Seamless Data Exchange: Advancing Healthcare with Cross-Chain Interoperability in Blockchain for Electronic Health Records

Reval Prabhu Puneeth[1], Govindaswamy Parthasarathy[2]
Assistant Professor, Department of Computer Science and Engineering,
NMAM Institute of Technology - Affiliated to NITTE (Deemed to be University)[1]
Research Scholar, School of Computing and Information Technology, REVA University, Karnataka, India[1]
Professor, School of Computing and Information Technology, REVA University, Karnataka, India[2]

***Abstract*—The rapid digitization of healthcare records has led to the accumulation of vast amounts of sensitive patient data, stored across various systems and platforms. To ensure the secure and efficient exchange of Electronic Health Records (EHRs) among healthcare providers, researchers, and patients themselves, the concept of cross-chain interoperability within blockchain technology emerges as a promising solution. Nevertheless, existing blockchain platforms exhibit several limitations. In order to address the issue of non-interoperability, the suggested method involves creating a connection between two similar blockchain networks. This solution is exemplified through the use of an Electronic Health Records (EHR) structure, which is distributed across distinct Ethereum Testnets and implemented via a Solidity Smart Contract. The paper aims to demonstrate the viability of bridging the gap and fostering seamless interoperability between blockchain networks. However, establishing effective communication between these smart contracts proves to be a complex endeavor, whether within a singular blockchain or spanning multiple blockchains. This complexity presents a formidable obstacle, particularly when diverse hospitals require the sharing or exchange of critical information. Consequently, a solution becomes imperative to facilitate cross-chain communication among smart contracts. This solution provides seamless operation both within the confines of a single blockchain and across disparate blockchains. By achieving this, cross-chain interoperability can be realized, enabling distinct blockchain networks to mutually comprehend and actively engage with each other.**

Keywords*—Electronic health records; data sharing scheme; blockchain technology; solidity smart contract; cross-chain interoperability

I. Introduction

Telecare Medicine Information System (TMIS) takes use of the dramatic improvement in telecommunications and information technologies to deliver healthcare to patients in their homes. TMIS enables doctors to collaborate and share vital information about their patients' conditions, even when they are physically separated by long distances and working from different offices. In this way, TMIS drastically reduces the price of care by making it more accessible to more people. If the most recent state of a patient's health is to be taken into account while making medical decisions, then an effective electronic-health (e-health) system is essential. However, it might be difficult for doctors to effectively diagnose and treat new patients because they lack immediate access to the patient's complete medical history and other relevant data [1]. EHRs contain information about patients, including demographics, lab results, medical scans, clinical notes, billing data, sensor data, medical history, medications, insurance details, and more; in an e-health system, these restrictions may be less of an issue. Ensuring the confidentiality, privacy, and integrity of data within this system is unquestionably crucial. Nevertheless, the specific needs of different e-health systems may vary depending on the privacy laws in place in the country where the system is located [2]. Although there is still work to be done on interoperability and privacy concerns, EHR are now widely recognized as an integral element of the healthcare business.

Many scholars have proposed confidential data-sharing strategies to meet the expanding demands of the healthcare industry. Conventional healthcare data-sharing systems, on the other hand, rely on a centralized system that does not provide a safe method of exchanging data with other medical-related organizations. However, because regulatory bodies may lack access to data held by medical institutions, there is a significant opportunity for improper exploitation of patients' medical information [3]. Consequently, in the event of resource sharing, data-sharing methods cantered around a centralized framework are not appropriate for the advancement of e-medical records.

A. Blockchain Technology

Blockchain stands as an advanced database technique that fosters transparent data exchange across a network. It operates on the principle of organizing data into interconnected "blocks" that form an unbroken "chain." In this analogy, the blocks in the blockchain are akin to nodes in a linked list, collectively constituting the chain [4].

Within each block of the blockchain, you find data and a hash value that establishes its connection to the preceding block. A significant feature of this technology is the inherent inability to modify links or alter the chain without gaining widespread consensus. This ensures that the information remains meticulously arranged in chronological order. As a result, blockchain technology provides an immutable ledger capable of recording a diverse range of transactions.

Blockchain solves problems by generating a decentralized, unchangeable method of recording transactions. Each party in a real estate deal may have their own ledger thanks to blockchain technology. Both parties must agree to a transaction before it is finalized, and the ledgers will be updated simultaneously. If any transaction in the past is changed, the integrity of the entire ledger is compromised [5]. These features of blockchain technology have led to its use in several fields, most notably the creation of digital currencies like Bitcoin.

The privacy concerns associated with the implementation of EHRs as healthcare data increasingly moves into the digital realm. Governments globally have introduced legislation and regulations to protect personal information, yet data breaches within electronic health records continue to rise, with theft and loss being the primary causes. This underscores the critical need for stricter control and limited access to patients' private medical data [6]. The blockchain technology could offer a potential solution. It describes blockchain as a decentralized, distributed ledger system that encrypts and links data in a secure and transparent manner. Consensus algorithms ensure agreement among network nodes regarding legitimate data access, and data is only added to the blockchain after undergoing validation for accuracy and relevance [7].

Blockchain is noted for its advantages, including user autonomy, increased data sharing transparency, and heightened data privacy and security. The importance of decentralization lies in its ability to create a robust and tamper-resistant system where altering data becomes difficult without alerting other nodes in the blockchain network. Encrypting data within each block using cryptographic hashes like the SHA-256 algorithm for enhanced privacy and security. These hashes make it extremely difficult to reverse-engineer the original data from the hash value, thereby protecting the blockchain against tampering by malicious actors. Through a combination of encryption, decentralization, and consensus mechanisms, blockchain offers a promising solution for safeguarding sensitive healthcare data in the increasingly digital healthcare landscape [8].

B. Blockchain Interoperability

Blockchain interoperability is the ability to view, access, and share data across various blockchain networks. It emphasizes the significance of interoperability in making blockchain applications more transparent and efficient. In the healthcare context, the term "interoperability" refers to the exchange of patient data between different electronic health record systems, with challenges arising from hardware and software heterogeneities. The idea of smart contracts, which are programs that execute, predefined operations on a blockchain [9]. However, it points out limitations in the inter-network communication between smart contracts, highlighting the need for solutions to enable cross-chain communication among them [10]. The ultimate goal is to achieve cross-chain interoperability, allowing different blockchains to understand and interact with each other. The importance of addressing non-interoperability issues and suggests building a bridge between similar blockchain networks, using Electronic Health Records (EHR) as an example.

