



ARTICLE

Decentralized Authentication and Secure Distributed File Storage for Healthcare Systems Using Blockchain and IPFS

Maazen Alsabaan¹, Jasmin Praful Bharadiya², Vishwanath Eswarakrishnan³,
Adnan Mustafa Cheema⁴, Zaid Bin Faheem⁵ and Jehad Ali^{6,*}

¹Department of Computer Engineering, College of Computer and Information Sciences (CCIS), King Saud University, Riyadh, 11451, Saudi Arabia

²Department of Computer Science, University of the Cumberlands, Williamsburg, KY 40769, USA

³Ads Publishing Infra, Meta Platforms Inc., CA 94025, USA

⁴Department of Information Technology, Rawalpindi Women University, Rawalpindi, 46000, Pakistan

⁵Department of Computer Science, Wuhan University, Wuhan, 430000, China

⁶Department of AI Convergence Network, Ajou University, Suwon, 16499, Republic of Korea

*Corresponding Author: Jehad Ali. Email: jehadali@ajou.ac.kr

Received: 22 April 2025; Accepted: 04 July 2025; Published: 29 August 2025

ABSTRACT: The healthcare sector involves many steps to ensure efficient care for patients, such as appointment scheduling, consultation plans, online follow-up, and more. However, existing healthcare mechanisms are unable to facilitate a large number of patients, as these systems are centralized and hence vulnerable to various issues, including single points of failure, performance bottlenecks, and substantial monetary costs. Furthermore, these mechanisms are unable to provide an efficient mechanism for saving data against unauthorized access. To address these issues, this study proposes a blockchain-based authentication mechanism that authenticates all healthcare stakeholders based on their credentials. Furthermore, also utilize the capabilities of the InterPlanetary File System (IPFS) to store the Electronic Health Record (EHR) in a distributed way. This IPFS platform addresses not only the issue of high data storage costs on blockchain but also the issue of a single point of failure in the traditional centralized data storage model. The simulation results demonstrate that our model outperforms the benchmark schemes and provides an efficient mechanism for managing healthcare sector operations. The results show that it takes approximately 3.5 s for the smart contract to authenticate the node and provide it with the decryption key, which is ultimately used to access the data. The simulation results show that our proposed model outperforms existing solutions in terms of execution time and scalability. The execution time of our model smart contract is around 9000 transactions in just 6.5 s, while benchmark schemes require approximately 7 s for the same number of transactions.

KEYWORDS: InterPlanetary file system; healthcare; electronic health record

1 Introduction

Electronic Health Records (EHRs) are a process of electronically storing and managing patients' healthcare records. According to a study, the market value of EHRs is expected to reach approximately 35 billion dollars by 2025 [1]. Several benefits are provided to hospitals and patients using the capabilities of EHRs. However, the authors in [2] observe that not all hospitals effectively utilize EHRs in their Information Technology (IT) sector. These hospitals are utilizing the traditional mechanism in which the records of



hospitals are stored on a centralized server, which causes the issues of data loss and single point of failure due to the involvement of third parties [3,4].

Today, healthcare data is observed to be vulnerable to severe security issues during data transfer. Furthermore, conventional healthcare data transfer mechanisms are unable to facilitate the transfer of large amounts of data due to their limited network bandwidth, which ultimately increases the cost of data transfer between hospitals [5]. To address these aforementioned issues, blockchain technology can be integrated with EHRs, thereby enhancing the data exchange rate of the network. Blockchain is a distributed protocol in which all participants, including sellers and buyers, form the foundation of the network. All transactions are verified in a distributed manner by high-resource nodes, which are referred to as miners [6]. However, storing data on the blockchain network is very expensive because a copy of the data is created and stored on different devices to mitigate the issue of data loss. Although the issue of data loss is solved by blockchain the cost of storing this data is very high. According to [7], storing 1 MB of data on the blockchain costs approximately 14,000 USD, which is not suitable for the resource-constrained healthcare sector. To address this challenge, we utilize the functionalities of an external data storage platform known as the InterPlanetary File System (IPFS). Within IPFS, data is partitioned into multiple chunks and distributed across globally dispersed nodes. This approach effectively resolves both the high storage cost limitation of blockchain systems and the single point of failure vulnerability inherent in traditional centralized storage architectures. The blockchain framework itself builds upon the foundational concept of Bitcoin, introduced by Satoshi Nakamoto in 2009. The blockchain network comprises multiple decentralized nodes that collectively verify all network transactions through a distributed consensus mechanism, as illustrated in Fig. 1.

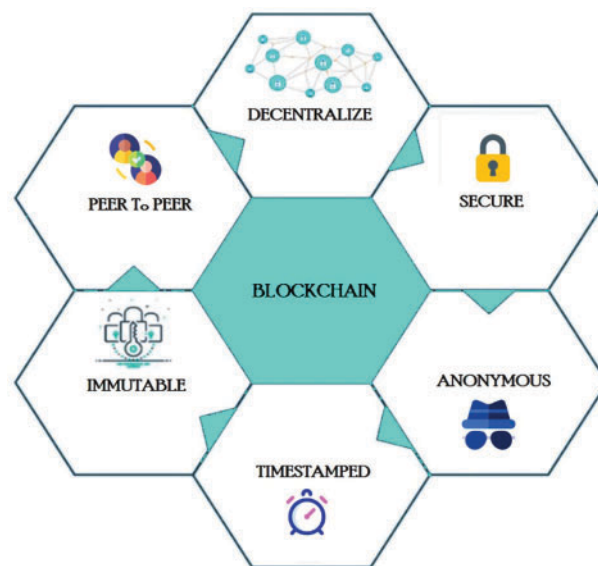


Figure 1: Blockchain structure

This not only provides a mechanism for saving monetary resources but also solves the issue of a single point of failure by using a distributed validation mechanism. Different studies indicate that approximately 24 cryptocurrencies are used to facilitate the operations of smart healthcare [8]. These currencies are stored in a digital wallet, and the currencies in these wallets can be accessed just by using an Internet connection. One of the most widely used cryptocurrencies is SOLVE, which is utilized in the healthcare sector. This currency is operated by SOLVE.CARE platform [9]. Such cryptocurrency tokens are used to facilitate the processing,

storage, and management of healthcare data. One of the most reliable and efficient tokens from the Medibloc organization is Medibloc, which operates within the group to facilitate healthcare operations. Furthermore, a blockchain decentralized protocol is used to build a decentralized access token, named Panacea, which is used to store sensitive information of healthcare stakeholders in the network [10].

Blockchain technology provides unique benefits that traditional distributed systems with PKI (Public-Key Infrastructure) infrastructure cannot fully achieve, particularly in scenarios involving decentralized trust. The distributed nature of blockchain ensures a tamper-proof and transparent mechanism for managing healthcare records, which is crucial in environments that demand high security and data integrity. In this study, we propose a mechanism for storing sensitive patient data and other electronic healthcare records on a decentralized blockchain-based network. This will not only encourage external entities to join such healthcare record networks but also facilitate internal users to share their data. Our proposed model also solves the security issues of data and ensures efficient data transfer between distributed entities. In our proposed model, the patient data is converted into ciphertext using the capabilities of proxy re-encryption [11]. A single key is used in our model to encrypt and decrypt the data of patients and when data is firstly encrypted by the healthcare providers then this data can not be decrypted by the intermediate service providers because these service providers do not have access to the single private key, which is only shared between communicating parties. The authors in [12] propose a mechanism to solve the issue of data storage with encryption techniques. However, the proposed model is centralized and vulnerable to collusion attacks. When any intermediate third party gets access to the private key in the network then this party can alter the data, and the security of the network will be at risk. To address the aforementioned issues, we propose a blockchain-based mechanism that integrates IPFS and an access control system. The proposed model addresses several potential security attacks, including poisoning attacks, unauthorized access, and data manipulation. Poisoning attacks, where adversaries inject malicious data into the system, are mitigated through a combination of encryption and digital signatures. Furthermore, the blockchain-based authentication mechanism prevents unauthorized nodes from accessing sensitive data. The contributions of our proposed model are given below.

- Our proposed model provides a mechanism to ensure data integrity with the help of Ethereum channels, which can offer a robust defense against network attacks and protect sensitive data from breaches, ultimately enhancing the integrity of the data in our model.
- In our model, a membership mechanism is proposed in which the identity of each user is authorized by higher authorities, which ultimately solves the issue of unauthorized access to the data in our proposed model.
- A distributed data storage platform IPFS is used to solve the issue of costly data storage on the blockchain.

2 Related Work

2.1 Decentralized Authentication Methods

The authors in [13] state that it is very difficult for sensor nodes to sense and send the data with their precise location as there is no efficient localization mechanism. Therefore, the authors propose a blockchain-based mechanism in which high-resource beacon nodes are used by unknown nodes to find their location. The beacon nodes already know their location, and unknown nodes find their distance from the beacon nodes by using the Euclidean distance formula and find their exact coordinates. The authors propose a trust evaluation mechanism for selecting the most suitable and legitimate beacon nodes. The performance of the proposed model is evaluated in terms of false positive rate, average localization error, detection accuracy, false negative rate, and average energy consumption. However, there is no mechanism to identify and remove malicious nodes within the trust evaluation mechanism. The authors in [14] state that existing

schemes for detecting intruders and malicious nodes are developed for static network topologies, and these techniques are not efficient for dynamic and mobile network structures. To solve this issue, the authors propose a blockchain-based mechanism for mobile Internet of Things (IoT) devices and sensor nodes. In this mechanism, the uncertainty principle is used to ensure the stability of the network. Furthermore, our model also develops dynamic and heterogeneous clusters, utilizing the capabilities of uncertainty principles. The blockchain-distributed architecture is utilized for developing paths for multi-hop routing, which not only facilitates the identification and removal of external attackers but also provides energy-efficient data transfer paths. The proposed model is evaluated in terms of network lifetime, consumption of energy, packet drop ratio, end-to-end delay, and routing overheads. In the future, the authors aim to use a realistic network setup to further enhance the performance of the proposed model. The author in [15] states that existing schemes for healthcare and industrial network security are not able to protect data against unauthorized access. Therefore, the authors propose a hybrid blockchain-based mechanism for the registration and authentication of various entities within the blockchain network. Higher authority nodes, such as sink nodes, are used for registering and authenticating cluster heads, which in turn register and authenticate low-energy, ordinary sensor nodes. The proposed model is evaluated in terms of message size, mutual authentication, replay attacks, and Sybil attacks. However, there is no mechanism to protect this blockchain-based model against external intruder nodes. Similarly, the authors in [16] identify the same issue that existing mechanisms for authentication are unreliable and unable to perform peer authentication. Therefore, the authors propose a blockchain-based model in which the trust of each node is calculated and data is validated, utilizing the capabilities of the blockchain's distributed protocol in the network architecture. Furthermore, the trust is evaluated based on human knowledge, and the reputation of each node is stored in a distributed manner throughout the network. The proposed model is evaluated in terms of trust value, false positive rates, energy consumption, reputation level, and false negative rates. In the future, the proposed model will be deployed on a large scale to enhance its performance further. The comprehensive analysis of decentralized existing approaches is shown in Table 1.

