Original Article

Access this article online
Quick Response Code:

Website:
www.jehp.net

DOI:
10.4103/jehp.jehp_984_23

Securing patient data in the healthcare industry: A blockchain-driven protocol with advanced encryption

Sourav Kunal, Parth Gandhi, Digvijaysinh Rathod, Ruhul Amin[1], Sachin Sharma[2]

Abstract:

BACKGROUND: Ensuring the security and privacy of patient data is a critical concern in the healthcare industry. The growing utilization of electronic data transmission and storage in medical records has amplified apprehensions about data security. However, due to varying stakeholder interests, not all data can be freely shared, necessitating the development of secure protocols.

MATERIALS AND METHODS: This study presents a highly secure protocol that integrates blockchain technology, patient biometric information, and robust cryptographic algorithms (elliptic curve cryptography (ECC) and advanced encryption algorithm (AEC)) to facilitate data encryption and decryption. The protocol encompasses secure login, secure key sharing, and data sharing mechanisms among miners, offering comprehensive security measures. To validate the effectiveness of the proposed protocol, both informal and formal security analyses are conducted. The security protocol description language in Scyther is utilized to evaluate the protocol's resilience against attacks.

RESULTS: The culmination of this research is a secure protocol that leverages blockchain technology and ECC for the secure storage and sharing of medical records. The protocol covers all stages, including system setup, user registration, login mechanisms, key exchange between users and blockchain, communication between blockchains, and interaction with other miners, with a steadfast emphasis on security. Furthermore, the protocol's communication and computation costs are assessed, with a comparison to existing blockchain-based schemes. Informal proofs establish the protocol's security against common attacks faced by medical institutions. Formal simulation of the protocol using the Scyther tool provides definitive evidence of its resistance to attacks.

CONCLUSIONS: As a result, this protocol presents a viable real-time implementation solution for safeguarding patient data within the healthcare domain, representing a significant contribution to data security.

Keywords:

Advanced encryption algorithm (AES), blockchain, elliptic curve cryptography (ECC), health care, privacy, protocol, robustness, Scyther, security

Department of School of Cyber Security and Digital Forensics, National Forensic Sciences University, Gandhinagar, Gujarat, India, [1]Department of Computer Science and Engineering, NIT Jamshedpur, Jharkhand, India, [2]Department of CSE, Indrashil University, Mehsana, Gujarat, India

Address for correspondence:
Dr. Sachin Sharma, Department of CSE, Indrashil University, Mehsana, Gujarat - 382 740, India.
E-mail: sharma.f@gmail.com

Received: 07-07-2023
Accepted: 12-12-2023
Published: 28-03-2024

Introduction

Medical data are one of the very sensitive data. The usage of blockchain[1] to secure the medical data is among the trending research topics at present because it is very necessary to secure the medical data as well as for the concept of information blocking. Information blocking[2] can be described as when patient not always wants to share their own data publicly and when they want to share data with someone, it needs to be done by protecting it from other parties. Also, issues such as time, storage, and speed are always there along with the security issues when data are transferred through paper. With the current trend and the evolution of the digital century, it is necessary that there is a shift from the older paper-based systems which

How to cite this article: Kunal S, Gandhi P, Rathod D, Amin R, Sharma S. Securing patient data in the healthcare industry: A blockchain-driven protocol with advanced encryption. J Edu Health Promot 2024;13:94.

are not only hard to generate and hard to archive and maintain but also tends to lose their integrity to the modern electronic data generation, storage, and transmission-based system. Along with that, in recent times, we see a new trend in the market, that is, the increase in the mobility of patients internally (within the country) and globally (across the globe). As such, the sharing of the medical records has become a very high priority but with the current laws that are prevailing such as the Health Insurance Portability and Accountability Act (HIPAA), it is also necessary for the healthcare institutions to share these data in a very secure form.[3] Not only that but there has been a rise in need of not only securing the medical records of a patient but also allowing them to access their past records, for instance, a person is suffering from brain tumor, in such a scenario, each and every past doses, chemotherapy sessions, and various other medications the patient may have gone through is a must for the doctor to be aware of. Without this critical information, there can be a serious mishap in the treatment of the patient.[4] Authors such as Zhang and Lin[5] have proposed a protocol to achieve security and privacy of personal health information (PHI).

As mentioned earlier, blockchain provides a distributed, immutable, and transparent history of the medical transactions, thus enabling the development of a trustworthy and secure application for medical purposes[4] but there can be some challenges that a developer might face such as the transaction forms that are used in the blockchain are created using programming languages and are thus vulnerable toward duplication. To remedy this contract, transactions were introduced that could be used for verification. Another such challenge that is faced by blockchain is bugs. These bugs can be found in the consensus and peer-to-peer (P2P) algorithms used in the blockchain. As an example, Tendermint[6] a quite famous P2P protocol was reported to have four bugs in the year 2019. Al Omar[7] discussed about storing of data in an encrypted format. Again, storing of data in centralized servers even if the data are encrypted becomes impractical to store a large amount of data for many people.