The structure of the upcoming sections in this paper is as outlined below: Section II elaborates on the prior approach to utilizing blockchain-based EHR. In Section III, the techniques proposed for this study are introduced. The advancement of the experiment, which validates the assertions of this research and includes the results, is covered in Section IV. Lastly, Section V provides the experiment's conclusions.

II. Literature Review: Related Studies

Blockchain is a decentralized ledger that records and shares a comprehensive history of transactions and electronic events among its participants. A significant feature is that most participants validate all public transactions, ensuring the permanence and non-disputability of stored information. This addressing the vital need to safeguard and maintain sensitive patient data in a secure cloud-based environment, addressing concerns related to data creation, distribution, storage, and retrieval in the healthcare sector [11].

The solution involves using Blockchain technology to protect cloud-based medical records. By combining distributed computing with blockchain, disparate healthcare providers can establish secure connections, facilitating remote access to patient information while ensuring its confidentiality. Data undergoes encryption before uploading to the cloud, and healthcare providers must decrypt it for access. The use of cryptography during encryption ensures secure data transmission between clients and servers [12].

Personal health records (PHRs) are often stored and processed in centralized client-server architecture in conventional healthcare systems. Due to technological and infrastructure limitations, PHR kept at a healthcare facility remain in repository and cannot be easily shared with other institutions [13]. There is no efficient and confidential data exchange process in place if a patient has to see many doctors or hospitals. Health Insurance Portability and Accountability Act (HIPAA) may safeguard patients' privacy; however this is questionable because it does not take into account whether or not the patient is personally involved.

According to the author [14], studies on the use of blockchain technology to ensure confidentiality and safety in healthcare are commonplace on the distributed ledger. However, they have diverted emphasis from the distribution of the encryption/decryption key needed to ensure PHR confidentiality and instead cantered it on the maintenance of individual health records. In order to construct trustworthy and decentralized systems, blockchain offers a shared, immutable, and visible history of all transactions. This opens the door for the use of blockchain technology in the creation of a safe and reliable PHR data management system. This study introduces an approach that empowers patients by necessitating them to possess the information required to deduce the encryption /decryption key from previous transactions within blockchains. Through this key-based access restriction, patients gain control over their own medical records. If you're looking for a vibrant industry that embraces technology to provide superior care with a focus on the patient, look no further than healthcare.

Artificial intelligence (AI), the Internet of Things (IoT), and blockchain provide a diverse set of uses that may be put to good use in the healthcare industry. Potentially improving monitoring processes and decreasing clinical-related mistakes is one role that healthcare environments may play. To improve healthcare delivery, [15] presents a new architecture that integrates ambient intelligence into the healthcare infrastructure. As the foundation of the network, blockchain ensures the safekeeping and sharing of data among all of its participants. In order to collect data on vital signs, a hardware prototype is created using a Raspberry Pi Model 4B.

The high-performance computing system, integrated with machine learning algorithms and blockchain capabilities, is employed to efficiently store critical patient data and notify healthcare professionals of any discrepancies. Comparative analysis reveals that this new system surpasses existing models in terms of reliability and latency. Metrics like mean average error (MAE), mean square error (MSE), and root mean square error (RMS) are used to comprehensively evaluate algorithm performance. Notably, this system offers the seamless integration of pre-existing models and demonstrates effective functionality overall.

However, the security challenges associated with patient data storage in IT systems have hindered the progress of e-healthcare. The introduction of blockchain technology offers a potential solution, which is explored in the work outlined in reference [16]. This research establishes the foundation for blockchain-based health information management, encompassing a public ledger, private ledger, smart contracts, and context-based access control. The proposed design ensures patient data access, security, and system compatibility, while also presenting an efficient approach to managing complex medical processes. Furthermore, the report delves into the application of blockchain technology in healthcare, emphasizing its potential for confidential patient data exchange for scientific research. Smart contracts are recommended for maintaining patients' medical histories, described as innovative, accessible, interoperable, and auditable.

Prominent healthcare communication networks generate data and information, but recent years have seen these systems become targets for cyberattacks due to inadequate security measures. The ease of conducting such attacks is attributed to the widespread availability of powerful computers and various malicious tools. The article compares several technology types and examines blockchain-based approaches to firmware enhancement, addressing their limitations such as large storage requirements and centralized firmware storage.

Additionally, the study in [17] outlines a general architectural framework for Internet of Healthcare Industry (IoH) applications, incorporating blockchain technology, Local Differential Privacy, and cloud computing (Icedrive). The study highlights the potential uses and challenges in integrating blockchain and cloud computing into IoT applications while also considering the application of blockchain in the future of the healthcare industry. This research is anticipated to facilitate the development of blockchain-based IoT applications.

At present, distinct blockchains within the same network lack the capability to seamlessly interact with each other. For instance, the exchange of data between Ripple and Ethereum remains infeasible. Furthermore, achieving blockchain interoperability entails navigating intricate procedures.

III. Methodology

A patient-centered approach has been put into practice, wherein patients take responsibility for controlling access to their Electronic Health Records (EHRs). The architectural plan is designed around the concept of hospitals using distinct EHR platforms. Both platforms require healthcare participants to register through smart contracts or chain code. The attending physician engages in consultations with the relevant patients and inputs their EHRs into the system. These EHRs are then hashed, and the resulting hash value is used to create a blockchain block, establishing ownership of the EHR. The proposal suggests dividing the EHR into offline and online sections, with the patient's identity characteristics linked to the offline data during online data uploads. Any document-oriented database can be used to store the offline data. Access requests to the electronic health record are routed to the patient for approval when initiated by a system participant. Patients retain control over their Electronic Health Records (EHRs) and can determine who has access to their records and the extent of information shared. A crucial element in our system is the use of hash locks, particularly when connecting to an EHR from an external system. For instance, if a stakeholder from System B requires access to a patient's EHR in System A, a hash lock is created for that specific EHR, as outlined in study [18]. This hash lock grants the stakeholder in System B access to the patient's EHR, facilitating information retrieval. Fig. 1 provides a graphical representation of our architecture, illustrating how blockchain technology can streamline the exchange of electronic health records.