Table 1: Comprehensive analysis of decentralized existing approaches: challenges, innovations, evaluations and future directions

Addressed limitations	Proposed contributions	Performance parameters	Research gaps
It is very difficult for sensor nodes to sense and send the data with their precise location as there is no efficient localization mechanism [13].	A blockchain-based mechanism is proposed in which high-resource beacon nodes are used by unknown nodes to find their location.	False positive rate, average localization error, detection accuracy, false negative rate, and average energy consumption.	There is no mechanism to identify and remove malicious nodes in the trust evaluation mechanism.
Existing schemes for intruders and malicious node detection are developed for static network topology, and these techniques are not efficient for dynamic and mobile network structures [14].	A blockchain-based mechanism is proposed for mobile Internet of Things (IoT) devices and sensor nodes. In this mechanism, the uncertainty principle is used to ensure the stability of the network.	Network lifetime, consumption of energy, packet drop ratio, end-to-end delay, and routing overheads.	A realistic network setup will be used to further enhance the performance of the proposed model.

(Continued)

Table 1 (continued)

Addressed limitations	Proposed contributions	Performance parameters	Research gaps
Existing schemes for healthcare and industrial network security are not able to protect data against unauthorized access [15].	A hybrid blockchain-based mechanism for the registration and authentication of different entities in the blockchain network.	Message size, mutual authentication, replay attacks, and Sybil attacks.	There is no mechanism to protect this blockchain-based model against external intruder nodes.
Existing mechanisms for authentication are not reliable and are unable to perform peer authentication [16].	Blockchain-based model in which the trust of each node is calculated and data is validated while utilizing the capabilities of blockchain.	Trust value, false positive rates, energy consumption, reputation level, and false negative rate.	The proposed model will be deployed on a large scale to further enhance the performance of the model.

2.2 Distributed File Storage Methods

The authors in [17] state that the existing routing schemes are not able to provide efficient routing paths as these schemes do not consider the untrusted behavior of network nodes. Furthermore, the activities of malicious nodes negatively impact the overall performance of the network, which is particularly unsuitable for wireless sensor networks and IoT device networks. Therefore, the authors propose a blockchain-based routing mechanism in which reinforcement learning is used for the detection of malicious nodes by utilizing their trust values. This detection mechanism enhances the routing mechanism by the selection of the most reliable and dynamic links based on the trust values of nodes. The proposed model is evaluated in terms of total transaction throughput, transaction gas consumption, transaction latency, network packet delay, and network storage. In the future, a more unique and efficient algorithm will be utilized to enhance the performance and portability of the proposed model. The authors in [18] state that existing security protocols for malicious node detection are not efficient, as their fairness and ability to provide traceability of actual malicious nodes is not trustworthy. Therefore, the authors propose a blockchain-based mechanism that utilizes a trust model for identifying and removing malicious nodes in the network. The authors in [19] state that existing routing mechanisms for selecting the routing paths are not efficient, as their fairness and ability to provide traceability of actual malicious nodes is not trustworthy. Therefore, the authors propose a blockchain-based mechanism that utilizes contractual routing to identify and select the most reliable paths in the network by detecting and removing malicious nodes. All the activities of nodes in the network are monitored and validated by the miner nodes. When a node performs malicious activity, it can be easily traced using the capabilities of the Merkle tree. In this way, the proposed model can provide an efficient mechanism for tracing and removing malicious nodes in the network. The performance of the proposed model is evaluated in terms of routing overheads, routing latency, throughput, route request packets, and packet delivery ratio. In the future, the performance of the proposed model can be further improved by implementing it on mobile ad-hoc networks.

Similarly, the authors in [20] state that ensuring the security of data in underwater IoT devices is very challenging, as these environments are highly dynamic, and existing schemes are unable to provide privacy simultaneously. Therefore, the authors propose a monitoring architecture for underwater IoT devices in

which the fog nodes and cloud servers are used for processing and storing the data of the underwater network. All the activities of IoT devices are monitored by blockchain nodes, and secure routing is provided by ensuring the legitimacy and honesty of data sources. The performance of the proposed model is evaluated in terms of energy consumption, time for block generation, network remaining energy, reliability, and number of rounds. In the future, the performance of the proposed model can be further enhanced by implementing it on terrestrial IoT devices. The author in [21] states that existing schemes for IoT network security are not able to protect data against unauthorized access. Therefore, the authors proposed a blockchain-based lightweight mechanism for registering and authenticating various IoT devices within the blockchain network. The higher authority nodes are responsible for registering and authenticating cluster heads and these cluster heads are used for the registration and authentication of low-energy ordinary sensor nodes. The proposed model is evaluated regarding message size, mutual authentication, and broadcasting requests. However, there is no mechanism to protect this blockchain-based model against external intruding IoT devices. The comprehensive analysis of distributed existing approaches is shown in Table 2.

Table 2: Comprehensive analysis of distributed existing approaches: challenges, innovations, evaluations and future directions

Addressed limitations	Proposed contributions	Performance parameters	Research gaps
Existing routing schemes are unable to provide efficient routing paths, as they do not consider the untrusted behavior of network nodes [17].	A blockchain-based routing mechanism is proposed in which reinforcement learning is used for the detection of malicious nodes by utilizing their trust values.	Total transaction throughput, transaction gas consumption, transaction latency, network packet delay, and network storage.	More unique and efficient algorithms will be utilized to enhance the performance and portability of the proposed model.
Existing security protocols for malicious node detection are not efficient as their fairness and ability to provide traceability of actual malicious nodes are not trustworthy [18].	A blockchain-based mechanism is proposed, utilizing a trust model for the identification and removal of malicious nodes in the network.	Credit score of sensor nodes, transaction cost, execution cost, and communication range.	The performance of the proposed model will be improved by using a proof-of-stake consensus algorithm instead of proof of work.
Existing routing mechanisms for selecting the routing paths are not efficient, as their fairness and ability to provide traceability of actual malicious nodes are not trustworthy [19].	A blockchain-based mechanism is proposed in which contractual routing is used for the identification and selection of the most reliable paths in the network.	Routing overheads, routing latency, throughput, route request packet, and packet delivery ratio.	The performance of the proposed model will be improved by implementing it on mobile ad-hoc networks.

(Continued)

Table 2 (continued)

Addressed limitations	Proposed contributions	Performance parameters	Research gaps
Ensuring the security of data in underwater IoT devices is very challenging, as these environments are highly dynamic and existing schemes are unable to provide privacy simultaneously [20].	A monitoring architecture is proposed for underwater IoT devices in which fog nodes and cloud servers are used for processing and storing the data of the underwater network.	Energy consumption, time for block generation, network remaining energy, reliability, and number of rounds.	The performance of the proposed model will be enhanced by implementing it on terrestrial IoT devices.
Existing schemes for IoT network security are not able to protect data against unauthorized access [21].	A blockchain-based lightweight mechanism for the registration and authentication of IoT devices in the network.	Message size, mutual authentication, and broadcasting request.	There is no mechanism to protect this blockchain-based model against external intruding IoT devices.

The authors in [22] state that existing schemes for intruders and malicious node detection in healthcare and industry are not efficient and are unable to protect healthcare networks against cyber-physical attacks. To solve this issue, the authors propose a blockchain-based mechanism for healthcare devices and sensor nodes. In this mechanism, cloud and fog servers are integrated with blockchain technology to ensure network stability. Furthermore, our model also develops dynamic and heterogeneous clusters, utilizing the capabilities of the blockchain decentralized protocol. The proposed model is evaluated in terms of execution delay, percentage of patterns, and total validation time. In the future, the authors aim to minimize network energy consumption and time by integrating the federated learning mechanism with our proposed model. Similarly, Shahidinejad et al. propose a decentralized authentication and key exchange protocol specifically designed for device-to-device (D2D) communication in edge-enabled IoT environments. Their approach combines lattice-based post-quantum cryptography with edge computing and blockchain technologies to address key challenges such as heavy storage requirements, weak anonymity, and inefficient key revocation in existing systems. By leveraging edge computing, the protocol reduces computational burdens on IoT devices, while blockchain ensures decentralized and secure public key management. Security analyses confirm resistance against classical and quantum attacks, and performance evaluations show a significant reduction in computational and communication overhead. This makes the protocol a lightweight, efficient, and quantum-resistant solution for secure D2D authentication in IoT [23].

Sivaprakash et al. introduce a decentralized framework that integrates the IPFS with blockchain technology to enhance the security, privacy, and accessibility of healthcare data. In this system, patients' EHRs are encrypted and stored on IPFS, ensuring data redundancy and resilience against single points of failure [24]. Each stored file is assigned a unique cryptographic hash, which is then recorded on the blockchain, providing an immutable and transparent audit trail of data access and modifications. Smart contracts govern access control, allowing patients to grant or revoke permissions to healthcare providers in real-time, thereby maintaining patient autonomy over personal health information. This architecture not only ensures data integrity and confidentiality but also facilitates interoperability among disparate healthcare systems, paving the way for a more secure and patient-centric approach to health data management. Similarly, Shankar et al. present a secure healthcare system that integrates blockchain technology with the IPFS to enhance the

security and privacy of patient data [25]. Recognizing the challenges of storing large medical files directly on the blockchain, the proposed system utilizes IPFS for off-chain storage, ensuring data integrity through its built-in hashing algorithm. To authenticate data exchanges, the system employs the Edwards-curve Digital Signature Algorithm (EdDSA), providing a robust consensus mechanism. All communications between nodes are encrypted, safeguarding against unauthorized access. Experimental evaluations demonstrate that this approach not only strengthens data security and privacy but also improves performance metrics, such as faster file upload speeds and higher transaction rates, compared to existing systems.

Nowadays, it is observed that healthcare data is vulnerable to severe issues of security in data transfer. Furthermore, the conventional healthcare data transfer mechanisms are not able to facilitate large amounts of data transfer due to their low network bandwidth, which ultimately increases the cost of data transfer between hospitals. To address these aforementioned issues, blockchain technology can be integrated with EHRs, thereby enhancing the data exchange rate of the network [26]. Blockchain is a distributed protocol in which all sellers and buyers act as the foundation of the network. All the transactions are verified in a distributed way by the high-resource nodes, which are called miners. However, it is very expensive to store data on the blockchain network because a copy of the data is created and stored on different devices to solve the issue of data loss. Although the issue of data loss is solved by blockchain the cost of storing this data is very high. According to, when we store 1 MB of data on the blockchain, it costs us around 14,000 USD, which is not suitable for the resource-constrained healthcare sector [27].

