the elliptic curve thereby forming a cyclic group of the elliptic curve. Using the integer set, the elliptic curve is encrypted and to strengthen the security of the key, it is integrated with an integrated encryption scheme (IES).

Using the ECIES, a pair of public keys are generated where in a sender generates a random private key denoted as *(RP_A P_A)* and selects a point on the elliptic curve *(G)*. Using these, the public key of the sender is determined *(PK_A)* as shown in Equation (3).

$$PK_A = RP_A \ x \ G \ and \ PK_A = P_A \ x \ G \qquad (3)$$

Where, *G* and PK_A are defined as points on the elliptic curve. When an EHR user sends PK_A to the receiver, the receiver will generate a key $R = r \ x \ G$, $S = r \ x \ PK_A$, where *r* is the random number generated by the receiver. The EHR data sent by the user are encrypted using a symmetric key *(S)*. Now, the EHR user will receive the encrypted message along with *R* and the user can obtain the same encryption key using Equation (4):

$$S = RP_A \ x \ R \qquad (4)$$

The symmetric key defined in Equation (4) can be further modified as shown in the equations below:

$$S = RP_A \ x \ (r \ x \ G) \qquad (5)$$

$$S = r \ x \ (RP_A \ x \ G) \qquad (6)$$

$$S = r \ x \ PK_A \qquad (7)$$

Finally, the symmetric key shown in Equation (7) is used for encrypting the key while sharing the EHR data.

3.2.3 ECDSA for authentication through digital signature

This research employs a cryptography-based digital signature algorithm known as the ECDSA for securing the EHR data and achieving anonymity along with security and data privacy. Using ECDSA, two prominent security verifications can be performed i.e. signature correctness and signers anonymity.

- ***Signature correctness:*** Any signature which is valid will be accepted and invalid signatures will be rejected.
- ***Signer's anonymity:*** A signature is made by the user using a public key. Hence, the identity of the user (also known as signer) will be hidden and is not visible to the peers in the network and it is not possible for one to find out the identity of the real signature holder. This plays an important role in enhancing the data privacy in the network.

The ECDSA is executed in three stages, namely a key pair generation, signature generation and signature verification, which are discussed as follows:

(i) Key Pair Generation: The key pair is generated by using a random integer $d \in [1, n\text{-}1]$ selected by the signer. Further, the public and private key is computed as follows:

$$Q = dG \qquad (8)$$

For *x* and *y* users, Equation (8) is modified as:

$$Q = (x_Q, y_Q) \qquad (9)$$

Here, *Q* is the public key and *d* is the private key.

(ii) Signature Generation: A random integer is selected by the signer denoted as $k \in [1, n\text{-}1]$. The integer is computed as $kG = (x_1, y_1)$ and $r = x_1 \ (mod \ n)$. If $r = 0$ then the integer is selected again. The inverse of the integer is computed as $k^{-1} \ (mod \ n)$. The hashing of the message *M* (here EHR data) is computed as SHA-1 (*M*) and the bit string is converted into an integer represented as $h = (Hash \ (M) = h)$. Further, the signature of the message is determined as $s = k^{-1} (h + dr) \pmod n$. If $s = 0$, then another random integer has to be selected. Finally, the signature for the message sent is given as $M (r, s)$.

(iii) Signature Verification: The terms r and s are verified and the integers selected for verifying the signatures are given as $r, s \in [1, n\text{-}1]$. It is further computed as $w = s^{-1} \pmod n$. The hashing is performed using SHA-1 (M) and the bit string is converted into an integer h $(Hash (M) = h)$. Further, two variables u and v are used for validating the signature. Let $u_1 = hw \pmod n$, $u_2 = rw \pmod n$ and compute $(x_1, y_1) = u_1G + u_2Q$, $v = x_1 \pmod n$. If $v = r$, then the signature is considered valid: otherwise it is considered invalid. After verifying the signature, it is important to provide proof of the signature verification process. The steps involved in this process are as follows:

$$(x_1, y_1) = u_1G + u_2Q \tag{10}$$

Substituting the values of kG, hw, rw and w in Equation (10), the signature verification can be proved.

$$kG = u_1G + u_2Q$$

$$kG = hwG + rwQ$$

$$kG = hs^{-1}G + rs^{-1}Q$$

$$kG = hs^{-1}G + rs^{-1}dG$$

$$k = s^{-1} (h + dr) \tag{11}$$

Hence, the signature verification is proved.

3.3 IPFS storage

Off-chain storage and a decentralized IPFS is used to ensure the security of the storage platform and avoid the changes of single point of failure. In this research, the immutable attribute of blockchain is leveraged to securely store the EHR data in the IPFS platform. The EHR data can be stored permanently with different types of files. Here, each file is assigned with a unique hash value, which makes it easy to identify and access the files. In addition, the IPFS incorporates a deduplication technique which avoids duplicate storing of data and hence saves storage space.

For a specific patient, a doctor can add the respective EHR containing details about the patient such as PatientID (PID), diagnosis, prescription, etc and upload the file containing the patient's report. The report containing EHR data is securely stored in the IPFS, which is a peer-to-peer network. The users (peers) located in any part of the world can access this information and store it for further use. Instead of relying on location details, the IPFS uses the content address of the file which connects the IPFS hosts for identification. After uploading the file into the IPFS, a unique content ID (CID) is assigned to each file. The CID is a 24-character hash ID which can be used to identify the file. The integrity of the file is ensured by recalculating the hash when it is retrieved. The report file's hash ID is then saved, along with the other information. Further, a JSON file with all the information and the file hash is created and published in the IPFS network. The patient's PID and the hash ID of the JSON file are added to the smart contract as records.

4 Patient-centric Access Control and Optimized Search Approach

4.1 Patient-centric access control

The proposed patient-centric access control allows the patient to decide with whom the data can be shared and update the shared doctors list. This provides complete control and ownership for the patients to read, edit or revoke access permission to other entities apart from the authorized entities and theory by maintaining secure access control. The patient-centric access control is designed using blockchain-based smart contracts along with the ECIES and ECDSA algorithms.