Proposed system has two major components. The system design along with appropriate representation and explanation has been given below:

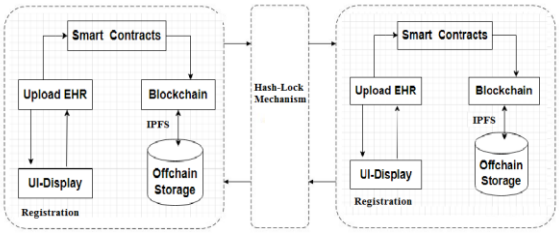

Fig. 1. Electronic health record framework.

A. Smart Contract Structure

Within a specific hospital's smart contract, two distinct user types are present: Doctors and Patients. Users can register themselves via the user interface and receive a private-public key pair to facilitate secure data sharing. Once registered, users can log in using their credentials, granting them access to their respective functionalities, as detailed in study [19]. Doctors have the ability to create records and perform record searches, while Patients can access their own records and share data when required.

The execution of these functions is achieved through a Solidity contract, accessed via a Python script. To ensure data security during storage and retrieval, a secure approach is maintained by utilizing the IPFS protocol. Data is securely stored on IPFS and the resulting hashes are recorded within the Ethereum blockchain for traceability and verification purposes. Fig. 2 illustrates the architecture of an individual smart contract.

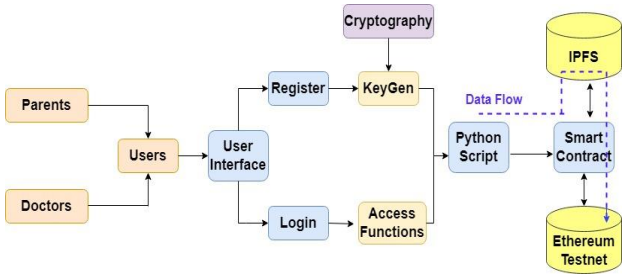

Fig. 2. Architecture flow of individual smart contract.

Certainly, the individual smart contract that operates within the context of a specific hospital for managing user interactions between Doctors and Patients, the individual smart contract streamlines the interactions between healthcare providers (Doctors) and patients, enhancing communication and data sharing. Patients have greater control over their medical records, promoting privacy and data autonomy [20, 21].The integration of IPFS and Ethereum blockchain ensures data security, traceability, and transparency. In essence, the individual smart contract serves as a pivotal component within Hospital X's digital infrastructure, providing a secure, efficient, and transparent means of managing medical records and interactions between healthcare providers and patients. Fig. 3 shows the flow of the user interface.

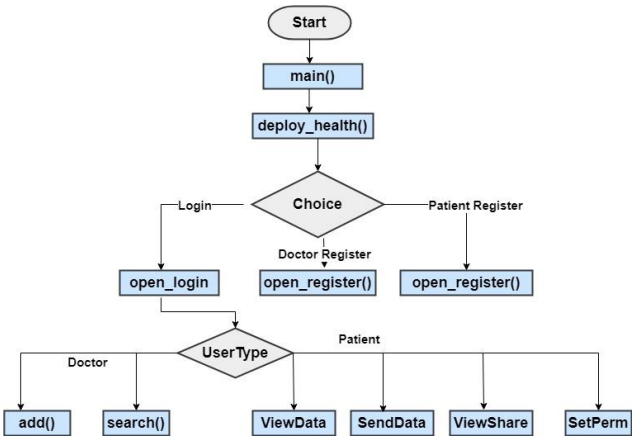

Fig. 3. Flow of the user interface.

B. Cross-Chain Interoperability

When two or more blockchain networks or platforms are able to interact with one another without any hitches in the flow of information or transactions, we say that they are cross-chain interoperable. It addresses the challenge of isolated blockchains that operate independently and cannot directly interact with each other [22, 23]. Achieving cross-chain interoperability is crucial for creating a more connected and efficient blockchain ecosystem.

Different blockchain networks, such as Ethereum, Binance Smart Chain, Polkadot, and others, have their own protocols, consensus mechanisms, and features. Traditional blockchains operate in isolation, and transactions within a specific blockchain are not easily accessible or verifiable by other blockchains. Cross-chain interoperability aims to enable communication, data sharing, and asset transfers across multiple blockchain networks.

C. Interoperability Structure

In Fig. 4, the architecture of the interoperability approach is depicted. It involves an Intermediate Contract that holds the Name, network, and address of each hospital contract. Every hospital must register its details with the intermediate contract. When Hospital A requires access to data from Hospital B, the following steps occur:

- Switch to the Intermediate contract network.
- Retrieve the network and address of Hospital B.
- Switch to the network of Hospital B.
- Retrieve the contents from Hospital B's contract.
- Revert back to the original contract network and return the data.

This process allows for secure and controlled data sharing between different hospital contracts.

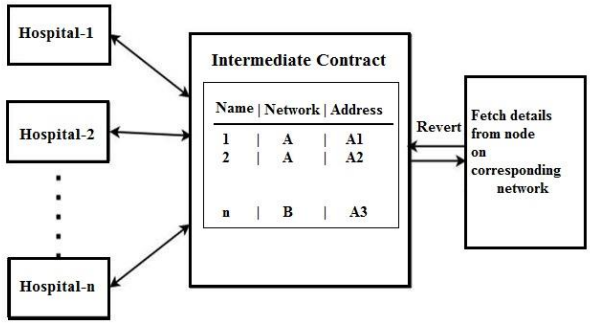

Fig. 4. Architecture of interoperability approach.

D. Approaches to Cross-Chain Interoperability:

Atomic Swaps: These allow users to directly exchange assets between different blockchains without the need for intermediaries. Wrapped Tokens: Tokens on one blockchain are "wrapped" to create a representation on another blockchain, enabling their use in a different ecosystem. Sidechains: Separate blockchains, known as sidechains, are linked to the main blockchain, allowing for specific tasks to be performed on the sidechain while retaining the connection to the main chain. Cross-chain Bridge: Specialized smart contracts act as bridges between different blockchains, facilitating the transfer of assets and data. Polkadot and Cosmos: These platforms are designed with native cross-chain interoperability features, allowing multiple blockchains to be connected within a larger network.