3 Proposed Methodology

We propose a mechanism, named Blockchain-based MedicalChain (BMC), which is used to share and store the sensitive information of medical patients. The smart contracts are utilized in our BMC model to ensure the reliable sharing of data while simultaneously protecting it against intruders and internal malicious nodes within the network, ultimately enhancing the integrity of the data. Furthermore, we also ensure that no one can access sensitive patient information without proper authorization. To ensure this, we propose a smart contract-based authentication mechanism. In our proposed mechanism, firstly, any node must have a valid identity for the authentication process in the EHR system [28]. Smart contracts in our system serve as the core enforcement mechanism for validating user identities, managing role-based access permissions, recording audit trails, and automating access decisions. Their updated placement and interconnections are now clearly defined to strengthen their visibility and relevance within the framework. Furthermore, every node in the network should have a specific responsibility and function associated with its particular identity. For the authentication process, each node first registers in the blockchain network by broadcasting its unique identity and role to the smart contract. All its credentials will be stored in the network for authentication purposes. In any next time, when any node wants to access the data of the network then this node needs to provide its specific identity and function [29]. The smart contract verifies the data provided by the node by matching this data with the already stored credentials. If both the data are matched then this node is given access to the data. Otherwise, this node is not given any access to the sensitive information of the patients or broadcaster as the malicious nodes in the network. The whole blockchain-based authentication process is shown in Algorithm 1. Furthermore, our proposed model ensures the transfer of large amounts of patients' sensitive data in the network as the entities in the network keep on increasing with time. Therefore, there should be an interface that streamlines all the resources of EHRs and their utilization. In our system, user verification is achieved through a secure, decentralized authentication process embedded within the blockchain infrastructure. Initially, each user (e.g., a healthcare provider or a patient) generates a unique identity that comprises their public key, role, and a digital signature. Upon registration, this information is sent to a smart contract deployed on the blockchain, which verifies the digital signature using cryptographic functions and stores

the verified identity along with metadata (such as role and timestamp). For example, when a user attempts to access a patient's file, they submit their credentials, which are matched against the verified entries stored immutably on the blockchain. If the signature and identity hash are valid, access is granted; otherwise, the request is rejected and logged as a potential threat. This ensures that only authenticated users can interact with the system.

Algorithm 1 presented outlines a smart contract-based authentication process for securing access to a blockchain network. Initially, the blockchain network \mathcal{B} is set up along with a smart contract \mathcal{S} , which serves as the central authority for verifying and authenticating nodes. The network consists of a set of nodes $\mathcal{N} = \{n_1, n_2, \dots, n_k\}$, where each node n_i is assigned a unique identity ID_i and a role R_i . The credentials of these nodes, including their identity and role, are stored in the blockchain as a set \mathcal{C} . During the registration process, each node broadcasts its identity and role to the smart contract \mathcal{S} . The smart contract verifies the credentials and stores them securely in the blockchain. This registration step ensures that every node in the network is authenticated before participating in network activities. When a node, say n_j , requests access to the network's data, it must provide its identity ID_j and role R_j to the smart contract for verification. The smart contract checks whether the credentials of n_j match the stored records in \mathcal{C} . If a match is found, n_j is granted access; otherwise, the request is denied, and the node is marked as malicious.

Algorithm 1: Smart contract-based authentication process

```

1: Initialization:
2:   Initialize the blockchain network  $B$ 
3:   Deploy and initialize the smart contract  $S$  on the blockchain
4:   Define a set of participating nodes  $N = \{n_1, n_2, \dots, n_k\}$ 
5:   Each node  $n_u$  is assigned a unique identity  $ID_u$  and a role  $R_u$ 
6:   Define a credential repository  $C$  maintained in the blockchain ledger
7: Node Registration Phase:
8: for each node  $n_i \in N$  do
9:   Node  $n_i$  generates a registration request containing its identity and role:  $\{ID_i, R_i\}$ 
10:   $n_i$  computes hash  $H(ID_i || R_i || T(t_i))$  using a secure hash function  $H(\cdot)$ 
11:   $n_i$  signs the hash with its private key to create a digital signature  $\sigma_i$ 
12:   $n_i$  sends  $(ID_i, R_i, H(ID_i || R_i || T(t_i)), \sigma_i)$  to the smart contract  $S$ 
13:  Smart contract  $S$  verifies the authenticity of the signature and the timestamp
14:  If valid, the tuple  $(ID_i, R_i, H(ID_i || R_i || T(t_i)))$  is stored in  $C$ 
15: end for
16: Authentication Request Phase:
17: A node  $n_j$  requests access to specific data or service within the network
18:  $n_j$  provides its identity and role along with a signed hash:  $(ID_j, R_j, H(ID_j || R_j || T(t_j)), \sigma_j)$ 
19: Verification Phase:
20: Smart contract  $S$  checks if  $H(ID_j || R_j || T(t_j))$  exists in  $C$ 
21:  $S$  verifies the digital signature  $\sigma_j$  and timestamp validity
22: if the hash is found in  $C$  and the signature  $\sigma_j$  is verified then
23:    $S$  grants access to node  $n_j$ 
24: else
25:    $S$  denies access and flags node  $n_j$  as potentially malicious
26: end if

```

4 System Architecture

The consortium blockchain-based architecture of our proposed model is shown in Fig. 2. There are three basic components of our proposed architecture. First of all, consortium blockchain is used to implement a decentralized blockchain-based protocol. Secondly, the application module is used to ensure the service provisioning mechanism is efficient and reliable. The last component is IPFS, which is used to store the data of the healthcare system on the globally distributed components.

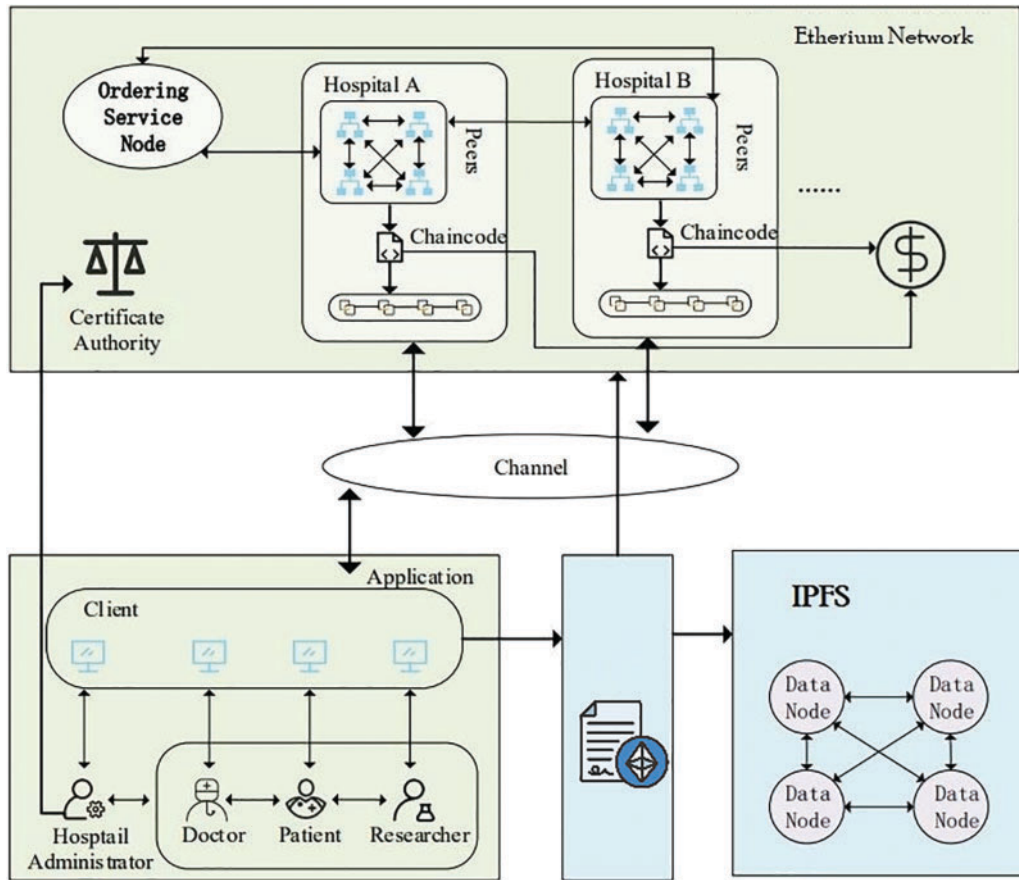
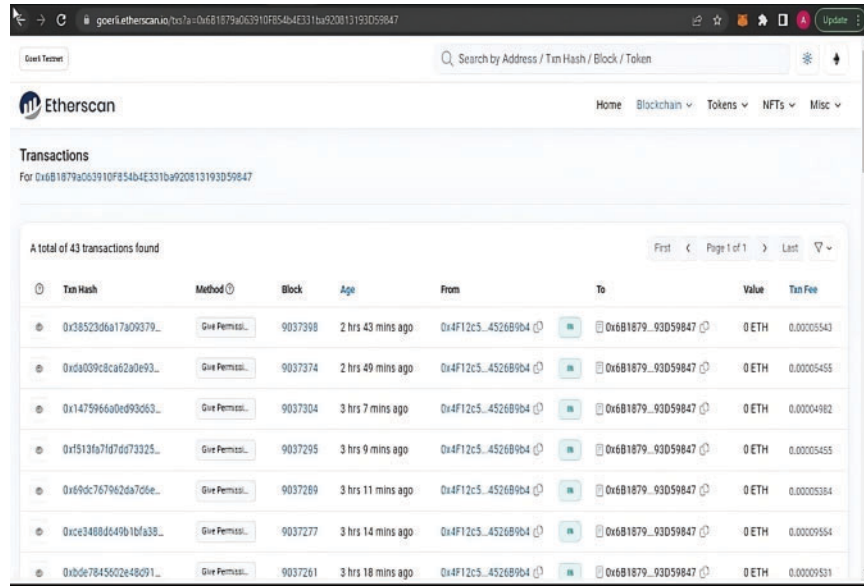


Figure 2: Consortium blockchain-based system architecture

4.1 Consortium Blockchain

Consortium blockchain is a decentralized protocol that operates without the involvement of any third party in the healthcare sector. All activities related to token allocation, credential verification for various entities, and arbitration of service provisioning mechanisms are handled by the consortium blockchain network. The nodes that are authenticated by the smart contract after providing their credentials have access to healthcare data [30]. This consortium blockchain mechanism not only facilitates the efficient accessibility of data but also ensures the reliability and tamper-proof storage of data with IPFS. Furthermore, our proposed model selects a reliable and efficient consensus algorithm through the access control mechanism. Beside this, our proposed model efficiently handles fault detection through blockchain-based mechanisms that ensure the integrity of participating nodes. The overview of blockchain transactions on ethereum platform is shown in Fig. 3 and smart contracts deployment in Fig. 4.