The main purpose of deploying smart contracts is to control and update the viewer access entry in a patient-service provider contract, wherein a new permission is granted for each viewer to access the information. The smart contract deployed in this research is executed every time a new data request is received by the blockchain. The contract identifies the requester's permission and authenticates the details before granting access. If the user details are authenticated, then the access information will be sent along with the hash of the EHR. Here, user details are authenticated using an encryption algorithm. The smart contract incorporates six important transactions namely data storage, shared EHR data, provide data access, update access for shared EHR, delete or revoke access and update the shared signature. The smart contracts for patient-centric access control are given in Code block 1.

Code block 1. *Smart contract functions.*

```
//View Medical record returns EHR for given patient id
 function viewMedRec(address id) public view returns
(MedRec memory)
 {
 return (Records[id]);
}
// get Shared Document for Doctor
function getPatRecord(address _owner, address _docID)
public
view
returns (ShareDoc memory)
{
return Shares[_owner][_docID];
}
```

```
//Share EHR with given docID with encrypted SK and signature
function shareMedRec(address _owner, address _docID, string
memory _sign, string memory _ck, uint8 _access) external
onlyPatient {
ShareDoc storage share = Shares[_owner][_docID];
share.owner = _owner;
share.docID = _docID;
share.sign = _sign;
share.ck = _ck;
share.access = _access;
Records[_owner].doctors.push(_docID);
}
```

```
//get shared Doctors for given patient
function getSharedDoctors(address _id)
public view
returns (ShareDoc[] memory)
{
MedRec storage rec = Records[_id];
ShareDoc[] memory _shareDocs = new
ShareDoc[](rec.doctors.length);
for (uint256 i = 0; i < rec.doctors.length; i++) {
if (Shares[_id][rec.doctors[i]].owner != address(0)) {
_shareDocs[i] = Shares[_id][rec.doctors[i]];
}  } return _shareDocs;   }
```

```
//update shared access for shared HER
function updateAccess(
 address _owner,
address _docID,
 uint8 _access
 ) public {
 Shares[_owner][_docID].access = _access;
 }
```

//delete shared doctor access	//update Shared Signature
function deleteAccess(address _owner, address _docID) public {	function updateSharedSign(address _owner, string memory _sign)
delete Shares[_owner][_docID];	public {
MedRec storage rec = Records[_owner];	MedRec storage rec = Records[_owner];
for (uint256 i = 0; i < rec.doctors.length; i++) {	for (uint256 i = 0; i < rec.doctors.length; i++) {
if (rec.doctors[i] == _docID) {	if (rec.doctors[i] != address(0)) {
delete rec.doctors[i];	Shares[_owner][rec.doctors[i]].sign = _sign;
}}}	}}}}

Initially, the medical records in the form of EHR for a given patient are viewed and stored. Each record consists of information such as owner and document address, patient ID, etc. In the second stage, the EHR data are shared with the corresponding doctor ID using an encrypted symmetric key and signature wherein the key is encrypted using an ECIES technique and the signature is verified using ECDSA. Here, the data of each patient are shared with the doctors by providing the address ID and record storage ID. Before sharing the data, the user has to submit a request for data access stating the type of EHR data which need to be accessed. The smart contract for access locates the EHR requested by the patient using the summary contract and checks the respective viewer-permission in the hash table. If the feature vector of the requested EHR matches with the user's access vector then the access details are provided for the user along with the requested EHR. Further, the shared access for each EHR is updated by using an update access function. The access provided for the doctor can be deleted or revoked based on the requirements. In the last stage, the shared signature is updated in order to strengthen the access control.

4.2 Optimized search process

In the traditional search process, the records are directly saved in the smart contract. All of the records included in the contract have to be compared because the PIDs are used as a metric for searching the records. As a result, the time required for searching increases *{O (m*n)}* which also increases the time complexity *{O(n)}* and space complexity to store the matching data. Here, *m* and *n* represent the number of patients and records respectively. In the proposed technique, a hash table with PIDs and the corresponding indexes that hold the records for each PID is created. In this approach, only the matching records have to be reviewed instead of viewing all records. This reduces the time required for searching the records. Now the time required for the search process is reduced to *{O (m+n)}* and corresponding time and space complexity is also reduced to *{O (m+n)}*. This shows that the proposed optimized search process successfully decreased the time complexity significantly with just an additional space of *O (m)*. The smart contracts for inserting and searching the records in the traditional approach and the proposed optimized search approach are given below.

4.2.1 Traditional Approach

The traditional approach discussed by Boumezbeur and Zarour (2022) implements a smart contract for inserting and searching of records using a Solidity-based algorithm as shown Code block 2.

Code block 2. *Solidity-based algorithm.*

```
Begin procedure AddRecordBF(string memory hashval , string memory pid):-
Step 1: Take the IPFS hash of the record and add it along with the pid into the Records data structure. i.e., Records.push(phealthrec(hashval,pid));
End procedure;


Begin procedure SearchRecordBF(string memory id):- with the return type of values( phealthrec[] memory)
Step 1: Declare variable i of type uint256;
Step 2: SET FilteredData =  Empty;
Step 3: Repeat step 3 to 6 while i < Records.length;
Step 4: if keccak256(abi.encodePacked
((Records[i].PID)))==keccak256(abi.encodePacked(pid))
            then :
Step 5: Perform adding of data in to
FilteredData.push(Records[i]) ;
End of if block;
Step 6: SET i := i + 1
End of for block;
          Return FilteredData
End procedure;
```

An Abstract Data Type known as phealthrec is declared using a Hash of the type string, PID of the type string and an array variable. The phealthrec consists of both the Hash and PID values of the structure members using which an array of the structure is created called Records. In the traditional approach, the hash value of the IPFS record is used for inserting the EHR data and the PID values are added along with it into the data structure of the records. For searching the respective EHR, a dummy data structure called FilteredData is used which store the matching records. The FilteredData function is initialized into an empty list while beginning the search process. Further, the searching process is carried out through all the records. In Solidity, it is not practically feasible to compare the strings directly and hence the hash values are compared to verify the records. If the hash value matches with the records, then they are added into the FilteredData. This shows that in the traditional approach, it is required to go through each and every record for finding the records, which is a complex and time-consuming process, which is discussed previously as the *{O (m*n)}* concept. This complexity is addressed using the proposed optimized approach which is discussed below.

