International Journal of Advanced Engineering and Management Research

Vol. 10, No. 06; 2025

ISSN: 2456-3676

Two-level Security Approach for Secure EHR Sharing via Blockchain and Cryptography

Gayathri Hegde M[1], P Deepa Shenoy[1], Venugopal K R[1]

[1]Department of Computer Science and Engineering, University Visvesvaraya College of Engineering,
Bangalore University, Bengaluru, Karnataka, India

doi.org/10.51505/ijaemr.2025.1505 URL: http://dx.doi.org/10.51505/ijaemr.2025.1505

Received: Oct 21, 2025 Accepted: Oct 30, 2025 Online Published: Nov 07, 2025

Abstract

Electronic Health Records (EHRs) have transformed healthcare by enabling the easy sharing of information, but large-scale deployment is raising important privacy, security, and effectiveness issues. Existing EHR-sharing infrastructures are biased toward single-layer cryptographic methods, which either limit performance or leave emergency and real-time applications vulnerable to weaknesses. To address these limitations, we present a two-level security solution that combines blockchain and cryptography to provide timely access while preserving privacy. Our research exhaustively compares symmetric (AES, XChaCha20) and asymmetric (RSA, ECC, ECDSA) cryptographic algorithms on medical records of varying sizes, showing that XChaCha20 and ECC dramatically outperform the others in encryption/decryption time. Building on these findings, we develop and deploy a blockchain-supported framework that uses dual-layer encryption to store and transfer EHRs over IPFS securely. The system is tested in a medical context during surgical second opinions, where EHRs are shared. Experimental results demonstrate that two-level security using XChaCha20 and ECC is reliable and effective. Hence, this method enhances EHR confidentiality, integrity and availability without compromising the practical needs of healthcare decision-making.

Keywords: Blockchain, Cryptography, Electronic Health Records, Security

1. Introduction

EHRs serve as the digital counterpart to traditional paper-based medical records, capturing a comprehensive view of a patient’s clinical history and treatment across healthcare visits. The main benefits of EHR systems lie in their capacity to facilitate seamless information sharing among healthcare providers, pharmacists, insurance companies, and patients, thereby enhancing the quality and effectiveness of healthcare services. However, it has also introduced new challenges, particularly in terms of security, privacy, and ethical considerations (Jamshed et al., 2015). Over the last decade, the HIPAA Journal (“HIPAA Journal,” 2022) reports an upward trend in the number of healthcare data breaches in the US Department of Health and Human Services. As a result of those breaches, 314,063,186 healthcare records were misplaced, misused, disclosed, or unlawfully released. On 23rd November 2022, AIIMS servers were suspected to have been targeted by a malware attack that breached approximately 30-40 million patient records (Telegraphindia, 2022). The records included patients' medical history and crucial information, such as Aadhaar and PAN card details linked to their bank accounts. The conventional client-server (Cifuentes et al., 2015; Holmes et al., 2021; Palabindala et al., 2016) or cloud-based EHR systems (Ganiga et al., 2017; Kavitha et al., 2016; Liu et al., 2016; Zaied et al., 2016) are plagued with centralization, which exposes them to unauthorized access, brute-force attacks and single points of failure.

Blockchain technology presents a compelling alternative by decentralizing data management, providing immutability, and supporting patient-centric control over health records. However, blockchain-based models in themselves are not sufficient; encrypting data stored on-chain creates scalability issues, and most existing models rely on cryptographic methods that either degrade performance (e.g., RSA) or do not adequately support emergency use cases (e.g., single-key symmetric encryption). This gap calls for a hybrid solution that not only enhances data confidentiality and integrity but also maintains efficiency in real-world healthcare settings, particularly during time-sensitive scenarios such as surgical decision-making. In this paper, we introduce a two-tier security model for sharing EHRs that amalgamates blockchain with optimized cryptographic methods.

Our method combines XChaCha20 (for high-speed symmetric cryptography) and ECC (for efficient asymmetric cryptography) to balance performance and security. Patient information is stored off-chain in the InterPlanetary File System (IPFS), with corresponding hashes stored on the Ethereum blockchain for integrity and traceability. This work also considers a case study of EHR sharing for surgical second opinions via a voting mechanism. The research contributions are:

- Comparative evaluation of symmetric and asymmetric cryptography algorithms on EHR records of different sizes.
- A two-layer cryptographic system on XChaCha20 and ECC, combined with IPFS and Ethereum.
- Implementation of a case study to secure EHR sharing procedures unique to surgical second-opinion.
- Performance validation showing significant improvements in encryption speed, decryption latency, and overall access efficiency compared to existing approaches.

The organization of the work is as follows: Section II comprises related work, while Section III elucidates the technical prerequisites. Section IV discusses the methodology adopted in the proposed work, the experimental setup, implementation and the results presented in Section V. In Section VI, the paper compares the performance of the proposed work with that of existing approaches, and Section VII concludes the paper.

2. Related Work

Numerous efforts have been made to securely store and share EHRs in cloud environments using cryptographic and blockchain technologies.

This subsection categorizes the state-of-the-art methods into two primary categories: Blockchain-based systems utilizing symmetric cryptography, asymmetric or hybrid cryptography-based schemes, combined with blockchain.

2.1. Blockchain-Based Symmetric Cryptography Methods:

Symmetric cryptographic techniques are pervasively employed because of their effectiveness, but they struggle with secure key exchange. Numerous blockchain-based EHR platforms use symmetric-key encryption, such as the AES algorithm, to encrypt medical records.

Dubovitskaya et al. (Dubovitskaya et al., 2017) introduced a blockchain framework for data sharing in the context of primary care for oncology patients undergoing cancer treatment. This framework ensures the critical aspects of access control, security, availability and privacy on EMR.

The BCHealth system (Mohammad Hossein et al., 2021) empowers data owners to establish access policies for their sensitive data. This innovative approach involves storing data locally on a machine and uses two distinct chains. These chains are used to maintain data confidentiality and control access to the data. Both the above works use the AES algorithm.

A MedBlock (Fan et al., 2018) uses a distributed ledger and symmetric-key encryption to store encrypted medical information, which can be accessed and retrieved efficiently via pointers and hash values. The system also includes a breadcrumbs mechanism to efficiently locate encrypted information.

Shuaib et al. (Shuaib et al., 2022) proposed a blockchain platform developed on Hyperledger Besu and using the IBFT consensus mechanism. The distinguishing cryptographic aspect is the use of a symmetric key, which is smartly split among multiple key holders.

2.2. Asymmetric and Hybrid Cryptographic Methods

Due to the one-key restriction of symmetric encryption, most recent designs use asymmetric cryptography, such as ECC and ECDSA, or blend it with symmetric schemes for combined security.

A Healthchain (Chenthara et al., 2020) is a patient-centric interoperability framework that enables efficient access management for stakeholders, including patients, doctors, and pharmacists, through public-key encryption and access-control technologies. Chen et al. (Chen et al., 2022) introduced a scheme designed to ensure the secure sharing of data and protect privacy within the realm of the IIoT. It provides data integrity protection, scalability, and access control mechanisms to safeguard enterprises' privacy.