Txn Hash	Method	Block	Age	From	To	Value	Txn Fee
0x38523d6a17a09379...	Give Permiss...	9037308	2 hrs 43 mins ago	0x4F12c5...45268904	0x6B1879...93D59847	0 ETH	0.00005543
0xd6d09c9ca2a9e93...	Give Permiss...	9037374	2 hrs 49 mins ago	0x4F12c5...45268904	0x6B1879...93D59847	0 ETH	0.00005456
0x1475966a0ed93653...	Give Permiss...	9037304	3 hrs 7 mins ago	0x4F12c5...45268904	0x6B1879...93D59847	0 ETH	0.00004982
0x1513b7d7d73925...	Give Permiss...	9037295	3 hrs 9 mins ago	0x4F12c5...45268904	0x6B1879...93D59847	0 ETH	0.00005455
0x69dc767962da706e...	Give Permiss...	9037289	3 hrs 11 mins ago	0x4F12c5...45268904	0x6B1879...93D59847	0 ETH	0.00005334
0xce3488d49b1bfab38...	Give Permiss...	9037277	3 hrs 14 mins ago	0x4F12c5...45268904	0x6B1879...93D59847	0 ETH	0.00005954
0xb5e7845602e48c91...	Give Permiss...	9037261	3 hrs 18 mins ago	0x4F12c5...45268904	0x6B1879...93D59847	0 ETH	0.00005331

Figure 3: Overview of blockchain transactions on ethereum platform

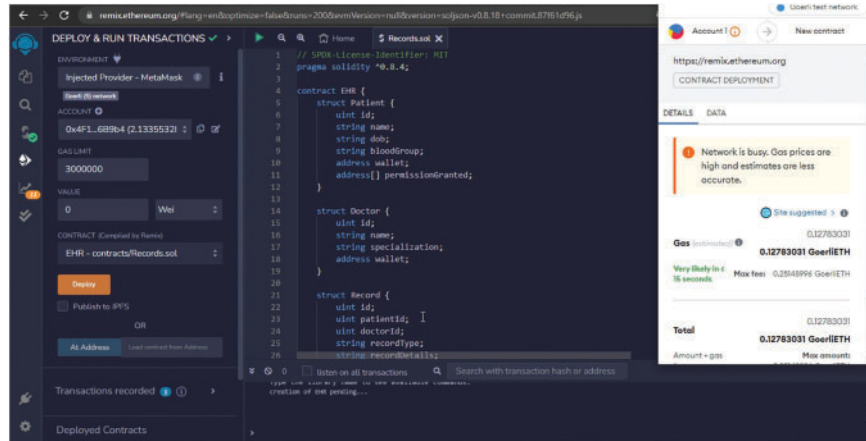


Figure 4: Smart contracts deployment

4.2 Application and Service Layer

In this layer, an application is provided to patients, researchers, and other medical stakeholders, allowing them to access the data of the EHR system [31]. The HTTP server is used in this layer to enable medical stakeholders to interact with the distributed data storage platform IPFS and the blockchain network.

Algorithm 2 outlines a process for smart contract-based authentication integrated with InterPlanetary File System (IPFS) storage. Initially, the blockchain network \mathcal{B} and the smart contract \mathcal{S} are initialized, along with the IPFS network \mathcal{I} , which is responsible for distributed data storage. A set of nodes $\mathcal{N} = \{n_1, n_2, \dots, n_k\}$ participates in the network, where each node n_i is assigned a unique identity ID_i and role R_i . These credentials are stored in the blockchain under the set \mathcal{C} after being verified by the smart contract. The node registration process involves broadcasting each node's identity and role to the smart contract, which then validates and stores these credentials in the blockchain for future authentication. Data storage is handled by high-resource nodes, represented as n_h , which process and send data D to the IPFS network \mathcal{I} . IPFS splits

the data into smaller chunks $\{d_1, d_2, \dots, d_m\}$, each with a size of 256 KB, and distributes these chunks across different devices in the network for decentralized storage. Large healthcare files, such as radiology images or genomic data, are efficiently handled in IPFS through its chunking and parallel distribution capabilities. IPFS automatically splits large files into smaller blocks (typically 256 KB each), which are then distributed across multiple nodes in the network. When a user requests a file, these chunks are fetched concurrently, improving retrieval speed. To maintain security, each chunk is addressed using a cryptographic hash, ensuring that even a single-bit change alters the entire hash reference. Our model also incorporates optional encryption at the chunk level before uploading to IPFS, ensuring that sensitive health data remains confidential even if intercepted during transmission or storage.

When a node, such as n_j , requests access to data stored on the network, it must provide its identity ID_j and role R_j to the smart contract S for verification. The smart contract checks if the credentials are part of the stored set C . If the credentials match, access is granted; otherwise, the request is denied, and the node is flagged as malicious. Data retrieval from the IPFS network is handled by a higher authority node, which requests the chunks from the distributed devices. IPFS aggregates the collected chunks, removes redundancies, and sends the complete data back to the requesting node. The algorithm employs a cryptographic hash function $\mathcal{H}(\cdot)$, digital signatures σ_i to ensure message authenticity, and a timestamp function $\mathcal{T}(\cdot)$ to add temporal validity to the authentication process.

Algorithm 2: Smart contract-based authentication and IPFS storage

- 1: **Initialization:** Deploy blockchain B , smart contract S , and IPFS network \mathcal{I} ; define node set $N = \{n_1, \dots, n_k\}$ with identities ID_i and roles R_i ; maintain on-chain credential ledger C .
 - 2: **Node Registration:** for each $n_i \in N$ do broadcast (ID_i, R_i) to S ; S verifies and records the tuple in C .
 - 3: **Data Storage:** A high-resource node n_h uploads data D to \mathcal{I} ; \mathcal{I} splits D into chunks $\{d_1, \dots, d_m\}$ and distributes them across peers.
 - 4: **Authentication Request:** A node n_j sends its credentials (ID_j, R_j) to S .
 - 5: **Verification:** If $(ID_j, R_j) \in C$ then grant access; otherwise deny and flag n_j as malicious.
 - 6: **Data Retrieval:** An authorized node requests D ; \mathcal{I} locates the chunks, reassembles them, and delivers the data.
 - 7: **Step 1 – Registration:** Each n_i computes $h_i = H(ID_i \| R_i \| T_i)$, signs it with σ_i , and submits $(ID_i, R_i, h_i, \sigma_i)$; S verifies σ_i and stores h_i in C .
 - 8: **Step 2 – IPFS Storage:** n_h uploads D ; \mathcal{I} derives chunks $\{d_j\}$ and distributes them among peers.
 - 9: **Step 3 – Authentication:** n_j computes $h_j = H(ID_j \| R_j \| T_j)$, signs it with σ_j , and submits $(ID_j, R_j, h_j, \sigma_j)$ to S .
 - 10: **Step 4 – Verification:** If $h_j \in C$ and σ_j is valid, S grants access; else it denies access and blacklists n_j .
 - 11: **Step 5 – Retrieval:** An authorized node asks \mathcal{I} for D ; \mathcal{I} gathers $\{d_j\}$, removes duplicates, reassembles D , and returns it.
-

Each node computes a hash of its identity, role, and a timestamp, signs it with its private key to generate a signature, and sends the signed message to the smart contract. The smart contract verifies the authenticity of the signature and the integrity of the hash. If the credentials and signature match a stored record, the node is granted access. Otherwise, access is denied. The smart contracts deployment on IDE and Remix is shown in Figs. 5 and 6. Smart contracts play a central role in our system by automating user authentication, data access control, and file management policies. For instance, the AccessManager smart contract is responsible for verifying digital signatures and granting or denying file access based on user roles and access policies. When a user submits the access request with a digital signature and timestamp, the

smart contract checks the blockchain-stored credentials and evaluates whether the user has the necessary permissions. If verified, it emits an access token that enables temporary retrieval of the file hash from IPFS. This ensures transparent, automatic enforcement of rules without requiring centralized oversight. This two-step process, which combine authentication with secure decentralized storage, ensures both access control and efficient data management in the blockchain-integrated IPFS network. The sample secure user interface of the medcare is shown in Fig. 7. To ensure the availability of health records stored in IPFS, our model employs pinning services and node redundancy. When a healthcare file is uploaded to IPFS, it is broken into smaller chunks and distributed across the network. These chunks are then pinned by designated high-availability nodes to prevent them from being garbage-collected. Additionally, we encourage redundancy by having multiple nodes voluntarily or programmatically replicate the data, ensuring persistence even if one or more nodes go offline. If no one pins the data, IPFS treats it as temporary, and it may be lost during garbage collection cycles. To counter this, our architecture includes a policy-driven smart contract that monitors pinning status and triggers automatic repinning or alerts when replication drops below a defined threshold.