4.2.2 Proposed optimized approach

Similar to the traditional approach, the optimized approach also uses a phealthrec structure which contains hash and PID values with an array called Records. Unlike the traditional approach, a structure similar to the hash table is created in the optimized search process which contains the PID and an array containing the details of the respective index where the records are stored. The process of inserting the

EHR data is similar to that of the traditional approach wherein a hash value of the IPFS record is used and is added into the Records along with the PID value. In addition to this, the optimized search process checks for the presence of other records belonging to the same patient in the structure. If the records are present, then the latest index is added to the corresponding PID in the hash table. Otherwise a new entry is created in the hash table and the latest index is added to it.

In the searching process, instead of searching the entire record list the proposed optimized process checks whether the PID is present in the hash table. If the PID is present, then the records present in the index are selected, stored in the hash table and then added to the FilteredData. In this way, the exact record indexes are used to find the records and the complexity of the search process is reduced to *{O (m + n)}* as discussed previously. The smart contract for inserting and searching of records using the proposed optimized approach is given in Code block 3.

Code block 3. *The proposed optimized approach.*

```
Begin procedure
AddRecord(string memory hashval , string memory pid):-
Step1:  Take the IPFS hash of the record and add it along with the pid into the Records data structure.
                    i.e., Records.push(phealthrec(hashval,pid));
Step 2: Declare the variables i and flag=0;
Step 3: Repeat step 3 to 4 while i < HashList.length;
Step 4: check if (keccak256(abi.encodePacked (HashList [i].pid))==      keccak256 (abi.encodePacked  (pid) ))
                       Then:
Step 5: Store the index of the record in the hash list ;
i.e., HashList[i].indexes.push(Records. length);
Step 6: set  flag = 1; go to step 7;
            End of if block;
End of for block;
Step 7: check if flag!=1
            Then:
Step 8: declare a new integer array and assign the
Records.length;
i.e., uint256[] memory arr = new uint256[](1);
arr[0] = Records.length;
Step 9: Add to hashlist;
HashList.push(hashtable(pid, arr));
End of if block;
End procedure
```

```
Begin procedure
SearchRecordBF(string memory pid):- with the return type of values( phealthrec[] memory)
Step 1: Declare variable i and j of type uint256;
Step 2: SET FilteredData := Empty;
Step 3: Repeat step 3 to 6 while i < HashList.length;
              // check whether the pid is present in hashtable
Step 4:  ifkeccak256(abi.encodePacked
((HashList[i].pid)))
           ==keccak256(abi.encodePacked(pid))))
            Then :
Step 5: Repeat step 5 to 6
while i < HashList[i].indexes.length;
Step 6:FilteredData.push(Records[HashList[i].
 indexes[j]-1]); // If it is present,we select the
records present in the index stored in the
hashtable and are hence added to FilteredData.
End of Forblock;
End of if block;
End of for block;
Step 7: return the FilteredData
End procedure;
```

Since the proposed approach searches only exact record indexes, the time required for the search process and the complexity is reduced significantly.

5 Results

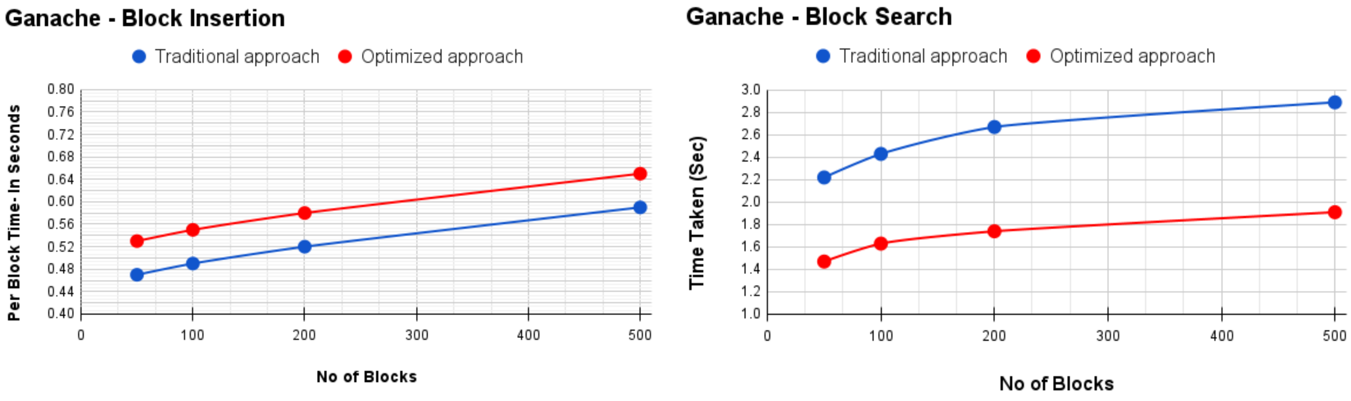
The performance of the proposed approach is experimentally evaluated using a public blockchain platform, Ethereum with a system configuration of Windows 10 with an Intel Core i3 @ 1 GHz processor and 4 GB memory. A solidity platform is used for developing smart contracts and an Ethereum framework with Ganache and Sepolia. The performance is tested on both the testnets as well as the local Ganache server. Like any other Ethereum testnet, Sepolia has an average transaction time of 10-15, seconds which is not feasible for a large dataset. Hence, Ganache is used for performance evaluation, which is independent of the network speed. Thus, using local Ganache readings, the readings can be predicted for Sepolia. The results of the Ganache framework are illustrated in Table 1.

Table 1. *Results of Ganache framework (in seconds).*

No of Records	50	100	200	500
Insert - Traditional	23.51	49.77	100.616	261.30

Per Block Time	0.47	0.49	0.52	0.59
Searching - Traditional	2.22	2.43	2.67	2.89
Insert - Optimized	25.52	50.25	105.75	294.73
Per Block Time	0.53	0.55	0.58	0.65
Search - Optimized	1.47	1.63	1.74	1.91

A comparison of the traditional and proposed search approaches is shown in Figure 3.



(a) (b)

Figure 3. *Insertion and search process using Ganache Framework.*

It can be inferred from the above figure that despite the minor increase in the insertion time, the slope of the optimal search line is flat compared to the traditional search line. Correspondingly, the results of the Sepolia framework are discussed in Table 2.