Le et al. (Le Nguyen et al., 2020) focused on establishing a secure and robust framework for the dependable sharing of IoT data, incorporating blockchain, ECC, and Ant Colony Optimization techniques with SVM(ACOMKSVM). The objective is to develop secure training algorithms tailored explicitly for IoT data. The framework in Egala et al. (2021), designed for secure and private IOMT with effective access control and an ECC cryptographic method.

Wang et al. (Y. Wang et al., 2019) proposed a scheme for secure EHR data sharing that ensures privacy by leveraging a consortium blockchain and cloud storage. Kim et al. (Kim et al., 2020) introduced a secure protocol based on blockchain for cloud-assisted EHR. Secure EHR sharing in the cloud is enabled by implementing ECC cryptography. BAN logic analyzes the secure mutual authentication.

Several hybrid approaches also combine symmetric and asymmetric cryptography (e.g., AES-RSA, ECC/AES) for improved efficiency and layered protection: Ghayvat et al. (Ghayvat et al., 2022) address the challenges of storing and accessing EHRs on cloud servers and present several contributions, such as a secure key exchange framework, fog-enabled light-weight signatures, and personalized segmentation for patients to ensure that only necessary information is delivered to authorized stakeholders.

Xia et al. (Xia et al., 2017), introduced a data-sharing framework based on a permissioned blockchain incorporating robust cryptographic methods, such as encryption and digital signatures, to establish effective access control for shared critical data pools. After verifying credentials, users within the framework can access data from the shared pool.

Boumezbeur et al. (Boumezbeur & Zarour, 2022) and Jayabalan et al. (Jayabalan & Jeyanthi, 2022) suggested a blockchain-based multi-factor authentication and access control system. This method encrypts secret keys in EHRs using the AES and RSA algorithms to provide a high degree of confidentiality and privacy.

3 Background

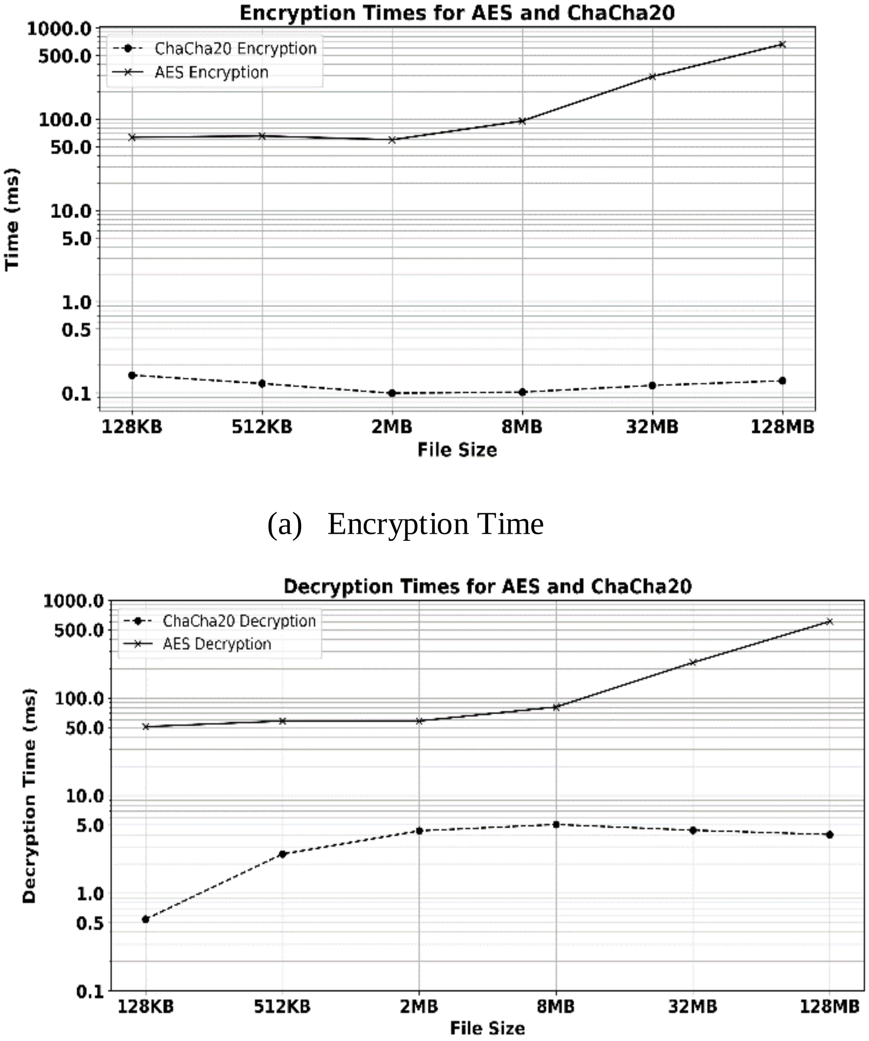
The secure sharing of EHRs relies heavily on cryptographic techniques. Existing work has explored both symmetric and asymmetric encryption methods to ensure the confidentiality and authenticity of sensitive healthcare data.

3.1. Symmetric Cryptography

Symmetric algorithms like Advanced Encryption Standard (AES) and ChaCha20/XChacha20 are most popular because they are computationally efficient and well-suited for encrypting large files such as CT scans and X-rays. Symmetric encryption, however, requires both the sender and receiver to possess the same secret key, which creates significant key distribution and management issues in multi-party healthcare settings.

To evaluate their suitability for EHR applications, they were compared in terms of encryption and decryption time across file sizes ranging from 128 KB to 128MB.

Figures 1(a) and 1(b) represent the Encryption/ Decryption time of Symmetric Algorithms. Results indicated that XChacha20 consistently outperformed AES, with faster encryption/decryption rates, particularly for large files. This makes XChacha20 better suited to real-time, large-scale healthcare settings where performance is crucial.



(a) Encryption Time

(b) Decryption Time

Figure 1. Comparison of Symmetric Cryptographic Algorithms

3.2. Asymmetric Encryption

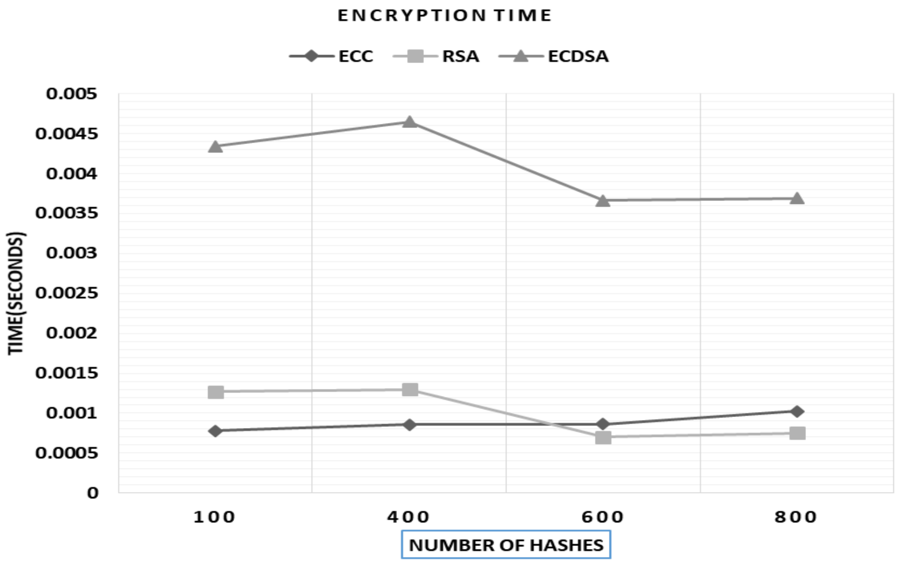
Asymmetric encryption solves the problem of key distribution through a pair of public and private keys. Popular algorithms include RSA, ECC (Elliptic Curve Cryptography), and ECDSA (Elliptic Curve Digital Signature Algorithm).