Cross-chain interoperability enables the use of specialized features from different blockchains within a unified ecosystem. Assets can be moved seamlessly between

blockchains, enabling more efficient trading and utilization. Interoperability can help alleviate congestion on a single blockchain network by distributing transactions across multiple chains. Cross-chain interoperability supports collaboration between different projects and platforms, fostering innovation [24, 25]. Cross-chain interoperability plays a vital role in overcoming the limitations of isolated blockchains and creating a more interconnected and versatile blockchain landscape. As the blockchain ecosystem continues to evolve, solutions for cross-chain communication and data sharing will be crucial for achieving widespread adoption and realizing the full potential of decentralized technologies.

IV. Results and Discussion

The effectiveness of the suggested model is measured in terms of the following indicators. The success of a blockchain network may be measured by the following indicators, which have been developed with consideration for real-world use cases:

A. Transaction Throughput

This indicator tracks how many deals the blockchain can handle in a given time frame. It's a measure of the network's ability to process several transactions at once.

B. Latency

Latency refers to the time taken for a transaction to be confirmed and included in the blockchain. Lower latency signifies quicker transaction validation and responsiveness of the network.

C. CPU Utilization

CPU usage is the rate at which a network's nodes use their central processing units. In our current use-case, each Hospital is associated to one smart contract instance. This smart contract provides various functionalities as required for the user operations. Each of these functions is explained in detail below:

D. Register

This function handles registration of the new users. For every new user created, it generates a key pair i.e., private key and the public key which will be used for data encryption and decryption. This function triggers the Register() in the smart contract which works as follows:

```
Function Register(UserDetails, keys, flag):
  For i = 0 to Number of Users:
    User = ith User
    If k256(User.username) == k256(UserDetails.username):
      Return False  // Username is already in use
  Add UserDetails to UserList
  If flag == 1:
    Add UserDetails to Ddetails  // For doctors
  Else:
    Add UserDetails to Pdetails  // For patients
  Return True  // Registration successful
```

After the execution of the above function, it displays the corresponding success/fail message. Following is a preview of the register window shown in Fig. 5.

Fig. 5. Register window.

E. Login

This function handles the login functionality for the existing users if the credentials provided are valid. It first triggers the Login() in the smart contract which works as follows:

```
Function Login(username, password):
  For i = 0 to Number of Users:
    User = ith User
    If k256(User.username) == k256(username) && User.password == k256(password):
      Return UserType  // Successful login, return user type
    End If,
  End For
    Return FailMessage  // Login failed, return a failure message
```

The login window appears as shown in Fig. 6. If the login is successful, the above function returns the user type as doctor or patient. If the type is doctor then available functionalities will be add and search, and if the type is patient then available functionalities will be View-data, Send-data, view-share and set-permission.

Fig. 6. Login window.

F. Add Record

This function handles the addition of new records. It is executable only if the user type is doctor. The doctor enters the required details in the form provided as shown in Fig. 8. Doctors can also upload files using the provided option. The file is uploaded to the IPFS Server which returns a hash. These details along with the address hash are converted to a JSON record. This record is again hashed using IPFS. Then AddRecord() is triggered in the smart contract which works as follows and UI is shown in the Fig. 7.

```
Function AddRecord(hash, PID):
    Add the record to the Records array
    If PID is present in the Hashlist:
        Add the current index to the corresponding PID in Hashtable
        Set the flag
    If flag is not set:
Push the PID and current index to the Hashtable as a new entry
```

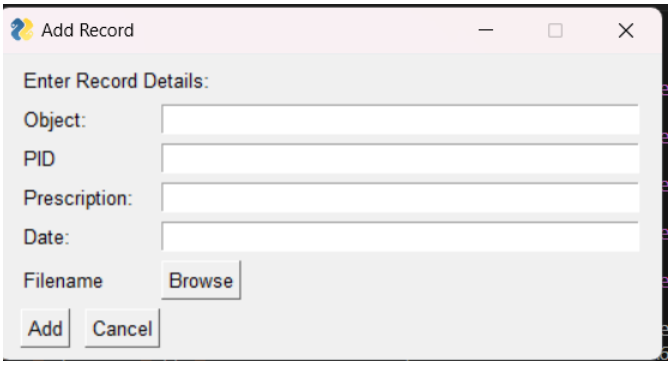

Fig. 7. Add record window.

G. Search Record

This function is used for searching and displaying patient records in tabular form. The search operation can be done based on two parameters, PID or SSN. For internal references, searching is done using PID, whereas, for cross-chain references, searching is done through SSN.

For the purpose of this explanation, let's focus on the internal reference using PID. First, a "Filtered Data" array is created to store the records that match the given pid. Then, the function iterates through a hash table that contains patient records. For each record in the hash table, the function checks if the pid matches the given pid. If there is a match, the function loops through all the indexes associated with the given pid. It pushes all matching records to the Filtered Data array. After all records have been checked, the function returns the Filtered Data array containing all the records that matched the given pid or returns error output as shown in Fig. 8. The pseudo code for SearchRecord() is as follows:

```
Function SearchRecord (PatientRecords, GivenPID):
    Create an empty array called FilteredData
        For each record in PatientRecords:
        If record.PID matches GivenPID:
            For each index associated with GivenPID:
                Add the matching record to FilteredData
        If FilteredData is not empty:
        Return FilteredData
    Else:
        Return ErrorOutput
```

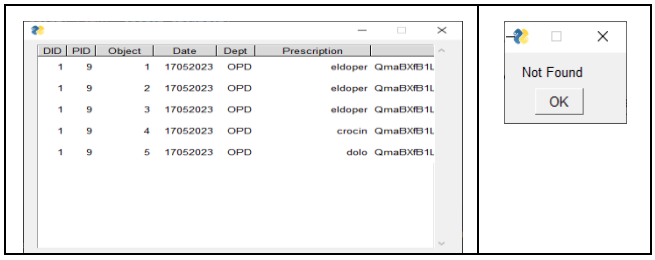

Fig. 8. Output for search record (positive and negative).