Table 2. *Results of Sepolia framework (in seconds).*

No. of Records	50	100	200	500
Insert traditional	719.75	~1441.55	~2884.37	~7220.30
Per block time	14.39	~14.46	~14.52	~14.85
Searching traditional	15.39	~15.62	~15.84	~16.06
Insert optimized	751.95	~1504.25	~3010.75	~7555.73
Per block time	14.72	~14.83	~14.92	~15.25
Searching optimized	14.01	~14.17	~14.28	~14.45

A comparison of the traditional and proposed search approaches is shown in Figure 4.

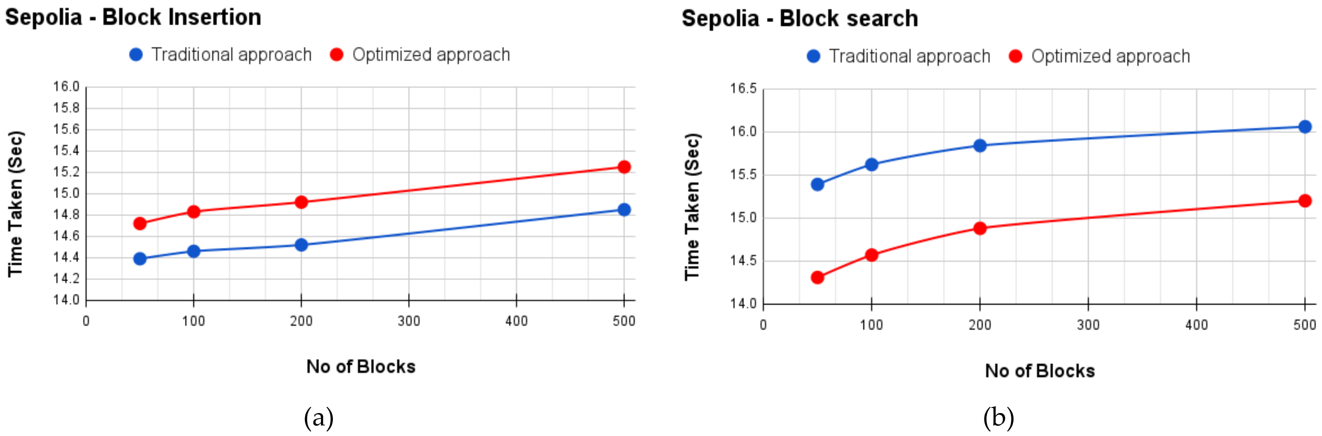


Figure 4. *Insertion and search process using Sepolia framework.*

The scalability of the proposed approach is achieved using the IPFS approach (Puneeth & Parthasarathy, 2021; Rao & Manvi, 2023). The experimental analysis shows that the proposed system can process large datasets with low latency. Data provenance is also achieved by securing user information in the blockchain and thereby provides non-repudiation. The smart contracts deployed for securing EHR provide high-level encryption and ensure the privacy and confidentiality of the EHR data. Further, the proposed system is designed to strengthen the scalability of EHR data by storing the hashes on chain and real-time information in the off-chain IPFS. The scalability of IPFS using EHR (document) data and image data is illustrated in Figures 5 and 6 with a size comparison up to 100 MB.