RSA is secure but has larger keys, which results in additional computational overhead. ECC, however, offers the same security with far fewer keys, making it lighter and more efficient for resource-constrained healthcare systems.

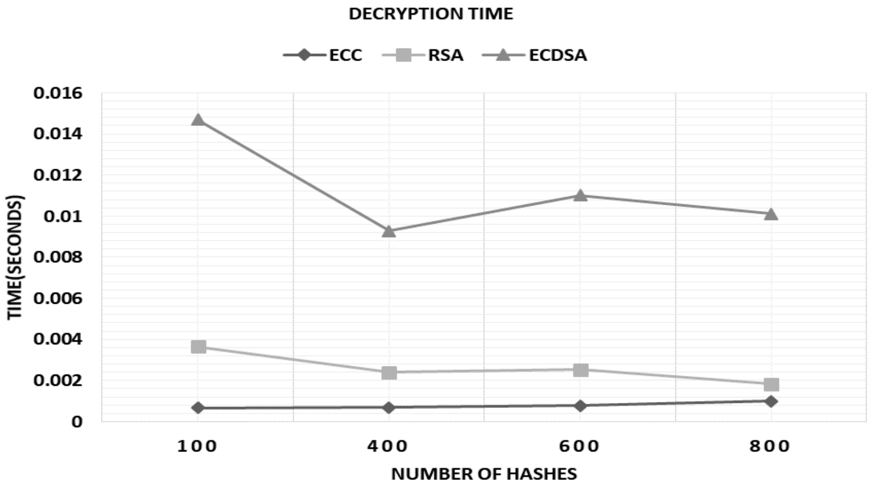
In this work, RSA, ECC, and ECDSA were experimentally tested for encryption/decryption times, key size efficiency, and computational overhead.

Figures 2(a) and 2(b) below plot the encryption and decryption times for ECC, ECDSA, and RSA. Results showed that ECC outperformed RSA and ECDSA, achieving faster performance with lower resource requirements without compromising security.

This makes ECC especially well-suited for applications such as secure key sharing in doctor-patient communications or multi-party voting in collaborative decision-making processes.



(a) Encryption Time



(b) Decryption Time

Figure 2. Comparison of Asymmetric Cryptographic Algorithms

3.3. Blockchain and Off-chain Storage

Cryptography provides confidentiality, blockchain technology adds immutability, auditability, and decentralized trust. Blockchain-based platforms enable secure access logging and tamper-proof storage of transaction history. Direct storage of large medical files on the blockchain is not practical due to scalability and cost constraints.

To address this, the InterPlanetary File System (IPFS) has been implemented as an off-chain data storage layer. IPFS stores encrypted EHRs and returns unique hash values that are irretrievably marked on the blockchain. This architecture combines efficiency and integrity: IPFS handles large-scale data storage, and blockchain securely stores references and enables transparent access control.

From the cryptographic analysis, XChacha20 is the most optimal symmetric encryption algorithm for bulk EHR data, and ECC is the most optimal asymmetric algorithm for secure key exchange. A blend of blockchain and IPFS acts as the building blocks of a two-level security framework that guarantees confidentiality, integrity, scalability, and patient-centric control in EHR sharing.

4. Methodology

Based on the findings of the cryptographic analysis and background research, this section introduces a two-tier security framework for privacy-preserving sharing of EHRs that combines XChaCha20 for symmetric encryption, ECC for asymmetric key management, blockchain for access control and auditing, and IPFS for off-chain storage scaling.

The proposed work presents a two-level security framework for sharing and storing EHR using blockchain, cryptographic algorithms, and decentralized storage. The design arises from the need to balance firm security guarantees with efficient, reliable access, especially in time-sensitive medical conditions. Figure 3 depicts a two-level security framework for secure EHR storage and sharing.

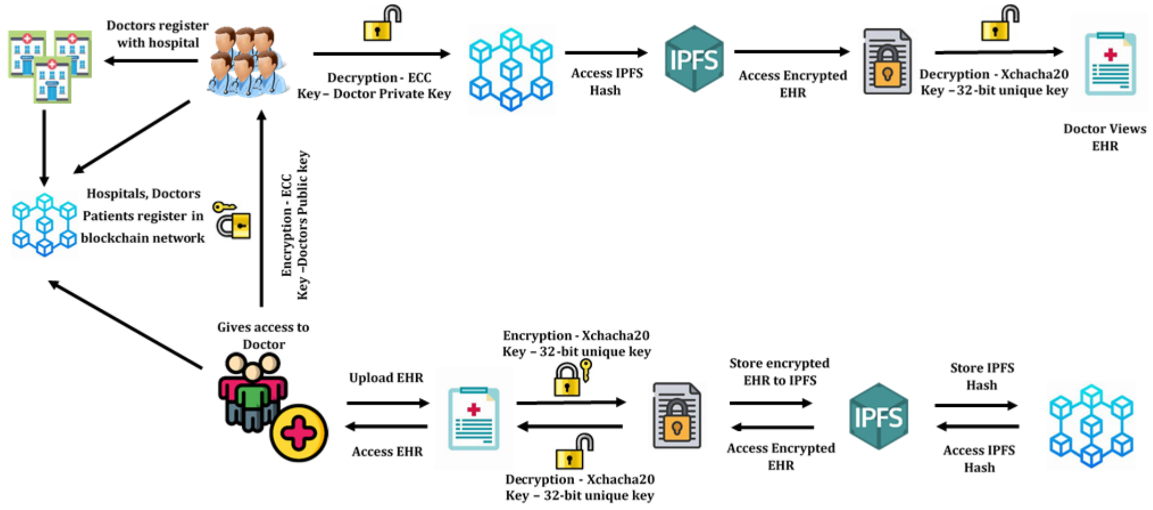

Doctors register with hospital
Decryption - ECC Key – Doctor Private Key
Access IPFS Hash
IPFS
Access Encrypted EHR
Decryption - Xchacha20 Key – 32-bit unique key
Doctor Views EHR
Hospitals, Doctors Patients register in blockchain network
Encryption - ECC Key –Doctors Public key
Gives access to Doctor
Upload EHR
Access EHR
Encryption - Xchacha20 Key – 32-bit unique key
Decryption - Xchacha20 Key – 32-bit unique key
Store encrypted EHR to IPFS
Access Encrypted EHR
IPFS
Store IPFS Hash
Access IPFS Hash

Figure 3. Two-level Security Framework for secure EHR storage and sharing.