H. Interoperability Operations

Certainly, let's elaborate on the provided pseudocode steps and explain the process in detail:

1) Retrieving SSN with getSSN(): The first step involves retrieving the Social Security Number (SSN) associated with the provided Patient ID (pid). This information is obtained by executing the getSSN() function. This function likely queries a smart contract or database to fetch the SSN based on the given patient ID.

2) Switching to intermediate network: After obtaining the SSN, the pseudocode suggests disconnecting from the current network. This indicates a transition from the main network to an intermediate network, which acts as a backup or alternative in case of network downtime or delays.

3) Choosing an intermediate network: Users are presented with the option to choose between two intermediate networks: Sepolia and Goerli. These networks serve as contingency plans, ensuring that even if one network experiences issues, the process can continue using the other network.

4) Connecting to intermediate network: Based on the user's selection, the pseudocode connects to the corresponding intermediate network (Sepolia or Goerli).

5) Accessing intermediate contract: Once connected to the chosen intermediate network, the pseudocode suggests accessing a previously deployed intermediate contract. This contract likely contains functions and logic required for the subsequent steps.

6) Retrieving list of hospitals: Within the intermediate contract, the pseudocode fetches a list of all hospitals using the GetH() function. This list likely contains identifiers or addresses of different hospital contracts.

7) Iterating over hospitals: For each hospital in the retrieved list, the pseudocode enters a loop. This loop iterates through the list of hospitals one by one.

8) Switching to hospital network: Within the loop, the pseudocode disconnects from the current intermediate network and connects to the network associated with the specific hospital's contract. This allows interaction with the smart contract of the hospital.

9) Searching and adding records: With access to the hospital's network, the pseudocode utilizes the SearchRecordSSN() function. This function likely searches for medical records associated with the retrieved SSN and adds any matching records to a temporary storage.

10)Completing hospital search: Once records have been searched and added for the current hospital, the pseudocode disconnects from the hospital's network and reconnects to the intermediate network.

11)Displaying stored records: After searching all hospitals, the pseudocode ends the loop and reconnects to the original network. The medical records that have been temporarily stored during the search process are now displayed to the user for viewing.

12)Visualization: The entire process described above, from SSN retrieval to displaying records, can be visualized using a diagram or flowchart, shown in Fig. 9.

In summary, the pseudocode outlines a process where the SSN of a patient is used to search for and retrieve medical records from multiple hospitals' contracts. It employs intermediate networks and contracts to ensure data availability and accessibility even in the face of network issues. The process involves several steps of switching networks, accessing contracts, and iterating through hospitals to ultimately present the user with the aggregated medical records.

The pseudocode for the logic is given below:

```
Function Interoperable()
Input:
pid = GetUserInput()  // Get the Patient ID from the user.
// Retrieve SSN
SSN = GetSSN(pid)  // Call a function to retrieve SSN based on the PID.
 // Disconnect from the current network
Network.Disconnect()
// Connect to the intermediate network
Network.Connect('intermediate')
// Get a list of hospitals from the intermediate contract
 Hosplist = IntermediateContract.GetHospitalList()
// For each hospital in the Hosplist
For i in Hosplist:
 nw, link = i[1], i[2]  // Get the network name (nw) and contract address (link).
Network.Disconnect()
// Connect to the hospital's network
 Network.Connect(nw)
// Access the hospital's smart contract
 Temp = SmartContract.At(link)
 // Search for patient records using SSN
 Records = Temp.SearchRecordSSN(SSN)
Network.Disconnect()
// Reconnect to the original network
Network.Connect(curNetwork)
```

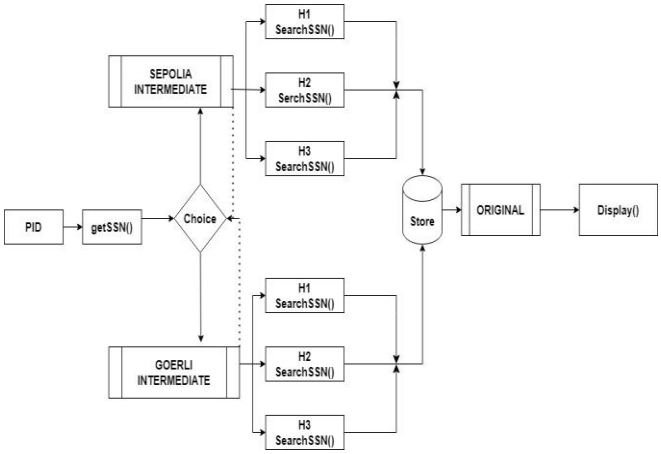

Fig. 9. Interoperability implementation.

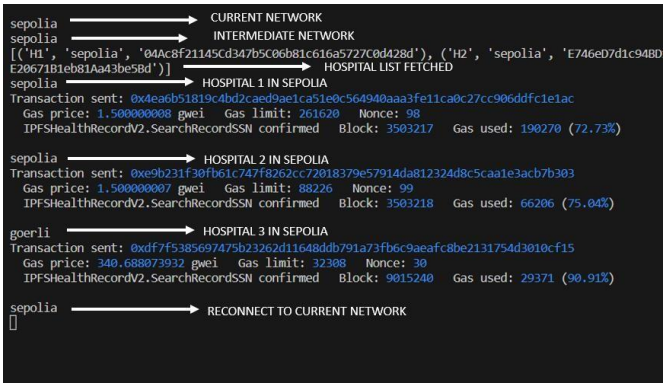

Fig. 10. Transaction flow during cross-chain call.

In the figure given above Fig. 10, shows clearly about the transaction calls that take place. In current scenario the example encompasses three hospital contracts, in Sepolia and Goerli respectively. The intermediate contract is deployed on Sepolia as well. Certainly, here's an elaboration of the cross-chain search operation we have outlined:

Cross-Chain Search Operation Steps:

1) *Initial network setup*

- The network is initially set to Sepolia, representing the primary network for the operation.

2) *Switch to intermediate contract network*

- To ensure a robust and reliable search operation, the process begins by connecting to the intermediate contract network, which is also Sepolia in this case.

3) *Fetching list of hospitals*

- Using the intermediate contract on the Sepolia network, the pseudocode fetches a list of hospitals: H1, H2, and H3. These hospitals represent the targets for the cross-chain search.