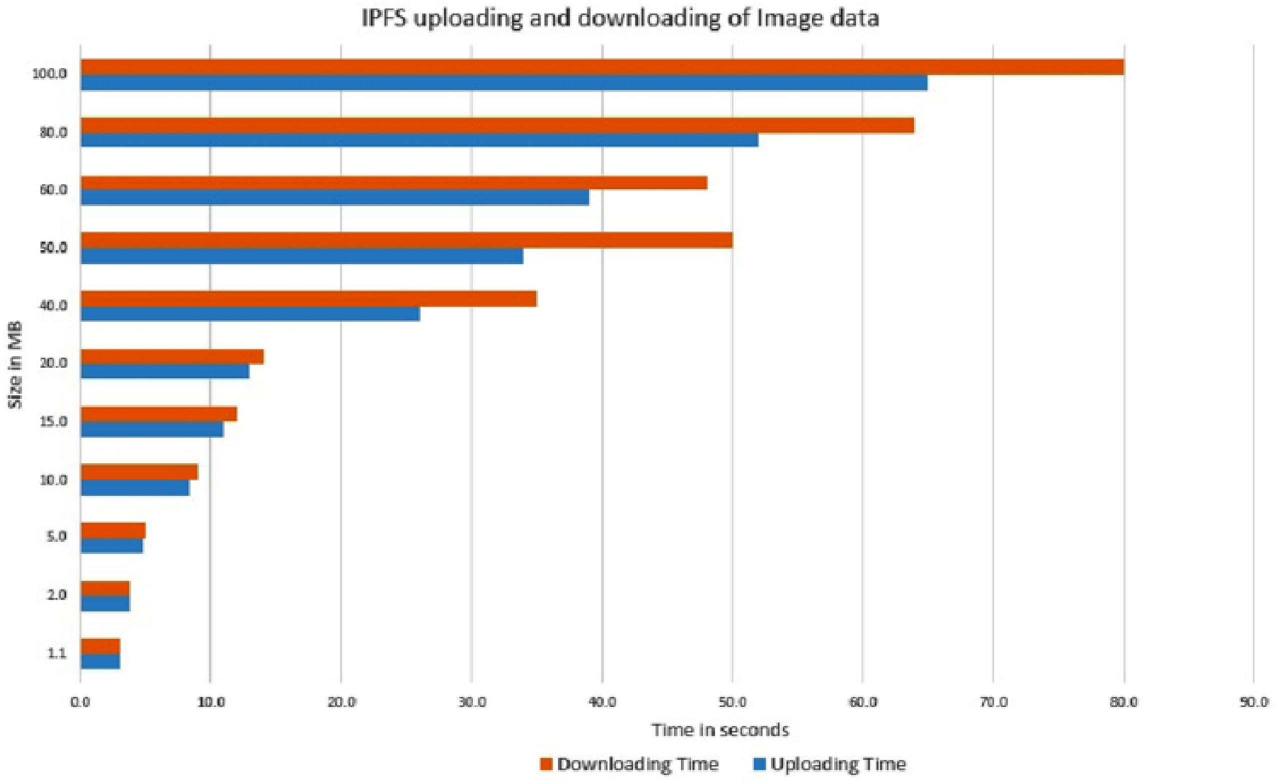


Figure 5. *Uploading and downloading time comparison of image data in IPFS.*

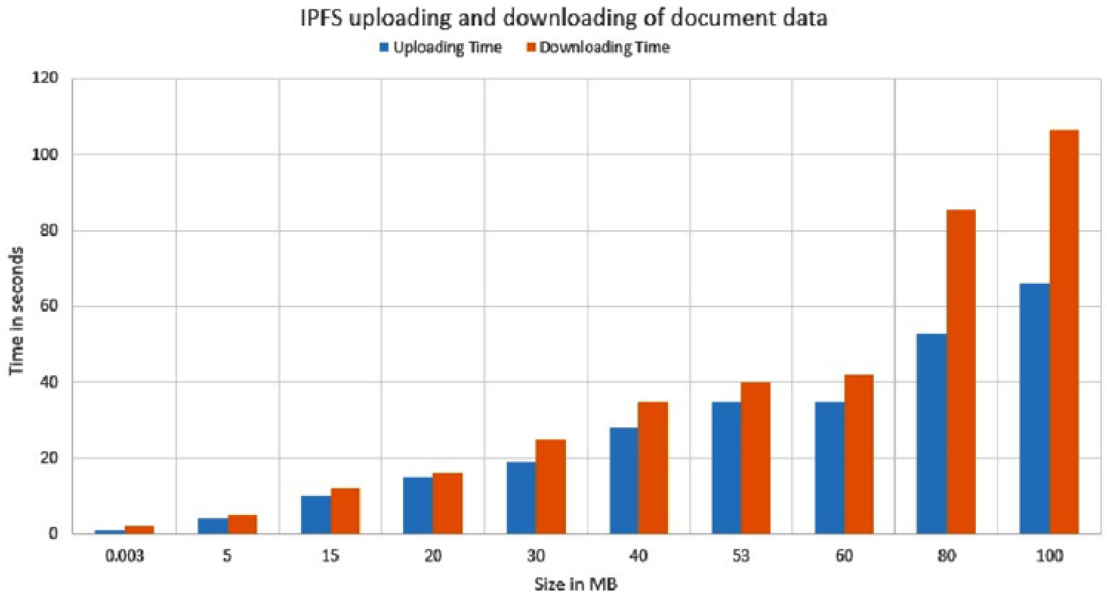


***Figure 6.** Uploading and downloading time comparison of document data in IPFS.*

The time comparison of image and document data is analysed by considering the transaction execution of five users with respect to uploading and downloading of the data in the IPFS. Based on the analysis, it was observed that the system requires an average time of 65 seconds for uploading a 100 MB image file and requires an average time of 80 seconds for downloading the image as shown in Figure 5. On the other hand, the system takes an average time of 65 seconds and 105 seconds for uploading and downloading a 100 MB document, as shown in Figure 6.

The performance of the proposed approach with respect to encryption and decryption is determined as depicted in Figures 7 and 8 respectively. The encryption and decryption performance is compared with other existing works as shown in Figures 8 and 9 respectively and the time taken for the encryption and decryption process is tabulated in Table 3.

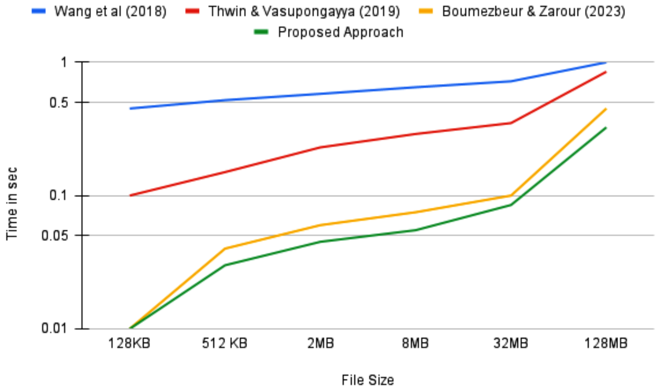


***Figure 8.** Comparison of encryption process.*

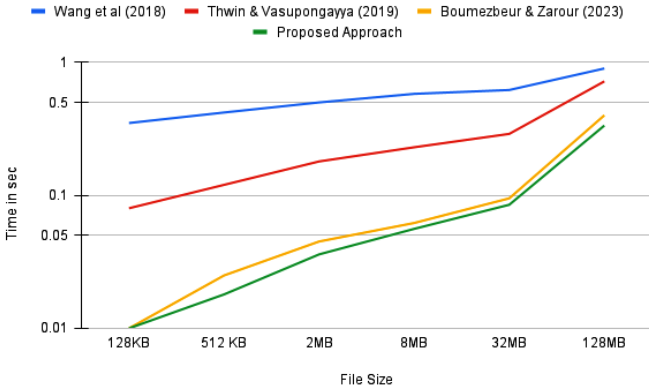


***Figure 9.** Comparison of decryption process.*

Table 3. *Comparison of proposed encryption and decryption process with existing works (in seconds).*

Works	**Wang et al. (2018)**		**Thwin and Vasupongayya (2019)**		**Boumezbeur and Zarour (2022)**		**Proposed**	
File Size	**Encryption**	**Decryption**	**Encryption**	**Decryption**	**Encryption**	**Decryption**	**Encryption**	**Decryption**
128 KB	0.45	0.35	0.1	0.08	0.01	0.01	0.01	0.01
512 KB	0.52	0.42	0.15	0.12	0.04	0.029	0.03	0.018
2 MB	0.58	0.5	0.223	0.18	0.06	0.049	0.045	0.036
8 MB	0.65	0.58	0.29	0.23	0.07	0.062	0.055	0.056
32 MB	0.72	0.62	0.35	0.29	0.1	0.095	0.085	0.085
128 MB	1.01	0.9	0.85	0.72	0.42	0.38	0.325	0.33

As observed from Figures 8 and 9, the time consumed by the proposed approach for encryption and decryption is shorter compared to other techniques. For a larger volume of EHR data, the efficiency of the encryption and decryption process of the proposed approach is significantly higher compared to other works. The large volume of EHR data is mainly constituted by larger files such as images of X-rays and CT scans and other health-related information. The results show that the proposed approach is more appropriate and efficient for encrypting and decrypting large-scale data with a shorter computation time.

The results of the proposed approach are evaluated in terms of different evaluation metrics and compared with other existing works, as shown in Table 3.