4.1. EHR Upload/Storage Process

Within the proposed framework, the EHR upload process is patient-oriented, in that the patient remains in control of and in possession of their medical records. When a new EHR is created (e.g., upon completion of a diagnostic test or hospital stay), the patient or authorized medical provider transfers the encrypted record to the system on the patient’s behalf. Every upload is associated with the patient's blockchain identity so that no record is ever shared, accessed, or changed without the patient's express permission.

Figure 4 illustrates the process of steps performed to upload and retrieve the EHR by the

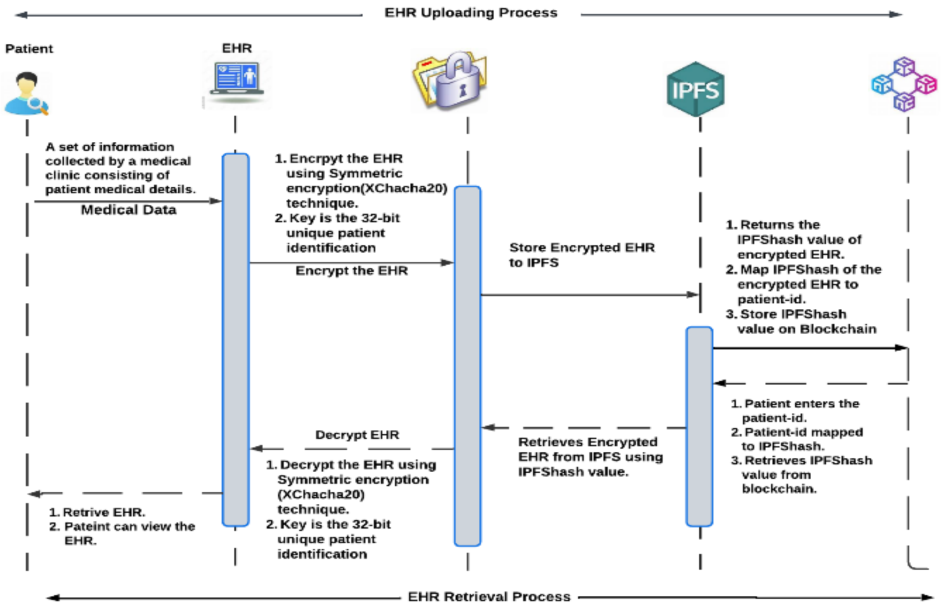

EHR Uploading Process
Patient
EHR
IPFS
A set of information collected by a medical clinic consisting of patient medical details.
Medical Data
1. Encrpyt the EHR using Symmetric encryption(XChacha20) technique.
2. Key is the 32-bit unique patient identification
Encrypt the EHR
Store Encrypted EHR to IPFS
1. Returns the IPFShash value of encrypted EHR.
2. Map IPFShash of the encrypted EHR to patient-id.
3. Store IPFShash value on Blockchain
1. Patient enters the patient-id.
2. Patient-id mapped to IPFShash.
3. Retrieves IPFShash value from blockchain.
Retrieves Encrypted EHR from IPFS using IPFShash value.
Decrypt EHR
1. Decrypt the EHR using Symmetric encryption (XChacha20) technique.
2. Key is the 32-bit unique patient identification
1. Retrive EHR.
2. Pateint can view the EHR.
EHR Retrieval Process

Figure 4. EHR Upload and Retrieval Process by patient

patient. For patient-centric control, the patient initiates the EHR upload using a 32-bit key generated with the UUID library to encrypt it. The encrypted EHR is then uploaded to IPFS, a decentralized storage network that provides resilience and scalability. The resulting IPFS hash is linked to the patient's unique 32-bit key through Solidity. This identifiable IPFS hash, crucial for EHR identification, is securely stored in the blockchain by associating it with the patient ID.

The encryption key generated for each record upload is unique and encrypted with the patient's public key before being shared with authorized parties. This guarantees that patients remain the primary custodians of their data and that access permissions can only be delegated through patient-approved smart contracts. Also, recording only the hash rather than the entire file significantly reduces on-chain storage costs and addresses scalability concerns while preserving data integrity and traceability.

4.2. EHR Retrieval

Access to stored EHRs varies slightly depending on whether the request is from the patient or a healthcare professional. Both processes work to maintain the confidentiality, authenticity, and integrity of health information while protecting the patient's control over access rights.

4.2.1. Patient Retrieval Process

The retrieval of EHR by the patient is straightforward without any authorization as shown in Fig. 4. To access their EHRs, the patient initiates the retrieval process by entering their unique patient ID. Given that the patient ID maps to the corresponding IPFS hash, the blockchain enables the retrieval of the specific IPFS hash for that patient. With the acquired IPFS hash, the encrypted EHR is then retrieved from IPFS. Subsequently, the 32-bit identification key is used for decryption, enabling the patient to access and view their EHR securely. This process guarantees that patients always remain the rightful owners of their data, with the ability to retrieve and view their medical history at any time securely.

4.2.2. Doctor Retrieval Process

Figure 5 depicts the process by which doctors retrieve the EHR. When granting access to their EHR, the patient securely transmits the file data alongside a 32-bit unique key. This unique key is encoded with ECC, utilizing the doctor's public metadata. The doctor starts by decrypting the metadata with their private ECC key. The file is then decrypted using XChacha20 with the metadata as the key. This effortless decryption process allows the doctor to view and peruse the patient's health record.

This two-step approach ensures that only authorized doctors explicitly approved by the patient can access the medical record, while all transactions are immutably logged on the blockchain for auditability. Through these complementary retrieval mechanisms, the system enables seamless patient self-access while ensuring controlled, secure sharing with healthcare professionals.

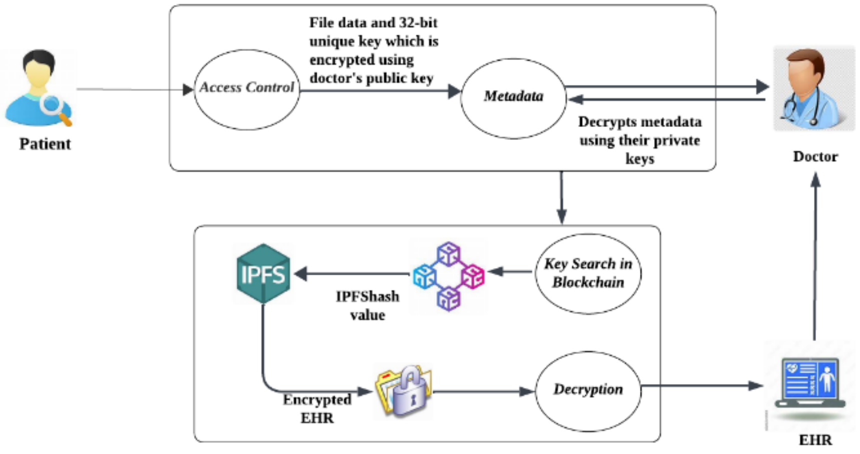

File data and 32-bit unique key which is encrypted using doctor's public key
Patient
Access Control
Metadata
Decrypts metadata using their private keys
Doctor
IPFS
IPFShash value
Key Search in Blockchain
Encrypted EHR
Decryption
EHR

Figure 5. Doctor Retrieval Process

4.3. Case study of EHR Sharing during surgical second opinions

The proposed framework is validated with real-world use cases in healthcare during surgical second opinions. The patient's EHR was shared with the doctors for obtaining surgical second opinions via a voting mechanism.