4) Searching hospital 1 (sepolia)

- The network connection switches to Hospital 1's network on Sepolia.
- The search transaction, likely involving the SearchRecordSSN() function, is executed for the patient's records associated with the retrieved SSN.
- Once the search transaction is confirmed, the retrieved records from Hospital 1 are temporarily stored.

5) Searching hospital 2 (sepolia)

- The network connection switches to Hospital 2's network on Sepolia.
- The search transaction for the same patient's records is executed within Hospital 2's network.
- After confirmation, the records from Hospital 2 are also temporarily stored.

6) Searching hospital 3 (goerli)

- The network connection switches to Hospital 3's network on Goerli. This represents a change in network from Sepolia to Goerli, emphasizing cross-chain operation.
- The search transaction for the same patient's records is executed within Hospital 3's network on the Goerli chain.
- Once confirmed, the records from Hospital 3 on the Goerli chain are temporarily stored.

7) Aggregating and returning records

- After successfully searching across multiple hospitals and networks, the temporary storage of retrieved records is aggregated.
- The aggregated records are then returned to the user, presenting a comprehensive overview of the patient's medical data from all the participating hospitals and chains.

This cross-chain search operation demonstrates the flexibility and versatility of the proposed model, allowing for seamless interaction with multiple hospital networks on different blockchain platforms (Sepolia and Goerli, in this case). By employing intermediate contracts and network switches, the model ensures data availability and continuity, even if issues arise in individual networks, enabling efficient retrieval and presentation of medical records across various chains.

Fig. 11 and Fig. 12 show the time taken for the operations GetH(), network switching and Searching times. These visual representations clearly indicate that fetching times and switching times are very low compared to the major search transaction.

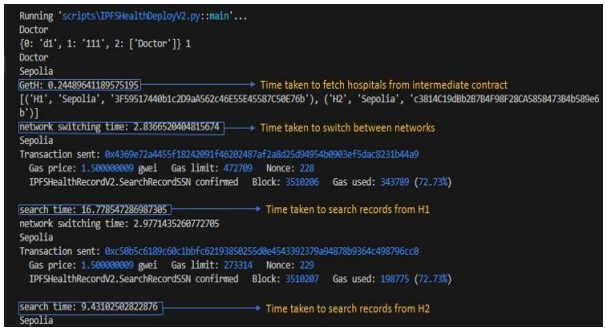

Fig. 11. Transaction logs with time measures.

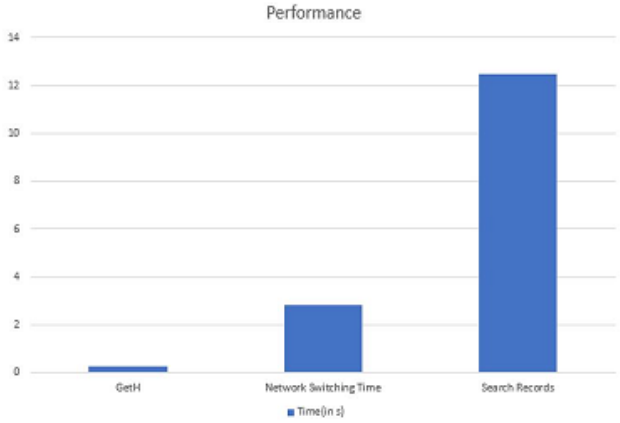

Fig. 12. Average time taken for operations.

TABLE I. PERFORMANCE ANALYSIS FOR NUMBER OF RECORDS SEARCHED

Hospitals	Record 1	Record 2	Record 3
1	15.53	15.63	15.66
2	30.12	30.33	30.45
3	45.45	45.66	45.89

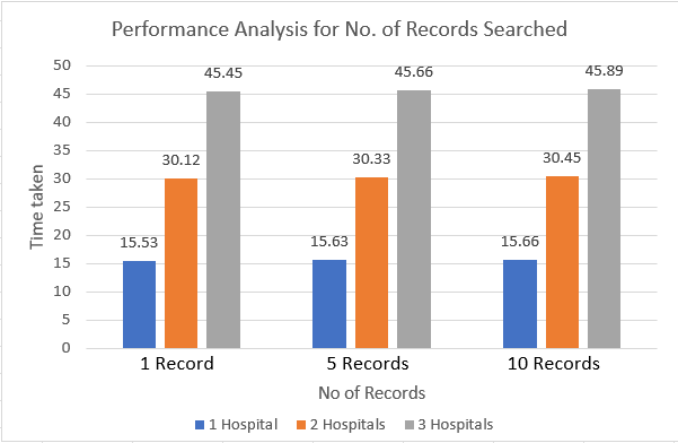

Fig. 13. Performance analysis for number of records searched.

The study involved measuring the average time required for searching records while varying the number of hospitals and records involved. It was observed that the search time was independent of number of records being searched shown in Table I and Fig. 13. The time taken was directly proportional to the number of hospitals involved in the search. This shows that the actual search operation takes place in the order of milliseconds but the majority of the time is due to transaction delay. The time taken for each of the above operations can be optimized if the average time taken for each transaction is relatively reduced by the Ethereum network.

I. Average Latency Comparison

Fig. 14 displays the results of measurements of the delay required to perform various blockchain operations locally as well as between blockchain networks. The Ethereum test bed consists of two virtual computers running on the same physical computer, each of which hosts a different set of test network components. Fig. 14 shows that the suggested approach requires between 4s and 50ms to complete the transaction across the two blockchains, whereas a local transfer on Ethereum requires just 14ms. Therefore, although there is a significant increase, 4s for a transaction in the analyzed use case is manageable.

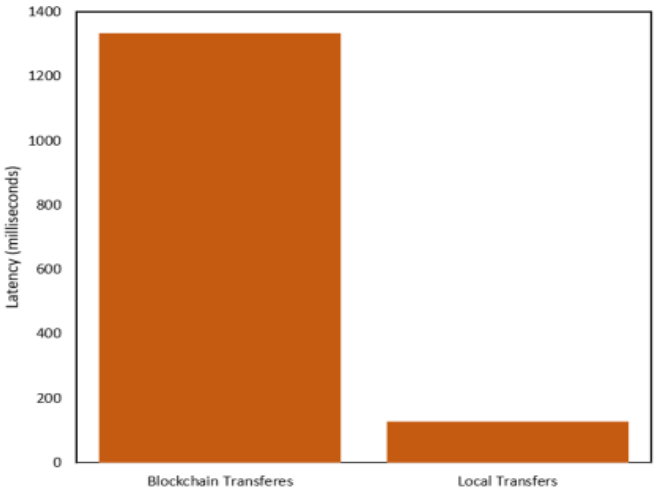

Fig. 14. Latency assessment.