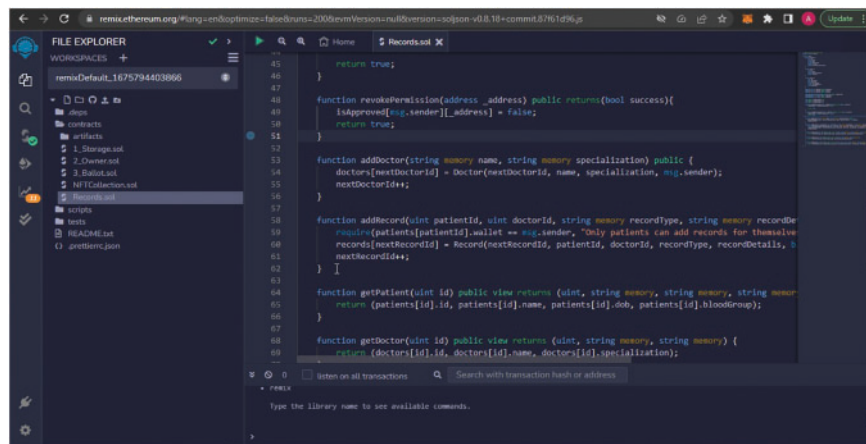


Figure 5: Smart contracts deployment on IDE

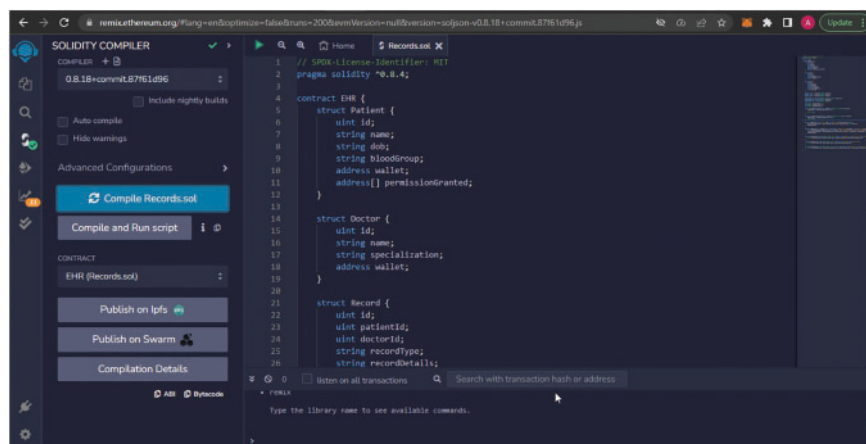


Figure 6: Smart contracts deployed on remix

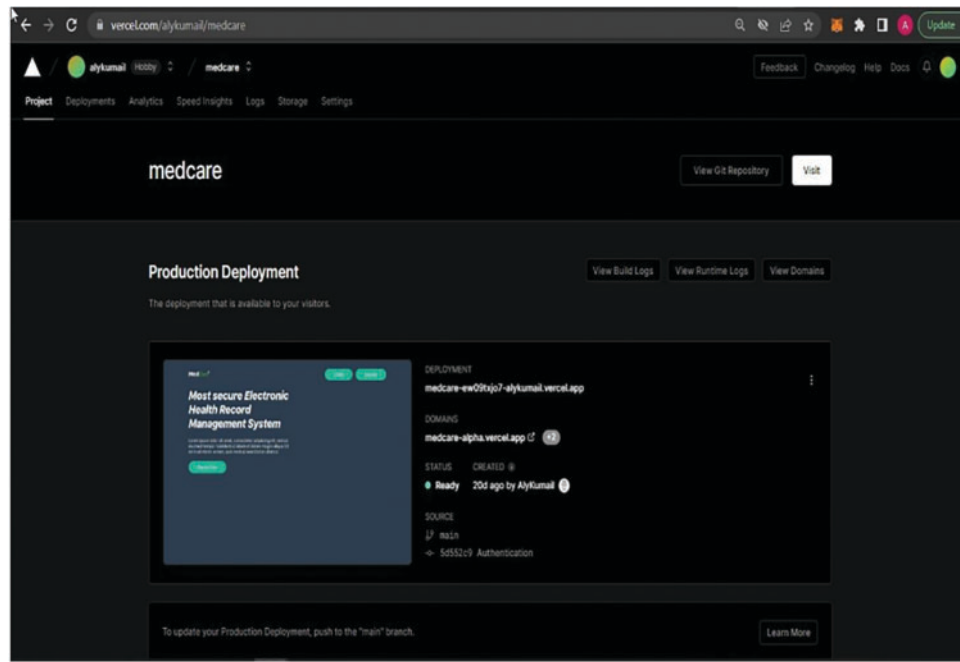


Figure 7: User interface

4.3 Data Provisioning Layer

The service provisioning layer is responsible for ensuring non-repudiation of services within the service provisioning mechanism, while simultaneously achieving high data security, which is not achievable with a conventional blockchain-based mechanism. Furthermore, the traditional blockchain-based healthcare mechanism is unable to store large amounts of data. On the other hand, the small amount of data that is stored on the blockchain network is very costly, as storing 1 MB of data on the blockchain costs around 14,000 US dollars. To solve this issue, we utilize the capabilities of IPFS, which is a distributed file storage system. First of all, when any data is processed by a high-resource node then it is sent to the IPFS for storage purposes. Initially, IPFS divides this data into small chunks of equal size, which is 256 KB. After dividing the entire data, each chunk of data is further sent to the distributed devices. In this way, the data is stored in different devices in a distributed way, described in Algorithm 2. When any node requests data, it is initially authenticated by matching its credentials with the data stored on the blockchain. If this node is legal then the higher node requests the data from IPFS then IPFS collects the data from each distributed device on its side. After collecting all the data, IPFS aggregated this data and removed all redundancies and duplicate values from it. Lastly, this data is sent to the higher authority node. In this way, IPFS not only solves the issue of a single point of data storage failure but also addresses the issue of costly storage of blockchain networks. In our proposed model, we implement redundancy strategies to address the critical importance of data availability and durability in healthcare systems. We replicate data chunks stored on IPFS across multiple nodes and perform periodic backups to cloud-based storage, providing additional fail-safe mechanisms. This hybrid approach ensures that data remains accessible even if individual IPFS nodes are compromised or go offline. Data stored on IPFS is replicated across multiple nodes, and periodic snapshots are archived to centralized cloud storage for added resilience. Therefore, the data availability is ensured in our model, even in the event of node failures. The consistency of data is ensured through our blockchain's consensus algorithm, which guarantees that all nodes have access to the latest authenticated data without discrepancies.

Furthermore, the record of other stakeholders in the network is stored on the client layer. When any node performs any malicious activity then it is immediately removed from the network and its record, along with its malicious activity, is updated on the client layer [32]. Furthermore, in our model shown in Fig. 8, the access layer is responsible for providing a gateway that enables clients and other stakeholders to access the data. Another important layer of our model is the application layer, which is responsible for providing the interface for authentication and transactions of blockchain [33]. Lastly, we utilize Node.js for verifying all transactions and adding blocks to the blockchain. The MongoDB database is used for storing profiles of users and hash values of data stored on the IPFS platform [34].

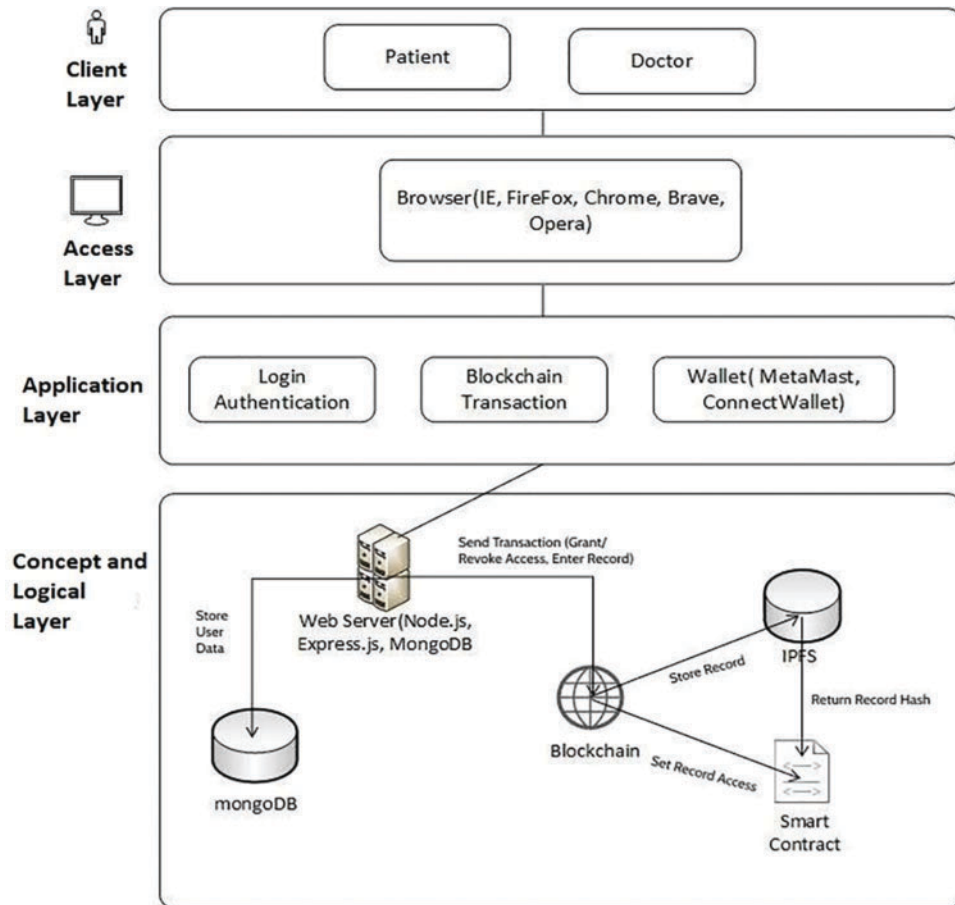


Figure 8: Proposed system architecture

5 Results and Analysis

In this section, we provide details about the implementation and performance evaluation of our proposed model. In our proposed model, we include real-world healthcare workloads and security scenarios for evaluation of our proposed model. We simulate large-scale hospital networks to test the system's performance under high transaction loads. Security evaluations consider scenarios such as malicious node behavior, data tampering attempts, and coordinated network attacks. By benchmarking the system against real-world requirements, such as handling EHRs for thousands of patients, we demonstrate the robustness and practicality of the proposed solution. First of all, the Ganache setup is installed in our system. This setup provides us the capabilities to trade with the Ethereum network as it provides us with some virtual accounts

with Ethereum balance, as shown in Fig. 9. Every account is held by a specific entity, and this entity uses this account to perform any transaction in the blockchain network. After that, the smart contract is deployed on the Ganache network. All the rules about the business of our healthcare sector are stored in the smart contract and Ganache provides us a platform to perform the transaction according to the business rules, written in the smart contract, as shown in Fig. 10.