This work assumes five doctors are part of the voting mechanism when a patient seeks opinions from multiple doctors regarding a surgery or disease.

In soliciting opinions from a panel of five doctors via a voting mechanism, the patient undergoes a well-defined procedure. At first, the patient carefully chooses five physicians based on their specialized knowledge and experience. For the process to begin, the patient provides their 32-bit unique key for identification. The unique key is then encrypted utilizing ECC and the public key of each specific physician. Next, doctors securely retrieve the patient's records from the Google Cloud Platform (GCP) by decrypting the patient's unique key using their private ECC key. The server is key to accessing the blockchain, creating a bridge between the patient's 32-bit key and the patient ID, and retrieving the IPFS hash. This hash is used to access IPFS and retrieve the encrypted patient record. The patient record is decrypted using the XChaCha20 algorithm and the patient's 32-bit unique key. The decrypted record is preserved on the server so doctors can review it and offer their opinions. It should be noted that the patient record remains on the server for only a limited time and is deleted thereafter. Once views from all five doctors have been received, the patient weighs the majority vote for 'YES' or 'NO' to make an informed choice about proceeding with the suggested surgery. Such a comprehensive process guarantees a safe and effective transfer of information between the medical staff and the patient.

5. Experimental Setup and Results

The proposed work is tested on a Windows system processor: Intel(R) Core(TM) i5-7300U CPU @ 2.60GHz, 2712 MHz. The comparative study of cryptographic algorithms is conducted on Google Colab using different Python libraries: pyAesCrypt (AES), pycryptodome (ChaCha20), ecdsa (ECDSA), rsa (RSA), and eciespy (ECC). The UUID library for generating unique IDs is further encoded into the desired form. The off-chain storage implementation uses the IPFS-Desktop, IPFS-Toolkit, and IPFS-HttpClient libraries to perform various IPFS operations. Smart contracts for access control are written in Solidity, and Ganache is used to test the multiple functions.

5.1. Result Analysis of EHR upload and Retrieval time with different file sizes

This section analyzes the upload and retrieval time of EHRs of different sizes. Initially, the EHR is encrypted using the XChacha20 encryption algorithm. The patient's encrypted EHR data is stored off-chain on IPFS, and only the EHR's hash is stored on-chain. Table 1 shows the total upload time to store encrypted EHRs on the blockchain for different file sizes. The total upload time of EHR on the blockchain is the sum of the time taken to store the EHR on IPFS, the IPFShash on the blockchain, and the encryption time.

Table 1. Total upload Time of EHR on Blockchain

File Size	T_{upIPFS}	$T_{blkstore}$	T_{enc}	T_{upEHR}
128KB	0.02	0.17	0.000191	0.190191
512KB	0.03	0.18	0.000078	0.210078
2MB	0.2	0.17	0.000073	0.370073
8MB	0.26	0.18	0.000132	0.440132
32MB	0.87	0.17	0.000109	1.040109
128MB	1.38	0.26	0.000153	1.640153

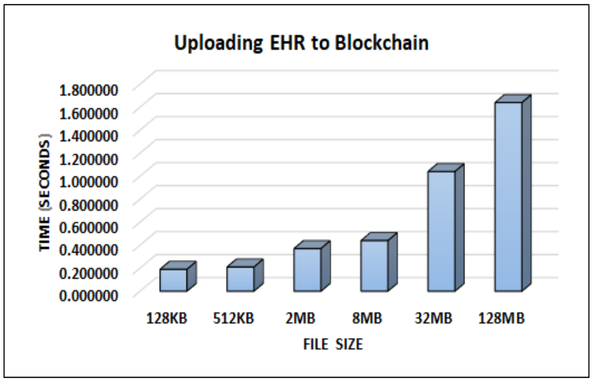


Figure 6. Upload EHR to Blockchain

Similarly, Table 2 shows the total time to download the EHR as the time to retrieve the IPFShash from the blockchain, the time to download the decrypted file from IPFS, and the decryption time. In contrast to uploading EHRs to the blockchain, downloading EHRs takes longer. From Fig. 9, for an EHR size of 2MB, the download time is more than 1 second, at 1.51486 seconds.

Table 2. Total Download time of EHR from Blockchain

File Size	$T_{blkretrieve}$	$T_{downIPFS}$	T_{dec}	$T_{downEHR}$
128KB	0.08	0.57	0.00061	0.65061
512KB	0.08	0.87	0.00231	0.95231
2MB	0.08	1.43	0.00486	1.51486
8MB	0.07	13.04	0.00496	13.11496
32MB	0.07	20.09	0.00481	20.16481
128MB	0.09	36.79	0.00699	36.88699

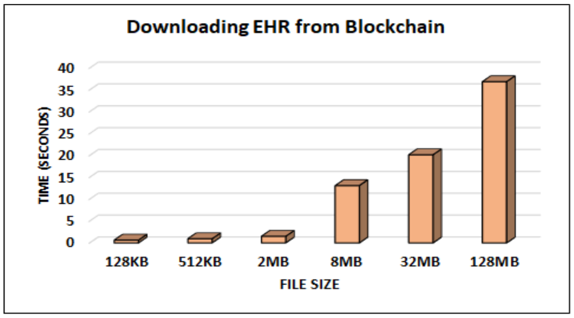


Figure 7. Download Time of EHR from Blockchain

5.2. Results of Transaction Latency

The study measured transaction latency for storing EHRs of different sizes on the blockchain. The Transaction Latency T_{tl} is the time it takes for a transaction to commit and become available across the blockchain network. Let T_{start} be the time at which storage of the encrypted file begins, and let T_{end} be the time at which storage of the IPFShash on the blockchain is completed. Hence, the transaction latency T_{tl} is the difference between the T_{end} and T_{start}. For files larger than 32 MB, transaction latency exceeds 1.04 seconds.

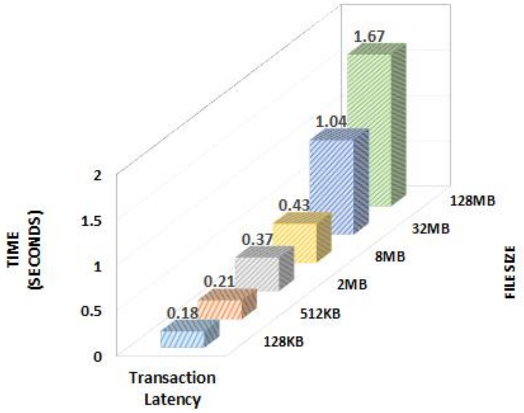
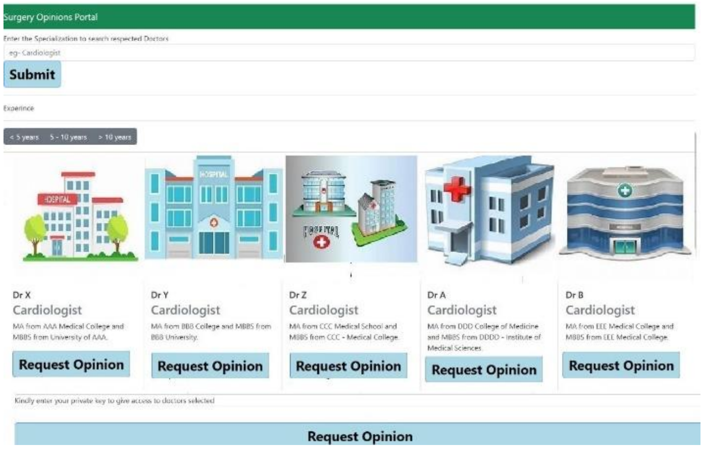