Table II and Fig. 15 provide an illustration of the total CPU utilization for both test networks, denoted as B1 and B2. Throughout the test period, B1 exhibits a CPU consumption of around 66%. As the transaction load increases, this utilization gradually climbs and peaks at approximately 74%. In contrast, B2, involving the operation of four healthcare entities, exhibits a higher CPU consumption of around 80% when the transaction load is 500. This stands as a 10% increase over B1 at the same transaction load. With a rise in the transaction load, B2's CPU consumption further escalates. At a transaction load of 6000, B2's CPU utilization reaches approximately 86%, leading to the occurrence of an average of 411 failed transactions. In conclusion, the findings emphasize the importance of considering and to optimizing CPU resources as the network accommodates a larger number of participants or entities.

TABLE II. CPU UTILIZATION

Transaction Rate	CPU Utilization	
	B1	B2
1000	67	78
2000	66	80
3000	70	80
4000	71	83
5000	73	85

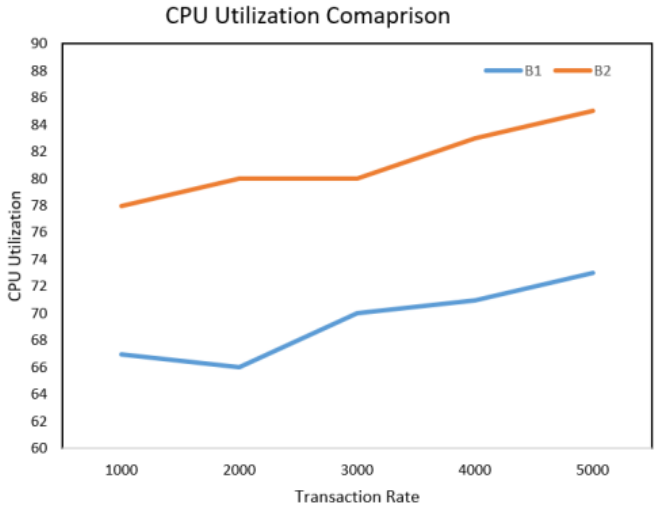

Fig. 15. CPU Utilization.

V. CONCLUSION AND FUTURE SCOPE

In conclusion, the utilization of blockchain technology introduces a promising solution to address the persistent challenges of interoperability and privacy within Electronic Health Records (EHR). This technology empowers patients by granting them centralized access to their medical histories while simultaneously relieving healthcare providers of the lifelong responsibility of safeguarding medical data. Nevertheless, current implementations of blockchain-based EHR systems can address crucial concerns such as efficiency, fairness, and trust. Integrating blockchain with EHR is a multifaceted issue that surpasses the realm of technical expertise and requires collaboration from various stakeholders. To counteract the challenge of non-interoperability, our approach involves constructing a bridge between two similar blockchain networks. Proposed approach illustrates the solution through an EHR Structure, stored across distinct Ethereum Testnets, and enacted via a Solidity Smart Contract. This enables to establish the feasibility of bridging the gap and fostering a seamless interoperability experience between different blockchain networks. The main intention is to utilize a smart contract to embody the EHR Structure specific to individual hospitals. However, the need arises for deploying separate smart contracts for each hospital. Ensuring effective communication between these smart contracts presents a complex challenge, whether within a single blockchain or spanning multiple blockchains. The presented protocol successfully achieves objectives such as privacy conservation, time-controlled annulment, search

functionality, and data security, according to by our extensive security study. It is very resistant to both large-scale and low-key attempts to breach its security. There appears to be an opportunity for the integration of various blockchains to enable the sharing of Electronic Health Records (EHR) within a healthcare consortium from an external viewpoint. The emphasis is on achieving heightened security and efficiency, which could be compared comprehensively with existing solutions in this domain. This ongoing effort seems dedicated to refining the approach for the advantage of the healthcare industry and its stakeholders.

REFERENCES

[1] Agarwal, A., R. Joshi, H. Arora, and R. Kaushik. “Privacy and Security of Healthcare Data in Cloud Based on the Blockchain Technology.” 2023 7th International Conference on Computing Methodologies and Communication (ICCMC), Erode, India vol. 2023: 87–92.

[2] Aich, S., N. K. Sinai, S. Kumar, M. Ali, Y. R. Choi, M. Joo, and H. Kim. “Protecting Personal Healthcare Record Using Blockchain and Federated Learning Technologies.” 2021 23rd International Conference on Advanced Communication Technology (ICACT), Pyeongchang, Korea (South) vol. 2021: 109–12.

[3] Puneeth, R. P., and Parthasarathy, G. “Security and Data Privacy of Medical Information in Blockchain Using Lightweight Cryptographic System” *International Journal of Engineering*, *36*(5), 925-933, 2023 doi: 10.5829/ije.2023.36.05b.09

[4] Baskar, S., and P. V. Gopirajan. “Application of Blockchain in Digital Healthcare.” 2023 International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE), Bengaluru, India vol. 2023: 591–5. DOI: 10.1109/IITCEE57236.2023.10091070.

[5] Gangothri, B. N., K. P. Satamraju, and B. Malarkodi. “Sensor-Based Ambient Healthcare Architecture Using Blockchain and Internet of Things.” 2023 10th International Conference on Signal Processing and Integrated Networks (SPIN), Noida, India vol. 2023: 543–6. DOI: 10.1109/SPIN57001.2023.10116867.

[6] Gul, M. J. J., A. Paul, S. Rho, and M. Kim. “Blockchain Based Healthcare System with Artificial Intelligence.” 2020 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, US vol. 2020: 740–1. DOI: 10.1109/CSCI51800.2020.00138.