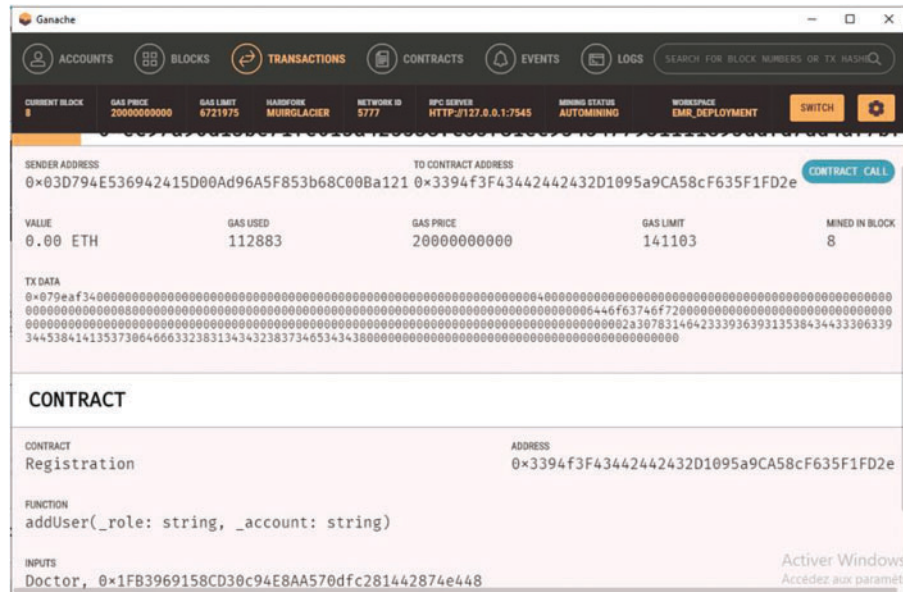


Figure 9: Ganache blockchain setup

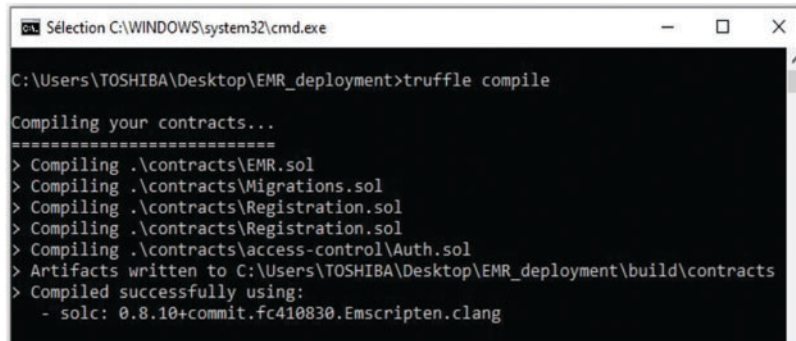


Figure 10: Smart contract

Fig. 11 shows the time that is spent to upload the EHRs on the blockchain network for our proposed model as well as benchmark schemes. In the proposed model the exchange of EHR data is divided into two parts, which are the uploading of data on the blockchain network and IPFS and the retrieval of data from the network. Different types of data are used for uploading and downloading purposes, such as images, text, and videos, which ultimately ensure that the proposed model can handle various types of EHR data. The figure shows the time that is used to encrypt the data and upload it on the network. It can be easily observed from the network that our proposed model outperforms both chain-based systems and the Ethereum network, which utilizes an IPFS distributed file storage system. Furthermore, the figure shows that the time required

for uploading the data keeps on increasing with the increasing amount of data. The processing time for uploading data that is lower than 100 MB is comparatively small as compared to the data having a size larger than 100 MB, as shown in Table 3. The simulation results indicate that the average time required to store data is approximately 2.9 s, demonstrating the effectiveness of our proposed model in uploading EHR data to the IPFS network.

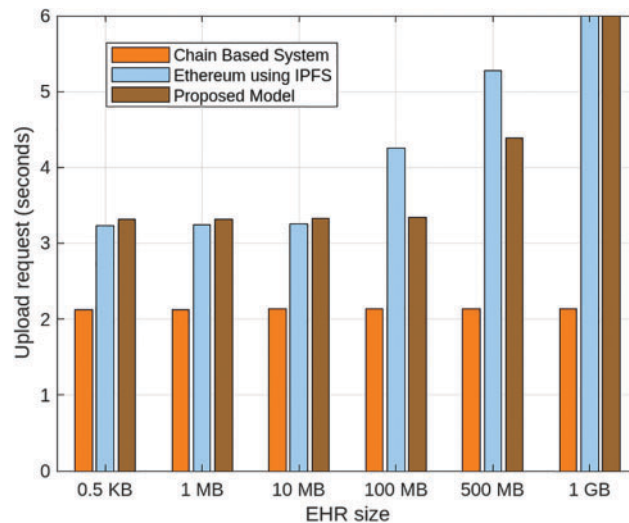


Figure 11: The upload time of EHRs

Table 3: Upload request times for different EHR sizes

EHR size	Chain based system (seconds)	Ethereum using IPFS (seconds)	Proposed model (seconds)
0.5 KB	2.0	3.0	3.0
1 MB	2.0	3.0	3.0
10 MB	2.0	3.0	3.0
100 MB	2.0	4.5	4.0
500 MB	2.0	5.5	5.0
1 GB	2.0	6.0	6.0

Furthermore, Figs. 12 and 13 show the time taken after requesting the network. The results show that the amount of time uploading the data on the IPFS network is affected by the time required for making the query. It can be easily observed from both figures that the average amount of time required for uploading 1 GB of EHR data on IPFS after the request is around 5.2 s which is smaller as compared to a based network, which has an average uploading time of 6.3 s for uploading 1 GB of EHRs data on the network. The upload time of different EHR sizes is shown in Table 4. The reason is that the Ethereum network has a drawback in the Ethereum-based network the patients need to broadcast their secret decryption key in the network, which ultimately results in compromising the privacy of patients. On the other hand, they need to decode data by themselves, which is also very time-consuming. To address this issue, our proposed model incorporates a re-encryption mechanism that eliminates the need for patients to share their private keys. As a result, they can easily decrypt their records without requiring the intervention of any third party, thereby enhancing network security. The security of the proposed mechanism is due to cryptographic hash functions, smart contracts, and digital signatures, ensuring data integrity and authentication.

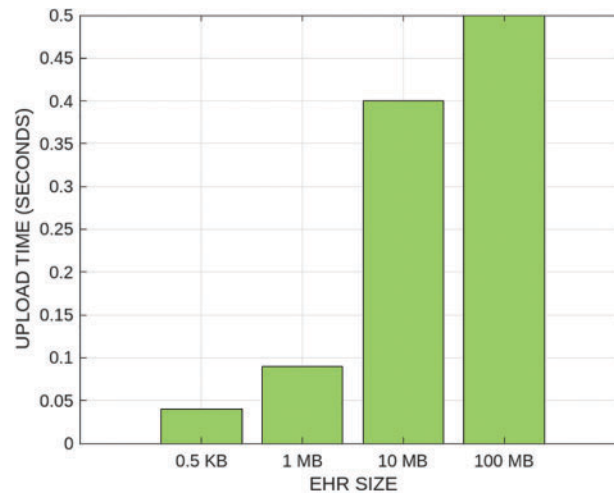


Figure 12: IPFS upload request for smaller amount of data

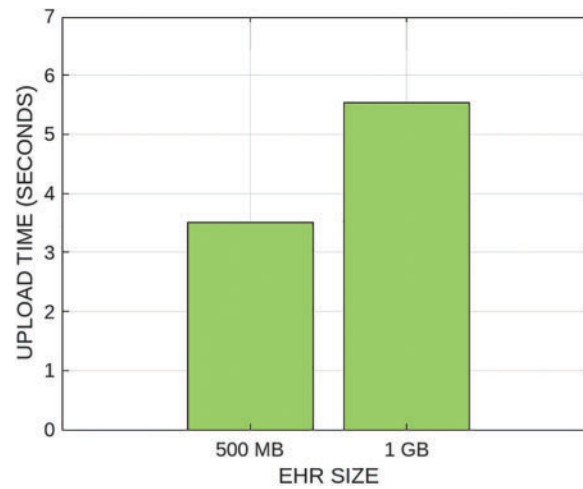


Figure 13: IPFS upload request for larger amount of data

Table 4: Upload times for different EHR sizes

EHR size	Upload time (seconds)
0.5 KB	0.05
1 MB	0.1
10 MB	0.35
100 MB	0.45

Furthermore, our proposed model can reduce network latency by resolving the issue of data redundancies in the network. Furthermore, our proposed model performs the redundancy and duplicate value removal task on the IPFS side, which reduces the workload on individual resource-constrained nodes and is ultimately helpful in the efficient and faster transfer of EHR data. Due to enhanced performance and faster processing time, our proposed model can efficiently handle a large amount of healthcare.

Figs. 14 and 15 download time for the EHR data for our proposed framework as well as for the Ethereum IPFS network. The different sizes of data are considered for evaluating the performance of both models. The results show that our proposed model is more efficient compared to the other schemes in terms of delivering data quickly, which ultimately demonstrates that our model is more scalable. The average time for downloading 1 MB of data from the network is around 0.02 s. The reason is that IPFS collects the data from different distributed devices and simultaneously removes the redundancies from the network. On the other hand, the average time for downloading 1 MB of data from the network for chain chain-based network is around 0.056 s, which is around 6 times higher than the former.

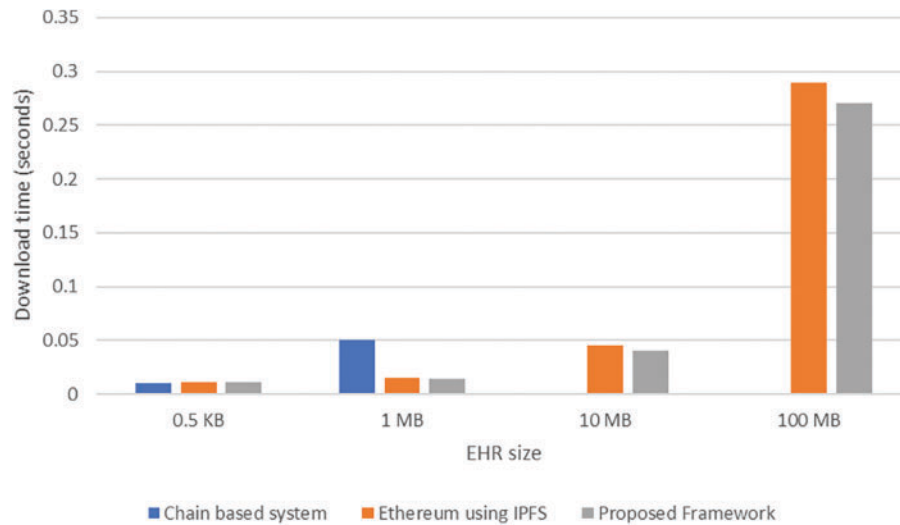


Figure 14: EHR data downloading time

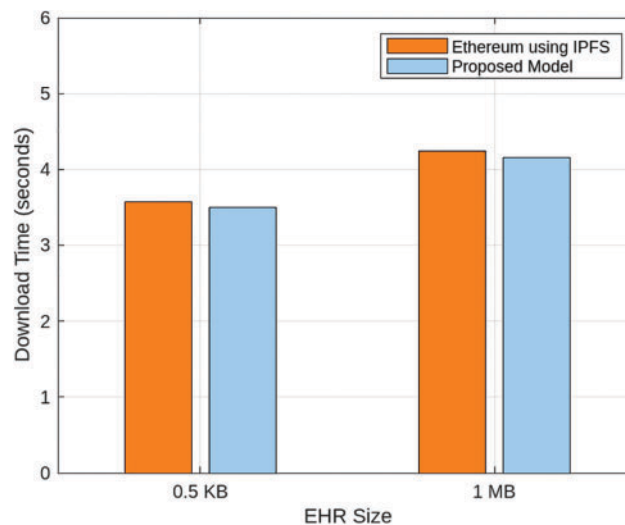


Figure 15: IPFS upload request for larger amount of data

Fig. 16 shows the execution time for the smart contract, which stores all the business rules related to data transfer. The figure illustrates the performance for approximately 9000 transactions, involving critical steps such as registration, authentication, data encryption, decryption, and transaction validation. The smart contract takes about 3.5 s to authenticate a node. The results show that the proposed model performs better than the benchmark scheme and executes around 9000 transactions in just 6.5 s, as shown in Table 5. On the other hand, the benchmark scheme takes approximately 7 s for the same number of transactions, indicating that our model has a better execution time. Due to which, our model is suitable for large-scale healthcare networks, where the number of requests and transactions are very high.