Figure 8. Transaction Latency

5.3. Results of Voting Mechanism

Fig. 9 below shows the patient selecting five doctors based on specialization and experience to obtain an opinion on surgery by entering the 32-bit unique key. The doctors view the patient reports and history stored on GCP for 1 day in an encrypted form. Later, EHR data gets deleted from the GCP to maintain security. Doctors reply in the form of YES/NO. The patient then takes the opinion based on the majority, YES or NO. Fig. 10 below shows the results of the opinion poll, with three doctors replying YES and 2 replying NO. Maximum votes YES; that is a green signal to proceed with the surgery.



Enter the Specialization to search respected Doctors

eg- Cardiologist

Experince

Dr X
Cardiologist
MA from AAA Medical College and MBBS from University of AAA.

Dr Y
Cardiologist
MA from BBB College and MBBS from BBB University.

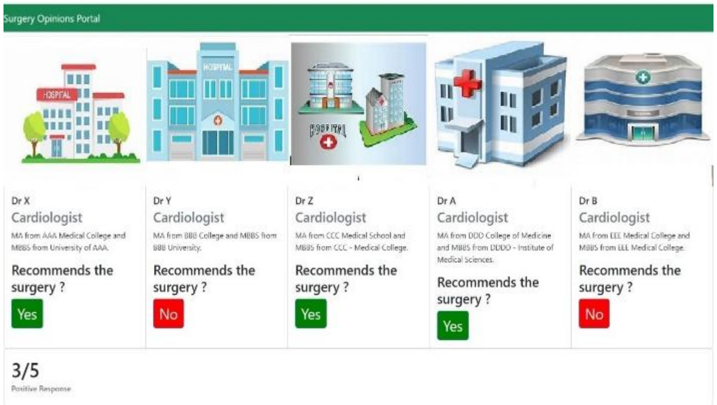
Dr Z
Cardiologist
MA from CCC Medical School and MBBS from CCC - Medical College.

Dr A
Cardiologist
MA from DDD College of Medicine and MBBS from DDDD - Institute of Medical Sciences.

Dr B
Cardiologist
MA from EEE Medical College and MBBS from EEE Medical College.

Kindly enter your private key to give access to doctors selected

Figure 9. Selecting doctors based on the specialization



Dr X
Cardiologist
MA from AAA Medical College and MBBS from University of AAA.
Recommends the surgery ?

Dr Y
Cardiologist
MA from BBB College and MBBS from BBB University.
Recommends the surgery ?

Dr Z
Cardiologist
MA from CCC Medical School and MBBS from CCC - Medical College.
Recommends the surgery ?

Dr A
Cardiologist
MA from DDD College of Medicine and MBBS from DDDD - Institute of Medical Sciences.
Recommends the surgery ?

Dr B
Cardiologist
MA from EEE Medical College and MBBS from EEE Medical College.
Recommends the surgery ?

3/5
Positive Response

Figure 10. Voting Mechanism for a second opinion

6. Discussion

The results from implementing and analyzing the proposed two-level security framework clearly demonstrate its efficiency in resolving the key challenges of EHR sharing. By integrating blockchain with cryptographic methods, the framework provides a secure solution to ensure the confidentiality and integrity of sensitive medical data. The performance analysis verified that selecting XChacha20 as the symmetric cryptography scheme and ECC as the asymmetric mechanism achieves a balance between computational efficiency and security strength. We assessed the efficiency of encryption and decryption processes in blockchain operations for EHRs of varying sizes. The time durations for the encryption and decryption procedures, as conducted by (H. Wang & Song, 2018), (Thwin & Vasupongayya, 2019) and (Boumezbeur & Zarour, 2022), and the proposed method are detailed in Table 3.

Table 3. Comparison of Encryption and Decryption Time with Existing Works and the Proposed Method

Work	(H. Wang & Song, 2018)		(Thwin & Vasupongayya, 2019)		(Boumezbeur & Zarour, 2022)		Proposed method	
File Size	T_{enc}	T_{dec}	T_{enc}	T_{dec}	T_{enc}	T_{dec}	T_{enc}	T_{dec}
128KB	0.36646	0.16169	0.0918	0.00319	0.0012	0.0013	0.000191	0.00061
512KB	0.37069	0.17001	0.094	0.0064	0.0158	0.0027	0.000078	0.00231
2MB	0.37585	0.17967	0.101	0.01662	0.0452	0.0157	0.000073	0.00486
8MB	0.42311	0.22602	0.142	0.05919	0.0615	0.048	0.000132	0.00496
32MB	0.59305	0.40503	0.303	0.23833	0.2064	0.20123	0.000109	0.00481
128MB	2.24242	1.95048	1.828	1.81479	1.4149	1.6284	0.000153	0.00699

Fig.11 shows the time disparity between encryption and decryption in XChaCha20 across various data sizes. This is due to additional computational overhead, including key expansion reversal, inverse substitution, inverse permutation, and vector handling, which contribute to the comparatively longer decryption times.

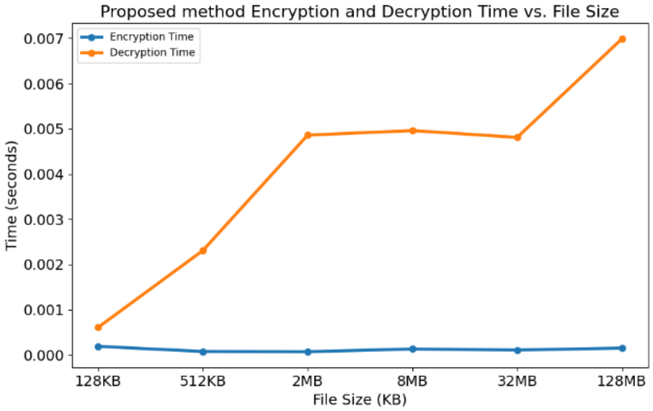
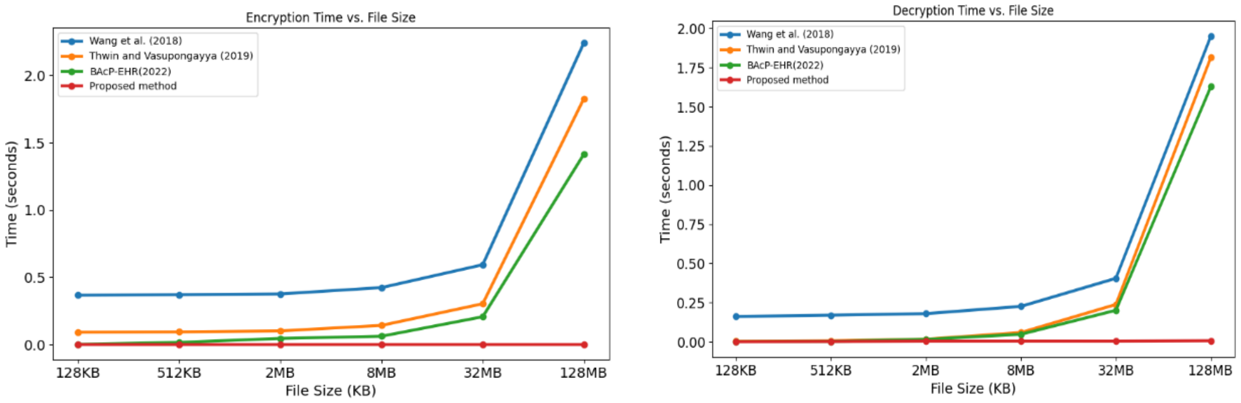