[7] Gunanidhi, G. S., and R. Krishnaveni. “Improved Security Blockchain for IoT Based Healthcare Monitoring System.” 2022 Second International Conference on Artificial Intelligence and Smart Energy (ICAIS), Coimbatore, India vol. 2022: 1244–7. DOI: 10.1109/ICAIS53314.2022.9742777.

[8] Gupta, K., N. Jiwani, M. H. U. Sharif, N. Adhikari, and N. Afreen. “Blockchain Technology in Healthcare Industry.” 2022 International Conference on Emerging Trends in Engineering and Medical Sciences (ICETEMS), Nagpur, India vol. 2022: 24–8. DOI: 10.1109/ICETEMS56252.2022.10093377.

[9] Haddad, A., M. H. Habaebi, M. R. Islam, and S. A. Zabidi. “Blockchain for Healthcare Medical Records Management System with Sharing Control.” 2021 IEEE 7th International Conference on Smart Instrumentation, Measurement and Applications (ICSIMA), Bandung, Indonesia vol. 2021: 30–4. DOI: 10.1109/ICSIMA50015.2021.9526301.

[10] Haidar, M., and S. Kumar. “Smart Healthcare System for Biomedical and Health Care Applications Using Aadhaar and Blockchain.” 2021 5th International Conference on Information Systems and Computer Networks (ISCON), Mathura, India vol. 2021: 1–5. DOI:

[11] Iftikhar, M., S. Tahir, F. Alquayed, and B. Hamid. “Blockchain and LDP Based Smart Healthcare IoT Applications: Architecture, Challenges and Future Works.” 2023 International Conference on Business Analytics for Technology and Security (ICBATS), Dubai, United Arab Emirates vol. 2023: 1–6. DOI: 10.1109/ICBATS57792.2023.10111134.

[12] Khujamatov, K., E. Reypnazarov, N. Akhmedov, and D. Khasanov. “Blockchain for 5G Healthcare Architecture.” 2020 International Conference on Information Science and Communications Technologies (ICISCT), Tashkent, Uzbekistan vol. 2020: 1–5. DOI:

[13] Lee, A. R., M. G. Kim, K. J. Won, I. K. Kim, and E. Lee. “Coded Dynamic Consent Framework Using Blockchain for Healthcare Information Exchange.” 2020 IEEE International Conference on Bioinformatics and Biomedicine (BIBM), Seoul, Korea (South) vol. 2020: 1047–50. DOI: 10.1109/BIBM49941.2020.9313330.

[14] Liu, Jingwei, Weiyang Jiang, Rong Sun, Ali Kashif Bashir, Mohammad Dahman Alshehri, Qiaozhi Hua, and Keping Yu. May 2023. “Conditional Anonymous Remote Healthcare Data Sharing over Blockchain.” in *IEEE Journal of Biomedical and Health Informatics* 27, no. 5: 2231–42.

[15] Marry, P., K. Yenumula, A. Katakam, A. Bollepally, and A. Athaluri. “Blockchain Based Smart Healthcare System.” 2023 International Conference on Sustainable Computing and Smart Systems (ICSCSS), Coimbatore, India vol. 2023: 1480–4.

[16] Puneeth, Reval Prabhu, and Parthasarathy Govindaswamy. "Survey on Security and Interoperability of Electronic Health Record Sharing Using Blockchain Technology." *Acta Informatica Pragensia* 12, no. 1 (2023): 160-78.

[17] Mukherjee, A., R. Halder, J. Chandra, and S. Shrivastava. “HealthChain: A Blockchain-Aided Federated Healthcare Management System.” 2023 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Dubai, United Arab Emirates vol. 2023: 1–5.

[18] Ramar, K., G. P. V, H. Shanmugasundaram, B. P. Andraju, and S. Baskar. “Digital Healthcare Using Blockchain.” 2022 1st International Conference on Computational Science and Technology (ICCST), CHENNAI, India vol. 2022: 651–5.

[19] Ren, J., J. Li, H. Liu, and T. Qin. August 2022. “Task Offloading Strategy with Emergency Handling and Blockchain Security in SDN-Empowered and Fog-Assisted Healthcare IoT.” in *Tsinghua Science and Technology* 27, no. 4: 760–76. DOI: 10.26599/TST.2021.9010046.

[20] Sheeraz, M. M., M. A. I. Mozumder, M. O. Khan, M. U. Abid, M.-I. Joo, and H.-C. Kim. “Blockchain System for Trustless Healthcare Data Sharing with Hyperledger Fabric in Action.” 2023 25th International Conference on Advanced Communication Technology (ICACT), Pyeongchang, Korea, Republic of vol. 2023: 437–40.

[21] Sinha, A., A. Patel, and M. Jagdish. “Application of Blockchain in Healthcare.” 2022 First International Conference on Artificial Intelligence Trends and Pattern Recognition (ICAITPR), Hyderabad, India vol. 2022: 1–4. DOI: 10.1109/ICAITPR51569.2022.9844186.

[22] Suciu, G., M. Balanescu, S. Mitroi, D. Trufin, M. Falahi, C. Serban, and N. Goga. “An Overview of Blockchain Technology in STAMINA Project.” 2022 IEEE International Conference on Blockchain, Smart Healthcare and Emerging Technologies (SmartBlock4Health), Bucharest, Romania vol. 2022: 1–4.

[23] Tidke, S. K., V. Khedkar, A. Banerjee, A. Mulik, A. Goyal, and Y. Chhabaria. “An Interactive and Secure Blockchain Web Portal for Online Healthcare Services.” 2022 International Conference on Decision Aid Sciences and Applications (DASA), Chiangrai, Thailand vol. 2022: 454–9. DOI: 10.1109/DASA54658.2022.9764973.

[24] Mousa Mohammed Khubrani, “Artificial Rabbits Optimizer with Deep Learning Model for Blockchain-Assisted Secure Smart Healthcare System” International Journal of Advanced Computer Science and Applications(IJACSA), 14(9), 2023. http://dx.doi.org/10.14569/IJACSA.2023.0140998.

[25] Zhu, T.-L., and T.-H. Chen. “A Patient-Centric Key Management Protocol for Healthcare Information System Based on Blockchain.” 2021 IEEE Conference on Dependable and Secure Computing (DSC), Aizuwakamatsu, Fukushima, Japan vol. 2021: 1–5. DOI: 10.1109/DSC49826.2021.9346259