Table 4. *Comparison of the proposed approach with existing works.*

	Hasib et al. (2022)	**Chelladuri and Pandian (2022)**	**Abunadi et al. (2021)**	**Boumezbeur and Zarour (2022)**	**Proposed**
Decentralization	✓	✓	✓	✓	✓
User Authentication	✓	✓	✓	✓	✓
Data Privacy	✓	✓	✓	✓	✓
Data Integrity	✓	✓	✓	✓	✓
Confidentiality	✓	✓	✓	✓	✓
Scalability	X	X	✓	✓	✓
Patient Centric Access Control	X	X	X	X	✓
Optimized Search	X	X	X	X	✓

As observed from the comparative analysis, the proposed blockchain-based approach has demonstrated its ability to replace the existing system of managing medical records in both standardized and decentralized manner. This paper demonstrates an effective design, and implementation of blockchain-based EHR management for healthcare providers. The proposed system enables safe and open access, viewing, and exchange of health data as well as a full life cycle of individual health records for patients, doctors and healthcare providers.

6 Discussion and Conclusion

In this approach, the decentralization is achieved using blockchain, and the proposed hybrid cryptographic technique provides better user authentication and ensures data privacy and integrity. An improved scalability of the blockchain is achieved through the IPFS and the patient access control is achieved through smart contracts. In addition, the optimized search process proposed in this work reduces the complexity and processing time required for accessing medical records. Compared to other existing approaches (Hasib et al., 2022; Chelladurai & Pandian, 2022; Abunadi & Kumar, 2021; Boumezbeur & Zarour, 2022), the proposed framework exhibits excellent performance in terms of all evaluation metrics and thereby proves its potential as a real time solution for improving the privacy and security of EHR data.

However, the proposed approach does not focus on critical issues such as high energy consumption of blockchain nodes, interoperability and vulnerabilities of smart contracts. The healthcare industry comprises diverse systems, platforms and standards. Integrating the proposed framework with existing EHR systems might require extensive effort to ensure seamless data exchange and interoperability across different healthcare providers and institutions. In addition, possible errors in smart contract code could lead to unintended data exposure or unauthorized access, emphasizing the importance of thorough security audits. These issues need a thorough analysis.

In our ongoing research, we intend to create an expanded version of this framework that may be used in a heterogeneous or homogeneous blockchain network to connect multiple hospitals. A cross-chain communication between two or more blockchains to achieve interoperability with an increased security level is regarded as one of the potential study areas in the field of blockchain in healthcare.

This paper presented a privacy preservation approach for securing EHR data with an emphasis of patient-centric access control and optimized searching. The proposed approach employed a hybrid cryptographic approach, which combines both symmetric and asymmetric encryption algorithms along with a digital signature for verification and authentication. The patient-centric access control was designed using smart contracts along with an optimized search process. The experimental evaluation showed that the proposed framework provides better access control for patients in terms of providing access to EHR data for concerned authorities. In addition, the proposed optimized search process significantly reduced the time complexity and space complexity compared to traditional search processes. The effectiveness of the framework was determined using two primary approaches, namely brute force and an optimized search approach. The results showed that the smart contract functions exhibited desired performance and the privacy was ensured using the hybrid cryptographic approach. The times taken by the traditional approach and the optimized approach were tested for performance evaluation and the optimized approach turned out to be more efficient as expected. The suggested system aims at privacy, security and transparency and makes it easier for medical history to be maintained among healthcare providers. Through the use of blockchain technology, this framework enables safe health information sharing among network users. By fusing the inherent security features of blockchain with patient-centric access control, this research presented a more secure, transparent and patient-empowered healthcare system. With the increasing digitization of healthcare applications, this framework provides a solid foundation for building secure, patient-centric and regulatory-compliant EHR systems that prioritize data privacy in an increasingly interconnected world.

Additional Information and Declarations

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

Author Contributions: R. P. P.: Conceptualization, Methodology, Data curation, Investigation, Writing – Original draft preparation. G. P.: Supervision, Validation, Writing – Reviewing and Editing.

References

Abunadi, I., & Kumar, R. L. (2021). BSF-EHR: Blockchain security framework for electronic health records of patients. *Sensors*, 21(8), 2865. https://doi.org/10.3390/s21082865

Hasib, K. T. a. M., Chowdhury, I., Sakib, S., Khan, M. M., Alsufyani, N., Alsufyani, A., & Bourouis, S. (2022). Electronic health record monitoring system and data security using blockchain technology. *Security and Communication Networks*, 2022, e2366632. https://doi.org/10.1155/2022/2366632

Awotunde, J. B., Jimoh, R. G., Folorunso, S. O., Adeniyi, E. A., Abiodun, K. M., & Banjo, O. O. (2021). Privacy and security concerns in IoT-based healthcare systems. In *Internet of things* (pp. 105–134). Springer. https://doi.org/10.1007/978-3-030-75220-0_6

Bamakan, S. M. H., Motavali, A., & Babaei Bondarti, A. B. (2020). A survey of blockchain consensus algorithms performance evaluation criteria. *Expert Systems with Applications*, 154, 113385. https://doi.org/10.1016/j.eswa.2020.113385

Boumezbeur, I., & Zarour, K. (2022). Privacy preservation and access control for sharing electronic health records using blockchain technology. *Acta Informatica Pragensia*, 11(1), 105–122. https://doi.org/10.18267/j.aip.176

Cerchione, R., Centobelli, P., Riccio, E., Abbate, S., & Oropallo, E. (2023). Blockchain's coming to hospital to digitalize healthcare services: Designing a distributed electronic health record ecosystem. *Technovation*, 120, 102480. https://doi.org/10.1016/j.technovation.2022.102480

Chelladurai, U., & Pandian, S. (2022). A novel blockchain based electronic health record automation system for healthcare. *Journal of Ambient Intelligence and Humanized Computing*, 13(1), 693–703. https://doi.org/10.1007/s12652-021-03163-3

Chenthara, S., Ahmed, K., Wang, H., & Whittaker, F. (2019). Security and privacy-preserving challenges of e-health solutions in cloud computing. *IEEE Access*, 7, 74361–74382. https://doi.org/10.1109/ACCESS.2019.2919982