Figure 11. Encryption and Decryption Time of the Proposed Method

We juxtaposed the results depicted in Fig. 11 with the time consumption for encryption and decryption reported in the studies by (H. Wang & Song, 2018), (Thwin & Vasupongayya, 2019), and (Boumezbeur & Zarour, 2022), as illustrated in Fig. 12a and 12b. Notably, the proposed encryption and decryption processes exhibit shorter time durations than those observed in the aforementioned works. In particular, as EHRs grow larger, the proposed scheme demonstrates significant improvements in time efficiency compared to existing works. Given the inclusion of numerous large image files, such as X-rays and CT scans, in EHRs, this approach proves more adept than previous endeavours in health record encryption and decryption.



(a) (b)

Figure 12. Comparison of proposed and existing approaches a) Encryption b) Decryption time

Recently, there has been a paradigm shift in how healthcare data's securely stored and shared transitioning from traditional cloud based systems to those utilizing blockchain technology. Current studies emphasize a growing preference for blockchain-based solutions in healthcare settings. Table 4 compares the existing works with the proposed work.

The research has been conducted across several blockchain platforms. The most popular open source blockchain platforms are Ethereum, Hyperledger Fabric, Hyperledger Composer, and Hyperledger Besu. This study uses a publicly accessible blockchain, Ethereum.

The aforementioned literature employs a range of cryptographic algorithms, including AES, RSA, ECC, and proxy reencryption. Few works (Boumezbeur & Zarour, 2022; Jayabalan & Jeyanthi, 2022) have implemented two-level security during the data storage and sharing.
The proposed work initially analyzes various symmetric and asymmetric cryptographic algorithms as mentioned in the Background section. The efficient algorithm with respect to encryption and decryption time is XChaCha20 for encrypting the EHR while storing it on IPFS, and ECC for encrypting the EHR during sharing with the doctor during the second opinion. Since this work utilizes two-level security while storing and sharing EHR, the resulting system is secure and preserves the privacy and integrity of the EHR.

Also, if the system uses on-chain data storage, it raises scalability concerns and increases storage costs. Some existing systems use either cloud or edge devices to store, which may be less secure. The proposed work uses off-chain storage via IPFS to store the encrypted EHR, which is re-encrypted to generate an IPFShash that is stored on the blockchain, thereby overcoming scalability concerns.

The experiments also highlight the trade-offs between scalability and performance in the system. Uploading EHRs via IPFS and logging their hashes on the Ethereum blockchain reduces storage overhead compared to storing them on-chain. Nevertheless, decryption time becomes an increasingly important factor as file size increases, leading to greater download latency. Although these delays are within reasonable clinical limits, they illustrate the need for further tuning, especially for large medical images such as CT scans and MRIs.

In addition to technical effectiveness, the approach demonstrates the excellent clinical applicability of collaborative decision-making, enabling multiple healthcare professionals to review and vote on a patient's condition without violating confidentiality. In the same vein, emergency access capability is a practical feature that balances the need to receive urgent medical attention in real time with stringent auditability and limited access. These safeguards illustrate that the system is not only theoretically sound but also sufficiently flexible to accommodate real-world healthcare realities.

Despite its strengths, the framework has some limitations. The assessment was done in a simulated testbed with Ganache Ethereum and local IPFS nodes. Real-world deployment in healthcare systems could face additional challenges, including higher blockchain gas fees, regulatory issues, and latency in distributed networks. In addition, the honest participation assumption in the second-opinion case could be susceptible to collusion or unfair decision-making that would demand stronger consensus mechanisms in future research.

Further improvement consists of the use of rotational keys to help patients continue improving the security of EHR sharing. These developments are all consistent with the continuous effort to improve the security and efficiency of healthcare data management processes.

Table 4. Comparing the Existing Approaches with the Proposed Work

Research Work	Blockchain Platform	Security	Privacy	Integrity	Access Control	Scalability	Cryptographic Functions	Storage
(Mohammad Hossein et al., 2021)	Permissioned Private	✓	✓	✓	✓	X	AES	Edge devices
(Jayabalan & Jeyanthi, 2022)	Not Mentioned	X	✓	✓	✓	✓	AES-128 RSA-4096	IPFS
(Boumezbeur & Zarour, 2022)	Ethereum	✓	✓	✓	✓	✓	AES RSA	Cloud
(Rajput et al., 2021)	Hyperledger Fabric	✓	X	✓	X	✓	Not mentioned	Off chain
(Azbeg et al., 2023)	Ethereum	✓	✓	✓	✓	✓	Proxy Reencryption	IPFS
(Egala et al., 2023)	Hyperledger Fabric	✓	✓	✓	✓	X	ECC	IPFS
Proposed Work	Ethereum	✓	✓	✓	✓	✓	XChacha20 ECC	IPFS

7. Conclusion

This research presented a blockchain-based framework for scalable, secure EHR management using XChaCha20 and ECC, along with IPFS and smart contracts on the Ethereum network. The proposed dual-encryption approach ensures confidentiality both in EHR storage and sharing, while off-chain storage addresses the cost and scalability issues of on-chain methods. Experimental results show a gradual increase in performance, with encryption and decryption speeds approaching those of current approaches. The results underscore the framework's real-world applicability to healthcare systems, delivering both security and efficiency.

In the future, this framework can be further developed by incorporating lightweight consensus protocols to boost performance, advanced access-control policies to support healthcare contexts, and interoperability with new blockchain platforms to enable mass deployment. Overall, the proposed system shows that blend of blockchain with effective cryptography and decentralized storage is a realistic and scalable path toward secure and patient-focused healthcare data management.