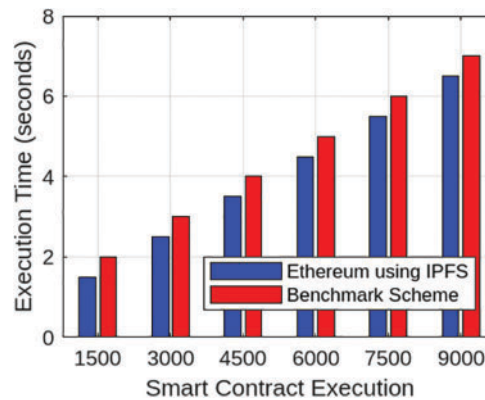


Figure 16: IPFS upload request for large amount of data

Table 5: Execution time comparison between ethereum using IPFS and benchmark scheme

Smart contract	Ethereum using IPFS	Benchmark scheme
1500	1.5	2
3000	2.5	3
4500	3.5	4
6000	4.5	5
7500	5.5	6
9000	6.5	7

Fig. 17 presents a comparative performance analysis of the proposed hybrid Blockchain+IPFS model against single-method systems, centralized cloud storage, IPFS-only, and traditional blockchain in terms of storage cost and data retrieval time. The hybrid model demonstrates superior efficiency by leveraging the immutability and verifiability of blockchain along with the lightweight, distributed nature of IPFS. Specifically, the hybrid model maintains a low storage cost of 0.05 USD per GB on par with IPFS-only systems and significantly lower than centralized cloud storage (0.15 USD per GB) and traditional blockchain (0.30 USD per GB). In terms of retrieval time, the hybrid approach achieves 0.8 s, which is faster than centralized storage (1.2 s) and substantially better than blockchain-only storage (3.5 s). This is made possible through IPFS's content-based addressing mechanism, which enables fast access by locating files via their unique cryptographic hash values. Meanwhile, the blockchain component ensures access control and auditability without burdening the storage system. Centralized models suffer from server load and geographic latency, while blockchain-only models are hindered by on-chain data size limitations. Thus, our

integrated Blockchain+IPFS solution offers a balanced and optimized performance profile, outperforming single-method approaches in both cost efficiency and responsiveness.

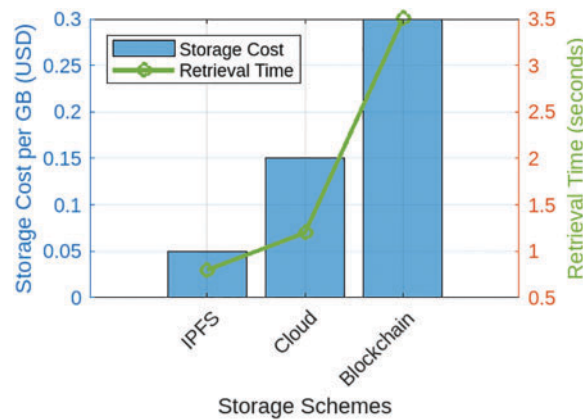


Figure 17: Comparative storage cost and retrieval time

Compared to existing healthcare blockchain systems such as MedRec and FHIRChain, our proposed model offers enhanced decentralization and data persistence using IPFS. MedRec, for instance, relies on Ethereum for data referencing but stores data off-chain in traditional databases, which introduces central points of failure. FHIRChain improves interoperability but lacks robust distributed storage mechanisms. In contrast, our model ensures that both authentication and file storage are distributed and tamper-proof, leveraging the blockchain for immutable user management and IPFS for scalable, content-addressed storage. This integration yields a more fault-tolerant, privacy-preserving, and verifiable system, better suited for modern healthcare data requirements.

Fig. 18 shows the comparison of scalability and fault tolerance between IPFS and a traditional blockchain mechanism. The results show that IPFS outperforms the traditional blockchain mechanism in both metrics. IPFS can handle 10,000 nodes, compared to the traditional blockchain mechanism, which handles 5000 nodes. This shows that the IPFS architecture not only provides effective and reliable storage but also minimizes performance bottlenecks due to centralization. Furthermore, IPFS enhances resource allocation and load balancing, allowing for seamless scalability as demand grows.

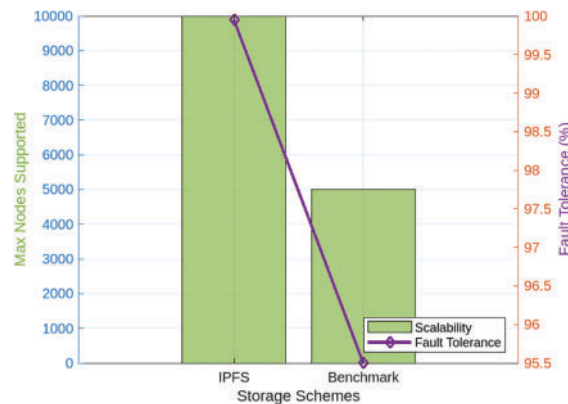


Figure 18: Comparison of scalability and fault tolerance

Fig. 19 shows the comparison of encrypted transaction latency between our proposed model, which employs the Keccak-256 hashing algorithm, and benchmark schemes that use the SHA-256 algorithm. The figure highlights a linear increase in latency for both algorithms as the number of transactions and EHR sizes increase, reflecting the expected computational overhead. However, Keccak-256 consistently demonstrates superior performance with lower latency across all transaction volumes. For instance, at 10,500 transactions, Keccak-256 and SHA-256 record latencies of 205,000 and 225,000 ms, respectively—indicating an approximate 9% reduction in latency. This efficiency is attributed to the sponge construction of Keccak-256, which performs hashing more quickly than the Merkle tree-based approach used in SHA-256. Additionally, we evaluated the system's transaction throughput under increasing EHR sizes and observed that Keccak-256 maintained stable throughput, while SHA-256 exhibited degradation in processing speed due to higher computation time per block. This analysis confirms that our model is both scalable and efficient, capable of handling larger EHR sizes and higher transaction loads while ensuring faster processing—an essential requirement for real-time and reliable healthcare systems.

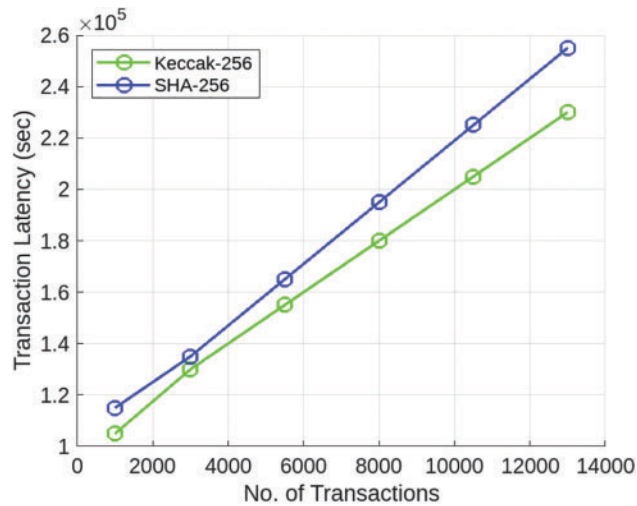


Figure 19: Comparison of transaction latency for increasing transactions

6 Security Analysis

In our proposed model, system security is reinforced through a comprehensive threat analysis that forms the foundation of the overall architecture. The authentication mechanism is rigorously analyzed under the Universal Composability (UC) framework, a formal cryptographic model that ensures the secure composition of protocols. This analysis confirms that our system is resilient to impersonation attacks, where malicious actors attempt to forge identities, and replay attacks, where adversaries reuse captured data to gain unauthorized access. Furthermore, the smart contracts central to enforcing authentication and access control policies on the blockchain are examined using Mythril, a symbolic analysis tool designed to detect vulnerabilities such as reentrancy, unchecked input, and integer overflows. This automated analysis ensures that the contract logic is robust, predictable, and secure from common exploits. For off-chain data storage, the system leverages the IPFS, which ensures content integrity and persistence through content-addressed storage and data replication across multiple distributed nodes. These mechanisms enhance data availability, fault tolerance, and protection against single points of failure. Our threat model considers a variety of attack vectors, including Sybil attacks, poisoning attacks, and man-in-the-middle attacks. These threats are mitigated using layered security measures such as cryptographic authentication, access control policies, and

consensus-based verification. Each defense mechanism is carefully mapped to specific threats in accordance with the taxonomy proposed by Shahidinejad et al. [35], thereby ensuring that the system maintains integrity, availability, and trustworthiness in a decentralized and adversarial environment.

Furthermore, our system defends against threats such as fake users and unauthorized access through a combination of blockchain-based identity verification, smart contract enforcement, and multi-factor cryptographic authentication. Every user must register through a secure process that involves hashing their credentials and signing them with their private key. These credentials are then verified and stored on-chain, making them tamper-proof and traceable. When a user attempts to access a resource, the system validates their identity and role via the smart contract. Unauthorized access attempts are automatically flagged, and the involved identities are blacklisted. Moreover, replay attacks are mitigated using timestamped authentication requests, and Sybil attacks are prevented through consensus-driven verification and resource commitment mechanisms.

7 Discussion

Our proposed model is able to efficiently ensure user authentication and secure and cost-effective data storage. However, IPFS is vulnerable to data loss if specific distributed nodes fail or are compromised. Additionally, the energy consumption of smart contract executions is not efficiently managed as increasing size and complexity of the network. It is crucial to address these limitations for the efficient and reliable application of the proposed model in real-world settings. Energy efficiency is a critical factor for the scalability of blockchain and IPFS systems in healthcare. Accurate power derivation methods should be used in the proposed model to analyze the energy consumption of smart contracts and data storage operations. These methods enable precise measurement of energy usage, which ultimately identifies inefficiencies and guiding optimizations. Lastly various consensus algorithms such as proof-of-stake, can be used to reduce energy consumption while simultaneously maintaining the performance of the system.

8 Conclusion

In this paper, a blockchain-based authentication mechanism is proposed to solve the issue of unauthorized access in the healthcare sector. All the healthcare stakeholders are authenticated based on the credentials they provided during their network registration. Furthermore, we utilize the capabilities of IPFS to store the EHR in a distributed way. This IPFS platform addresses not only the issue of high data storage costs on blockchain but also the issue of a single point of failure in the traditional centralized data storage model. The simulation results demonstrate that our model outperforms all benchmark schemes and provides an efficient mechanism for handling the operations of the healthcare sector. The results show that the average time required to store data is around 2.9 s, indicating the effectiveness of our proposed model in uploading EHR data on the IPFS network. The proposed model is efficiently able to solve the issues of centralized failure, high blockchain storage, and unauthorized access. However, it uses IPFS, which faces the issue of data loss because data is stored on isolated devices. If any distributed node of IPFS is attacked and data is lost then there is no mechanism to recover the data. In the future, we will integrate PQC (Post-Quantum Cryptography) techniques, such as lattice-based cryptography and schemes like Raccoon, to ensure quantum resilience. We will combine IPFS with cloud or fog-based storage systems to improve scalability and fault tolerance. Additionally, federated learning models will be utilized for real-time detection of malicious nodes and prediction of anomalies in dynamic healthcare networks.