Escorcia-Gutierrez, J., Mansour, R. F., Leal, E., Villanueva, J. A., Jiménez-Cabas, J., Soto, C. Y., & Soto-Díaz, R. (2023). Privacy Preserving Blockchain with Energy Aware Clustering Scheme for IoT Healthcare Systems. *Mobile Networks and Applications*, (in press). https://doi.org/10.1007/s11036-023-02115-9

Garcia, R. D., Ramachandran, G., & Ueyama, J. (2022). Exploiting smart contracts in PBFT-based blockchains: A case study in medical prescription system. *Computer Networks*, 211, 109003. https://doi.org/10.1016/j.comnet.2022.109003

Genç, Y., & Afacan, E. (2021). Design and implementation of an efficient elliptic curve digital signature algorithm (ECDSA). In *2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS).* IEEE. https://doi.org/10.1109/IEMTRONICS52119.2021.9422589

Ghayvat, H., Pandya, S., Bhattacharya, P., Zuhair, M., Rashid, M., Hakak, S., & Dev, K. (2022). CP-BDHCA: Blockchain-Based Confidentiality-Privacy Preserving Big Data Scheme for Healthcare clouds and applications. *IEEE Journal of Biomedical and Health Informatics*, 26(5), 1937–1948. https://doi.org/10.1109/jbhi.2021.3097237

Gopinath, S., & Olmsted, A. (2022). Mitigating the effects of ransomware attacks on healthcare systems. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2202.06108

Guo, H., & Yu, X. (2022). A survey on blockchain technology and its security. *Blockchain: Research and Applications*, 3(2), 100067. https://doi.org/10.1016/j.bcra.2022.100067

Gupta, B. B., Gaurav, A., & Panigrahi, P. K. (2023). Analysis of security and privacy issues of information management of big data in B2B based healthcare systems. *Journal of Business Research*, 162, 113859. https://doi.org/10.1016/j.jbusres.2023.113859

Hathaliya, J. J., & Tanwar, S. (2020). An exhaustive survey on security and privacy issues in Healthcare 4.0. *Computer Communications*, 153, 311–335. https://doi.org/10.1016/j.comcom.2020.02.018

Jin, H., Luo, Y., Li, P., & Mathew, J. (2019). A review of secure and privacy-preserving medical data sharing. *IEEE Access*, 7, 61656–61669. https://doi.org/10.1109/ACCESS.2019.2916503

Joe, C. V., & Raj, J. S. (2021). Deniable authentication encryption for privacy protection using blockchain. *Journal of Artificial Intelligence and Capsule Networks*, 3(3), 259–271. https://doi.org/10.36548/jaicn.2021.3.008

John, J., & Norman, J. (2019). Major vulnerabilities and their prevention methods in cloud computing. In Advances in big data and cloud computing. In *Advances in Big Data and Cloud Computing. Advances in Intelligent Systems and Computing*, (pp. 11–26). Springer. https://doi.org/10.1007/978-981-13-1882-5_2

Keshta, I., & Odeh, A. (2021). Security and privacy of electronic health records: Concerns and challenges. *Egyptian Informatics Journal*, 22(2), 177–183. https://doi.org/10.1016/j.eij.2020.07.003

Kruse, C. S., Mileski, M., Vijaykumar, A. G., Viswanathan, S. V., Suskandla, U., & Chidambaram, Y. (2017). Impact of electronic health records on long-term care facilities: Systematic review. *JMIR Medical Informatics*, 5(3), e35. https://doi.org/10.2196/medinform.7958

Lakhan, A., Mastoi, Q. U. A., Elhoseny, M., Memon, M. S., & Mohammed, M. A. (2022a). Deep neural network-based application partitioning and scheduling for hospitals and medical enterprises using IoT assisted mobile fog cloud. *Enterprise Information Systems*, 16(7), 1883122. https://doi.org/10.1080/17517575.2021.1883122

Lakhan, A., Mohammed, M. A., Nedoma, J., Martínek, R., Tiwari, P., & Kumar, N. (2023). Blockchain-Enabled Cybersecurity Efficient IIOHT Cyber-Physical System for medical applications. *IEEE Transactions on Network Science and Engineering*, 10(5), 2466–2479. https://doi.org/10.1109/tnse.2022.3213651

Lakhan, A., Mohammed, M. A., Elhoseny, M., Alshehri, M. D., & Abdulkareem, K. H. (2022c). Blockchain multi-objective optimization approach-enabled secure and cost-efficient scheduling for the Internet of Medical Things (IoMT) in fog-cloud system. *Soft Computing*, 26(13), 6429–6442. https://doi.org/10.1007/s00500-022-07167-9

Lakhan, A., Mohammed, M. A., Nedoma, J., Martinek, R., Tiwari, P., & Kumar, N. (2023). DRLBTS: Deep reinforcement learning-aware blockchain-based healthcare system. *Scientific Reports*, 13(1), 4124. https://doi.org/10.1038/s41598-023-29170-2

Lee, Y. L., Lee, H. A., Hsu, C. Y., Kung, H. H., & Chiu, H. W. (2022). SEMRES-A triple security protected blockchain based medical record exchange structure. *Computer Methods and Programs in Biomedicine*, 215, 106595. https://doi.org/10.1016/j.cmpb.2021.106595

Luong, D. A., & Park, J. H. (2022). Privacy-preserving blockchain-based healthcare system for IoT devices using zk-SNARK. *IEEE Access*, 10, 55739–55752. https://doi.org/10.1109/access.2022.3177211

Mikula, T., & Jacobsen, R. H. (2018). Identity and Access Management with Blockchain in Electronic Healthcare Records. In *2018 21st Euromicro Conference on Digital System Design (DSD),* IEEE. https://doi.org/10.1109/DSD.2018.00008

Mohammed, M. A., Lakhan, A., Abdulkareem, K. H., Zebari, D. A., Nedoma, J., Martinek, R., Kadry, S., & Garcia-Zapirain, B. (2023). Energy-efficient distributed federated learning offloading and scheduling healthcare system in blockchain based networks. *Internet of Things*, 22, 100815. https://doi.org/10.1016/j.iot.2023.100815

Naser, M., Naser, M. M., Shehata, L. H., & Nassr, T. (2022). Cybersecurity in health systems: Challenges, and proposals. *International Journal of Progressive Sciences and Technologies*, 35(1), 195–208.