References

AIIMS-AIIMS's unprecedented data breach sparks fears hackers could misuse information-Telegraph India. (2022, February 12). https://telegraphindia. com/india/aiims-unprecedented/data-breach-sparks-fears-hackers-could-misuse-information/cid/ 1901550. [Online;]

Azbeg, K., Ouchetto, O., & Jai Andaloussi, S. (2023). Access Control and Privacy-Preserving Blockchain-Based System for Disease Management. *IEEE Transactions on Computational Social Systems*, *10*(4), 1515–1527. https://doi.org/10.1109/TCSS.2022.3186945

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

Chen, C.-L., Yang, J., Tsaur, W.-J., Weng, W., Wu, C.-M., & Wei, X. (2022). Enterprise Data Sharing with Privacy-Preserved Based on Hyperledger Fabric Blockchain in IIOT's Application. *Sensors*, *22*(3), 1146. https://doi.org/10.3390/s22031146

Chenthara, S., Ahmed, K., Wang, H., Whittaker, F., & Chen, Z. (2020). Healthchain: A novel framework on privacy preservation of electronic health records using blockchain technology. *PLOS ONE*, *15*(12), e0243043. https://doi.org/10.1371/journal.pone.0243043

Cifuentes, M., Davis, M., Fernald, D., Gunn, R., Dickinson, P., & Cohen, D. J. (2015). Electronic Health Record Challenges, Workarounds, and Solutions Observed in Practices Integrating Behavioral Health and Primary Care. *The Journal of the American Board of Family Medicine*, *28*(Supplement 1), S63–S72. https://doi.org/10.3122/jabfm.2015.S1.150133

Dubovitskaya, A., Xu, Z., Ryu, S., Schumacher, M., & Wang, F. (2017). Secure and Trustable Electronic Medical Records Sharing using Blockchain. *AMIA ... Annual Symposium Proceedings. AMIA Symposium*, *2017*, 650–659.

Egala, B. S., Pradhan, A. K., Badarla, V., & Mohanty, S. P. (2021). Fortified-Chain: A Blockchain-Based Framework for Security and Privacy-Assured Internet of Medical Things With Effective Access Control. *IEEE Internet of Things Journal*, *8*(14), 11717–11731. https://doi.org/10.1109/JIOT.2021.3058946

Egala, B. S., Pradhan, A. K., Dey, P., Badarla, V., & Mohanty, S. P. (2023). Fortified-Chain 2.0: Intelligent Blockchain for Decentralized Smart Healthcare System. *IEEE Internet of Things Journal*, *10*(14), 12308–12321. https://doi.org/10.1109/JIOT.2023.3247452

Fan, K., Wang, S., Ren, Y., Li, H., & Yang, Y. (2018). MedBlock: Efficient and Secure Medical Data Sharing Via Blockchain. *Journal of Medical Systems*, *42*(8), 136. https://doi.org/10.1007/s10916-018-0993-7

Ganiga, R., Pai, M. R., Pai, M. M. M., & Sinha, R. K. (2017). Cloud-Enabled Standard Electronic Health Record Architecture for Indian Healthcare Sector. *Indian Journal of Public Health Research & Development*, *8*(4), 554. https://doi.org/10.5958/0976-5506.2017.00398.9

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

HIPAA Journal. (2022). *HIPAA Journal*. https :// www .hipaajournal .com/healthcare-data-breach-statistics/.[

Holmes, J. H., Beinlich, J., Boland, M. R., Bowles, K. H., Chen, Y., Cook, T. S., Demiris, G., Draugelis, M., Fluharty, L., Gabriel, P. E., Grundmeier, R., Hanson, C. W., Herman, D. S., Himes, B. E., Hubbard, R. A., Kahn, C. E., Kim, D., Koppel, R., Long, Q., … Moore, J. H. (2021). Why Is the Electronic Health Record So Challenging for Research and Clinical Care? *Methods of Information in Medicine*, *60*(01/02), 032–048. https://doi.org/10.1055/s-0041-1731784

Jamshed, N., Ozair, F., Sharma, A., & Aggarwal, P. (2015). Ethical issues in electronic health records: A general overview. *Perspectives in Clinical Research*, *6*(2), 73. https://doi.org/10.4103/2229-3485.153997

Jayabalan, J., & Jeyanthi, N. (2022). Scalable blockchain model using off-chain IPFS storage for healthcare data security and privacy. *Journal of Parallel and Distributed Computing*, *164*, 152–167. https://doi.org/10.1016/j.jpdc.2022.03.009

Kavitha, R., Kannan, E., & Kotteswaran, S. (2016). Implementation of Cloud-based Electronic Health Record (EHR) for Indian Healthcare Needs. *Indian Journal of Science and Technology*, *9*(3). https://doi.org/10.17485/ijst/2016/v9i3/86391

Kim, M., Yu, S., Lee, J., Park, Y., & Park, Y. (2020). Design of Secure Protocol for Cloud-Assisted Electronic Health Record System Using Blockchain. *Sensors, 20*(10), 2913. https://doi.org/10.3390/s20102913

Le Nguyen, B., Laxmi Lydia, E., Elhoseny, M., V. Pustokhina, I., A. Pustokhin, D., Mohamed Selim, M., Nhu Nguyen, G., & Shankar, K. (2020). Privacy Preserving Blockchain Technique to Achieve Secure and Reliable Sharing of IoT Data. *Computers, Materials & Continua*, *65*(1), 87–107. https://doi.org/10.32604/cmc.2020.011599

Liu, Z., Weng, J., Li, J., Yang, J., Fu, C., & Jia, C. (2016). Cloud-based electronic health record system supporting fuzzy keyword search. *Soft Computing*, *20*(8), 3243–3255. https://doi.org/10.1007/s00500-015-1699-0

Mohammad Hossein, K., Esmaeili, M. E., Dargahi, T., Khonsari, A., & Conti, M. (2021). BCHealth: A Novel Blockchain-based Privacy-Preserving Architecture for IoT Healthcare Applications. *Computer Communications*, *180*, 31–47. https://doi.org/10.1016/j.comcom.2021.08.011

Palabindala, V., Pamarthy, A., & Jonnalagadda, N. R. (2016). Adoption of electronic health records and barriers. *Journal of Community Hospital Internal Medicine Perspectives*, *6*(5), 32643. https://doi.org/10.3402/jchimp.v6.32643

Rajput, A. R., Li, Q., & Ahvanooey, M. T. (2021). A Blockchain-Based Secret-Data Sharing Framework for Personal Health Records in Emergency Conditions. *Healthcare*, *9*(2), 206. https://doi.org/10.3390/healthcare9020206

Shuaib, K., Abdella, J., Sallabi, F., & Serhani, M. A. (2022). Secure decentralized electronic health records sharing system based on blockchains. *Journal of King Saud University - Computer and Information Sciences*, *34*(8), 5045–5058. https://doi.org/10.1016/j.jksuci.2021.05.002

Thwin, T. T., & Vasupongayya, S. (2019). Blockchain-Based Access Control Model to Preserve Privacy for Personal Health Record Systems. *Security and Communication Networks*, *2019*, 1–15. https://doi.org/10.1155/2019/8315614

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

Wang, Y., Zhang, A., Zhang, P., & Wang, H. (2019). Cloud-Assisted EHR Sharing With Security and Privacy Preservation via Consortium Blockchain. *IEEE Access*, *7*, 136704–136719. https://doi.org/10.1109/ACCESS.2019.2943153

Xia, Q., Sifah, E., Smahi, A., Amofa, S., & Zhang, X. (2017). BBDS: Blockchain-Based Data Sharing for Electronic Medical Records in Cloud Environments. *Information*, *8*(2), 44. https://doi.org/10.3390/info8020044

Zaied, A. N. H., Elmogy, M., & Elkader, S. A. (2016). A Proposed Cloud-based Framework for Integrating Electronic Health Records. *Proceedings of the 10th International Conference on Informatics and Systems*, 139–145. https://doi.org/10.1145/2908446.2908478