So, researchers proposed a blockchain solution that could protect the data from tampering and even leakage. Not only this but the proposed solution could be actually very reliable as it deals with both the privacy and confidentiality of the patient's data. Li *et al*.[8] have developed a data preservation scheme and the method to check the validation of the preserved data even. They have used Ethereum to actually showcase the whole scenario. Fan *et al*.[9] have worked on basically the access and retrieval of the data sharing process in detail due to the advent of electronic medical records (EMR). Azaria *et al*.[10] state four major problems that are encountered during the generic health record maintenance system namely the fragmented data, infrequent availability of data, interoperability of systems, and improvement in the quantity and quality of medical research. They were one of the pioneers in using blockchain technology for medical records, stating that blockchains have been previously applied to permission management systems and as such is possible to use that same characteristic of blockchain and apply them in the field of health care. The blockchain technology supports the use of "smart contracts" which is nothing but the transaction-based state machine generalization of the blockchain that enables the tracking and automation of transactions. Every block in the blockchain not only represents the ownership but also depicts various permissions associated with it. These blocks when added or modified are notified to the owners which then accept or reject the said changes.

A holistic approach is crucial in protecting medical data and addressing security concerns, including information blocking. To achieve this, it is essential to explore innovative design ideas and research avenues. Understanding the complete data flow, from end-to-end, along with storage, will provide insights into areas where security can be enhanced. Moreover, considering the collaboration of multiple hospitals and their private blockchains, research should focus on secure data communication and robust key agreements.

In this paper, we aim to investigate various research ideas within the blockchain framework, seeking to develop a resilient model that not only safeguards against known attacks but also addresses pertinent research questions surrounding data security in the healthcare domain. These research questions include how user authentication and access control mechanisms can be effectively implemented within blockchain networks to protect against unauthorized access and user impersonation, how cryptographic techniques and key management schemes can be leveraged to enhance the confidentiality and integrity of medical data stored on the blockchain, and what are the implications of scalability and performance when implementing blockchain solutions for medical data security, and how can they be addressed effectively. By addressing these research questions, we aim to contribute to the development of robust solutions that ensure secure user authentication, protect against unauthorized access and impersonation, strengthen the confidentiality and integrity of medical data through advanced cryptographic techniques, and tackle the scalability and performance challenges associated with implementing blockchain in healthcare systems.

Organization and Contribution of the Paper

This paper is prefaced with an abstract in the beginning, and it is continued with an introduction in Section 1.

Section 2 discusses the organization and contributions made by the author, and it is followed by Preliminaries in Section 3. The proposed protocol is discussed in Section 4, which highlights the aim of this research using various algorithms or technologies, and it also discusses phases of the proposed protocol in detail. Section 5 discusses the real-world implementation challenges along with informal security analysis conducted for the proposed protocol. After this, a formal analysis is conducted using a security tool in Section 6. Following this, performance evaluation is conducted in Section 7. Section 8 concludes this paper, and it is followed by the list of references in the later Section.

The contribution of the paper is discussed below:

- We proposed a secure patient-centric model for the healthcare industry.
- Based on the proposed model, we have proposed a secure communication protocol for the patient's data sharing that is based on blockchain and elliptic curve cryptography (ECC).
- To prove the security claims of the proposed protocol, we have performed the informal security analysis and also the formal security analysis by the tool named "Scyther."
- As a part of performance evaluation, we have compared our model with the relevant state-of-the-art in terms of computation and comparison overhead.

Preliminaries

Xia *et al*.[11] introduced a blockchain-based framework that can protect the autonomy of data using cloud technology. Only the verified users can access the system, and the user's activities are monitored. Cryptographic techniques are implemented while sharing patient's data. A lightweight blockchain is implemented for faster transactions and better efficiency. They have introduced a three-layer model namely user layer, system management layer, and storage layer. As the name suggests, user layer contains all the users that are going to access the system. The system management layer is the crux of this model and as such very important as all the connections for secure transaction are established at this layer, and lastly, the storage layer where all the important data are securely stored at cloud for further use.

Xia *et al*.[12] proposed a system that will provide efficiency, authenticity, and accountability to healthcare records and having minimal risk to health records called MedShare. The records are stored such that tampering can be prevented. The system introduced contains four layers. The first layer is the user layer which as name suggests is made up of all the users and blockchain miners who accesses the system and who can request for a transaction. The second layer is the data query layer whose job is to either process or forward the queries it receives from the miners; it has two components a querying layer and a trigger layer of which the former processes the queries it receives and the later acts as a mediator between the blockchain and the real world. The data provenance layer is the third layer of the system which contains an authenticator, smart contracts, smart permissioned database, processing and consensus nodes, and blockchain network. The database infrastructure layer is the last layer that contains data.