Acknowledgement: The authors extend their appreciation to Ongoing Research Funding program (ORF-2025-636), King Saud University, Riyadh, Saudi Arabia.

Funding Statement: This study was supported by the Ongoing Research Funding program (ORF-2025-636), King Saud University, Riyadh, Saudi Arabia.

Author Contributions: Maazen Alsabaan: Writing—review & editing, Visualization, Validation, Supervision. Jasmin Praful Bharadiya: Writing—review & editing, Writing—original draft, Visualization, Validation, Supervision, Methodology, Investigation, Formal analysis, Data curation, Conceptualization. Vishwanath Eswarakrishnan: Writing—review & editing, Visualization, Validation, Formal analysis. Adnan Mustafa Cheema: Writing—review & editing, Visualization, Validation, Supervision. Zaid Bin Faheem: Writing—review & editing, Visualization, Validation, Data curation, Conceptualization. Jihad Ali: Writing—review & editing, Visualization, Validation, Supervision. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: No datasets were generated in this research.

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest to report regarding the present study.

References

1. Le HH, Yamada T, Honda Y, Sakamoto T, Matsuo R, Yamazaki T, et al. Methods for analyzing medical-order sequence variants in sequential pattern mining for electronic medical record systems. *ACM Trans Comput Healthcare*. 2023;4(1):1–28. doi:10.1145/3561825.
2. Taramasco C, Rivera D, Guerrero C, Márquez G. Design of an electronic health record for treating and monitoring oncology patients in Chile. *IEEE Access*. 2023;11:119254–69. doi:10.1109/ACCESS.2023.3327058.
3. Zhou A, Piramuthu S. Smart IoMT applications in senior healthcare: balancing functionality, security, and privacy challenges. In: 2024 Ninth International Conference On Mobile And Secure Services (MobiSecServ); 2024; Miami Beach, FL, USA. p. 1–11. doi:10.1109/MobiSecServ63327.2024.10760186.
4. Gupta NS, Kumar P. Perspective of artificial intelligence in healthcare data management: a journey towards precision medicine. *Comput Biol Med*. 2023;162(1988):107051. doi:10.1016/j.compbimed.2023.107051.
5. Zhang WH, Qamar F, Abdali T-AN, Hassan R, Jafri STA, Nguyen QN. Blockchain technology: security issues, healthcare applications, challenges and future trends. *Electronics*. 2023;12(3):546. doi:10.3390/electronics12030546.
6. Ghosh PK, Chakraborty A, Hasan M, Rashid K, Siddique AH. Blockchain application in healthcare systems: a review. *Systems*. 2023;11(1):38. doi:10.3390/systems11010038.
7. Andrew J, Isravel DP, Sagayam KM, Bhushan B, Sei Y, Eunice J. Blockchain for healthcare systems: architecture, security challenges, trends and future directions. *J Netw Comput Appl*. 2023;215(21):103633. doi:10.1016/j.jnca.2023.103633.
8. Irimia C-I, Iftene A. Decentralized infrastructure for digital notarizing, signing and sharing documents securely using microservices and blockchain. *IEEE Access*. 2024;12:195816–29. doi:10.1109/ACCESS.2024.3518977.
9. Datta S, Namasudra S. Blockchain-based smart contract model for securing healthcare transactions by using consumer electronics and mobile edge computing. *IEEE Trans Consum Electron*. 2024;70(1):4026–36. doi:10.1109/TCE.2024.3357115.
10. Dulce ER, García-Alonso J, Moguel E, Alegría JAH. Blockchain for healthcare management systems: a survey on interoperability and security. *IEEE Access*. 2023;11(2):5629–52. doi:10.1109/ACCESS.2023.3236505.
11. Ahmed I, Chehri A, Jeon G. Artificial intelligence and blockchain enabled smart healthcare system for monitoring and detection of COVID-19 in biomedical images. *ACM Trans Comput Biol Bioinformatics*. 2023;21(4):814–22. doi:10.1109/TCBB.2023.3294333.
12. Kang J, Wen J, Ye D, Lai B, Wu T, Xiong Z, et al. Blockchain-empowered federated learning for healthcare metaverses: user-centric incentive mechanism with optimal data freshness. *IEEE Trans Cogn Commun Netw*. 2023;10(1):348–62. doi:10.1109/TCCN.2023.3316643.

13. Kim TH, Goyat R, Rai MK, Kumar G, Buchanan WJ, Saha R, et al. A novel trust evaluation process for secure localization using a decentralized blockchain in wireless sensor networks. *IEEE Access*. 2019;7:184133–44. doi:10.1109/ACCESS.2019.2960609.
14. Haseeb K, Islam N, Almogren A, Din IU. Intrusion prevention framework for secure routing in WSN-based mobile Internet of Things. *IEEE Access*. 2019;7:185496–505. doi:10.1109/ACCESS.2019.2960633.
15. Cui Z, Xue F, Zhang S, Cai X, Cao Y, Zhang W, et al. A hybrid blockchain-based identity authentication scheme for multi-WSN. *IEEE Trans Serv Comput*. 2020;13(2):241–51. doi:10.1109/TSC.2020.2964537.
16. Moinet A, Darties B, Baril JL. Blockchain based trust and authentication for decentralized sensor networks. *arXiv:1706.01730*. 2017. doi:10.48550/arXiv.1706.01730.
17. Yang J, He S, Xu Y, Chen L, Ren J. A trusted routing scheme using blockchain and reinforcement learning for wireless sensor networks. *Sensors*. 2019;19(4):970. doi:10.3390/s19040970.
18. She W, Liu Q, Tian Z, Chen J-S, Wang B, Liu W. Blockchain trust model for malicious node detection in wireless sensor networks. *IEEE Access*. 2019;7:38947–56. doi:10.1109/ACCESS.2019.2902811.
19. Ramezan G, Leung C. A blockchain-based contractual routing protocol for the internet of things using smart contracts. *Wirel Commun Mob Comput*. 2018;2018:4029591. doi:10.1155/2018/4029591.
20. Uddin MA, Stranieri A, Gondal I, Balasurbramanian V. A lightweight blockchain based framework for underwater IoT. *Electronics*. 2019;8(12):1552. doi:10.3390/electronics8121552.
21. Hong S. P2P networking based internet of things (IoT) sensor node authentication by Blockchain. *Peer-to-Peer Netw Appl*. 2020;13(2):579–89. doi:10.1007/s12083-019-00739-x.
22. Mohammed MA, Lakhan A, Zebari DA, Ghani MK, Abd Marhoon HA, Abdulkareem KH, et al. Securing healthcare data in industrial cyber-physical systems using combining deep learning and blockchain technology. *Eng Appl Artif Intell*. 2024;129(6):107612. doi:10.1016/j.engappai.2023.107612.
23. Shahidinejad A, Abawajy J. Decentralized lattice-based device-to-device authentication for the edge-enabled IoT. *IEEE Syst J*. 2023;17(4):6623–33. doi:10.1109/JSYST.2023.3319280.
24. Sivaprakash P, Charaam RMD, Ithayan JV, Sankar M, Chithambaramani R, Marichamy D. IPFS-based blockchain enabled system for secure data storage and access in healthcare. In: *2024 Second International Conference on Intelligent Cyber Physical Systems and Internet of Things (ICoICI)*. Coimbatore, India: IEEE; 2024. p. 203–8. doi:10.1109/ICoICI62503.2024.10696438.
25. Shankar G, Singh P, Dewangan NK, Chandrakar P. DEMRISEC: security enhancement of patient data in decentralized medical records with IPFS. *Multimed Tools Appl*. 2025;84(13):12123–40. doi:10.1007/s11042-024-19444-w.
26. Jiang BH, Li CY, Tang Y, Xin XJ. Secure cross-chain transactions for medical data sharing in blockchain-based Internet of Medical Things. *Int J Netw Manag*. 2025;35(1):e2279. doi:10.1002/nem.2279.
27. Li CY, Jiang BH, Dong MX, Chen YL, Zhang ZF, Xin XJ, et al. Efficient designated verifier signature for secure cross-chain health data sharing in biomed. *IEEE Internet Things J*. 2024;11(11):19838–51. doi:10.1109/JIOT.2024.3370708.
28. Alowais SA, Alghamdi SS, Alsuhebany N, Alqahtani T, Alshaya AI, Almohareb SN, et al. Revolutionizing healthcare: the role of artificial intelligence in clinical practice. *BMC Med Educ*. 2023;23(1):689. doi:10.1186/s12909-023-04698-z.
29. Almalawi A, Khan AI, Alsolami F, Abushark YB, Alfakeeh AS. Managing security of healthcare data for a modern healthcare system. *Sensors*. 2023;23(7):3612. doi:10.3390/s23073612.
30. Cascella M, Montomoli J, Bellini V, Bignami E. Evaluating the feasibility of ChatGPT in healthcare: an analysis of multiple clinical and research scenarios. *J Med Syst*. 2023;47(1):33. doi:10.1007/s10916-023-01925-4.
31. Chengoden R, Victor N, Huynh-The T, Yenduri G, Jhaveri RH, Alazab M, et al. Metaverse for healthcare: a survey on potential applications, challenges and future directions. *IEEE Access*. 2023;11(1):12765–95. doi:10.1109/ACCESS.2023.3241628.
32. Kuwaiti AAl, Nazer K, Al-Reedy A, Al-Shehri S, Al-Muhanna A, Subbarayalu AV, et al. A review of the role of artificial intelligence in healthcare. *J Pers Med*. 2023;13(6):951. doi:10.3390/jpm13060951.
33. Sezgin E. Artificial intelligence in healthcare: complementing, not replacing, doctors and healthcare providers. *Digit Health*. 2023;9:20552076231186520. doi:10.1177/20552076231186520.

34. Khan B, Fatima H, Qureshi A, Kumar S, Hanan A, Hussain J, et al. Drawbacks of artificial intelligence and their potential solutions in the healthcare sector. *Biomed Mater Devices*. 2023;1(2):731–8. doi:10.1007/s44174-023-00063-2.
35. Shahidinejad A, Abawajy J. An all-inclusive taxonomy and critical review of blockchain-assisted authentication and session key generation protocols for IoT. *ACM Comput Surv*. 2024;56(7):1–38. doi:10.1145/3645087.