Nath, S. S., Sadagopan, S., Babu, D. V., Kumar, R. D., Jonnala, P., & Murthy, M. Y. B. (2023). Block chain-based security and privacy framework for point of care health care IoT devices. *Soft Computing*, (in press). https://doi.org/10.1007/s00500-023-07932-4

Pal, O., Alam, B., Thakur, V., & Singh, S. (2021). Key management for blockchain technology. *ICT Express*, 7(1), 76–80. https://doi.org/10.1016/j.icte.2019.08.002

Patel, V. (2019). A framework for secure and decentralized sharing of medical imaging data via blockchain consensus. *Health Informatics Journal*, 25(4), 1398–1411. https://doi.org/10.1177/1460458218769699

Paul, M., Maglaras, L., Ferrag, M. A., & Almomani, I. (2023). Digitization of healthcare sector: A study on privacy and security concerns. *ICT Express*. https://doi.org/10.1016/j.icte.2023.02.007

Pourvahab, M., & Ekbatanifard, G. (2019). Digital forensics architecture for evidence collection and provenance preservation in IaaS cloud environment using SDN and blockchain technology. *IEEE Access*, 7, 153349–153364. https://doi.org/10.1109/ACCESS.2019.2946978

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. (2021). A Comprehensive Survey on Privacy-Security and Scalability Solutions for Blockchain Technology. In *Smart Intelligent Computing and Communication Technology* (pp. 173–178). IOS Press. https://doi.org/10.3233/APC210031

Raj, A., & Prakash, S. (2023). Privacy preservation of the internet of medical things using blockchain. *Health Services and Outcomes Research Methodology,* (in press). https://doi.org/10.1007/s10742-023-00306-1

Rao, K.P.N., & Manvi, S. (2023). Survey on Electronic Health Record Management Using Amalgamation of Artificial Intelligence and Blockchain Technologies. *Acta Informatica Pragensia*, 12(1), 179–199. https://doi.org/10.18267/j.aip.194

Rijanto, A. (2021). Blockchain technology adoption in supply chain finance. *Journal of Theoretical and Applied Electronic Commerce Research*, 16(7), 3078–3098. https://doi.org/10.3390/jtaer16070168

Sharma, P., Namasudra, S., Gonzalez Crespo, R., Parra-Fuente, J., & Chandra Trivedi, M. C. (2023a). EHDHE: Enhancing security of healthcare documents in IoT-enabled digital healthcare ecosystems using blockchain. *Information Sciences*, 629, 703–718. https://doi.org/10.1016/j.ins.2023.01.148

Sharma, P., Namasudra, S., Chilamkurti, N., Kim, B., & Gonzalez Crespo, R. (2023b). Blockchain-Based Privacy Preservation for IoT-Enabled Healthcare System. *ACM Transactions on Sensor Networks*, 19(3), 1–17. https://doi.org/10.1145/3577926

Sharma, S., & Chopra, V. (2017). Data encryption using advanced encryption standard with key generation by elliptic curve Diffie-Hellman. *International Journal of Security and its Applications*, 11(3), 17–28. https://doi.org/10.14257/ijsia.2017.11.3.02

Singh, A. K., Anand, A., Lv, Z., Ko, H., & Mohan, A. (2021). A survey on healthcare data: A security perspective. *ACM Transactions on Multimedia Computing, Communications, and Applications*, 17(2s), 1–26. https://doi.org/10.1145/3422816

Singh, S., Rathore, S., Alfarraj, O., Tolba, A., & Yoon, B. (2022). A framework for privacy-preservation of IoT healthcare data using Federated Learning and blockchain technology. *Future Generation Computer Systems*, 129, 380–388. https://doi.org/10.1016/j.future.2021.11.028

Thamer, N., & Alubady, R. (2021). A survey of ransomware attacks for healthcare systems: Risks, challenges, solutions and opportunity of research. In *1st Babylon International Conference on Information Technology and Science (BICITS).* IEEE. https://doi.org/10.1109/BICITS51482.2021.9509877

Thwin, T. T., & Vasupongayya, S. (2019). Blockchain-based access control model to preserve privacy for personal health record systems. *Security and Communication Networks*, 2019, 8315614. https://doi.org/10.1155/2019/8315614

Velmurugadass, P., Dhanasekaran, S., Shasi Anand, S., & Vasudevan, V. (2021). Enhancing Blockchain security in cloud computing with IoT environment using ECIES and cryptography hash algorithm. *Materials Today: Proceedings*, 37, 2653–2659. https://doi.org/10.1016/j.matpr.2020.08.519

Wang, H., & Song, Y. (2018). Secure cloud-based EHR system using attribute-based cryptosystem and blockchain. *Journal of Medical Systems*, 42(8), 152. https://doi.org/10.1007/s10916-018-0994-6

Xiang, T., Zeng, H., Chen, B., & Guo, S. (2023). BMIF: Privacy-preserving blockchain-based medical image fusion. *ACM Transactions on Multimedia Computing, Communications, and Applications*, 19(1s), 1–23. https://doi.org/10.1145/3531016

Yaqoob, I., Salah, K., Jayaraman, R., & Al-Hammadi, Y. (2021). Blockchain for healthcare data management: opportunities, challenges, and future recommendations. *Neural Computing and Applications*, 34(14), 11475–11490. https://doi.org/10.1007/s00521-020-05519-w

Zhai, S., Yang, Y., Li, J., Qiu, C., & Zhao, J. (2019). Research on the application of cryptography on the blockchain. *Journal of Physics: Conference Series*, 1168(3), 032077. https://doi.org/10.1088/1742-6596/1168/3/032077

Zhu, C., Li, J., Zhong, Z., Yue, C., & Zhang, M. (2023). A survey on the integration of blockchains and databases. *Data Science and Engineering*, 8(2), 196–219. https://doi.org/10.1007/s41019-023-00212-z

Editorial record: The article has been peer-reviewed. First submission received on 24 May 2023. Revisions received on 28 August 2023 and 22 November 2023. Accepted for publication on 29 November 2023. The editor in charge of coordinating the peer-review of this manuscript and approving it for publication was Michal Dolezel.

Acta Informatica Pragensia is published by Prague University of Economics and Business, Czech Republic.

ISSN: 1805-4951