Al Omar *et al*.[7] suggested a new decentralized data management system that uses blockchain technology for integrity and accountability and anonymity using cryptographic mechanism. There is a data sending module whose has twofold role of checking whether the information is correct or not; if correct, it will encrypt the data and preserve it. On the other end, there is a data receiver module whose job is to receive the data and authenticate it. Along with these main modules, there is also a registration unit that registers users using their username, password, and biometrics, log-on module, and private accessible unit which provides a secure channel for users to communicate and initiate transactions, acting as a mediator between user and blockchain module. The user receives an identifier with which he can access his data from the blockchain.

Li *et al*.[8] introduced an information-preserving framework for stocking information and used blockchain technology and cryptography for protecting user's information. The system is developed on Ethereum that provides security and efficiency. In the proposed system, as a new data of patient are encountered, a new block is added to the already existing chain of blocks where all the blocks are connected with each other in a distributed decentralized form. The new block has a timestamp entry which is verified and also has a hash entry entered by calculating hash of all the existing blocks, thus providing integrity to the data.

Ji *et al*.[13] proposed a model multilevel location sharing scheme using blockchain technology. It guarantees assurance, decentralization, dependability, and correctness of patient's location. The new model contains a data sending layer for sending data in encrypted form, data receiving module to receive data along with authenticating it, registration unit for user registration log-on unit for secure log-on, and private accessible unit for establishing a secure channel for communication.

Zhou *et al*.[14] proposed a novel framework which is fast and uses less memory and processing. The stakeholders of this framework are clinics, patients, and insurance companies. It was developed on a secure framework called Ethereum. This framework contains user level that contains user information, system management layer that establishes secure communication for transaction, and storage layer for storing information in the cloud environment.

Fan *et al*.[9] depicted a scenario where the patient's records are stored in multiple databases, that is, at different hospitals due to various reasons during such a scenario, data sharing becomes a problem. For such a problem, Fan *et al*. suggest a decentralized approach using blockchain. As a new patient is added, a separate block is added in the chain. For the given block, a timestamp is added along with hash info. All the previous blocks are added, thus providing a decentralized solution that solves the single point of failure. Legalized care has to be taken, and monitoring is required when adding data in the chain. This solution can provide data from multiple sources, thus solving the problem of data sharing.

Yang H and Yang B[15] insisted a blockchain-based approach for protecting Confidentiality, Integrity, and Availability (CIA) of the data as well as maintaining the interoperability of the data so that secure data sharing in health care can be made possible. This framework has membership services to verify the users and miners of the software, local database, and cloud-based secure data storage using symmetric encryption, nodes, and application programming interfaces (APIs). If a doctor queries about a patient, the profile gets verified using encryption and digital signature. The access to all data is based on access control defined for every user. The privacy, scalability, and security are taken as parameters for evaluating the performance of the framework.

Zhang and Lin[5] proposed a new blockchain mechanism that uses two blockchains. The private blockchain stores the medical records of the patients, while the consortium blockchain creates secure indexes for data stored in the private blockchain. The data of the patients and their identity are public key encrypted. After every transaction, the authenticity of the user is checked using various cryptographic techniques, and if matches, the block is added to the chain. This mechanism is very useful in storing a huge number of patient records, fast retrieval, and great measure of security is required, that is, to protect against laws enforced due to breaches in medical records of patients.

Uddin *et al*.[16] proposed a novel framework for remote patients in the healthcare system using blockchain-based technology. The architecture has sensors which collects healthcare information. After that, the info is stored in the blockchain by creation of new blocks for every information. The mining system for the proposed architecture is different from traditional blockchain as if in contrast to multiple miners, only a single miner mines the blocks. The miner is selected through patient agent, thus creating a patient-centric architecture. The architecture lacks block validation and authentication protocols.

Materials and Methods

Our aim is to address the existing problem of security in medical data by implementing a comprehensive approach that combines cutting-edge encryption algorithms and blockchain technology. The security of medical data has become a pressing concern, with numerous incidents of unauthorized access, data breaches, and compromised patient privacy.

To combat these challenges, we have developed a robust solution that encompasses the utilization of ECC and advanced encryption standard (AES), alongside the integration of blockchain for data storage. By adopting ECC, we ensure strong encryption while optimizing key lengths, making it ideal for resource-constrained environments commonly found in healthcare settings. AES, a trusted and efficient symmetric encryption algorithm, further bolsters our security measures. Moreover, we have embraced blockchain technology to securely store the encrypted medical data. The blockchain's inherent features, including immutability, decentralization, and transparency, address the vulnerabilities associated with centralized data repositories. By leveraging blockchain, we can establish a tamper-resistant and auditable environment for medical data storage.

Through our integrated approach, combining ECC, AES, and blockchain, we strive to mitigate the prevalent security risks surrounding medical data. Our solution not only fortifies the confidentiality, integrity, and privacy of patient information but also enhances trust and transparency within the healthcare ecosystem. By proactively addressing the existing security challenges, we aim to ensure the utmost protection of sensitive medical data, fostering a safer and more secure healthcare landscape for all stakeholders involved.

So, we have proposed a six-phase protocol to consider the security of the data which uses Delegated Proof of Stake (DPoS) consensus mechanism.[17] Our proposed model is shown in Figure 1, and the phases of the protocol are shown from the flowchart in Figure 2.

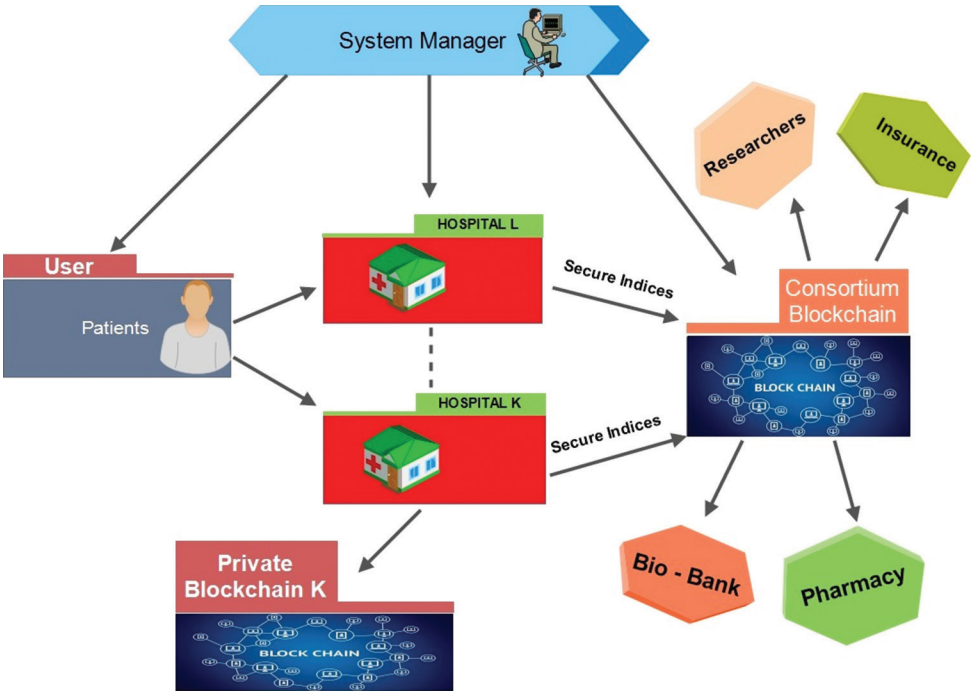

Figure 1: Proposed model

The proposed model consists of patients as user, and it is connected with the system manager and the hospital. Each hospital has its own private blockchain with all the sensitive data. There is another blockchain known as consortium blockchain which gets data from various hospitals, and these data will be limited to the requirements such as blood required, medicines prescribed, insurance subscribed, and even about the new things discovered for our researchers. All these data will be available only to the specific people who needs that. The whole process of communication and data sharing in detail is described below.

Table 1: Abbreviations used

Symbol	Description
CSM	Cloud system manager
ID_p	Identity of the patient
PD_p	Password of the patient
BI_p	Biometric template of the patient
R_p	Random number generated by CSM
T_1	Timestamp
$\oplus$	Bitwise XOR operation
k	Concatenation operation
H (i)	One-way hash function, where i stands for 1, 2, etc.
||	Concatenation

Phases of our protocol

In this subsection, the phase of our protocol is discussed, and in Table 1, all the abbreviations used in this protocol are listed.

1. System setup phase
2. Patient registration to cloud server as shown in Figure 3
3. System login phase as shown in Figure 4
4. Key agreement between patient and private blockchain of hospitals as shown in Figure 5
5. Secure communication between private blockchain of hospitals and consortium blockchain as shown in Figure 6
6. Secure communication between consortium blockchain and blockchain miners as shown in Figure 7

System setup phase

- Cloud system manager (*CSM*) chooses a private key (Y) and computes public key (Z); $Z = Y.G$, where G is the generator of the group.
- For the setup of the network, a system administrator (SM) chooses a unique identity ID_{sm}, and computes
  $ID_{sm} = H(ID_{sm} \text{ k } Y)$ and $Z_{sm} = Y_{sm}.G$
- Now, SM stores $< ID_{sm}, Y_{sm} >$ in the CSM and announces Z_{sm} as the public information. $Z_{sa} = Y_{sm}.Z_{sm}$

Patient registration to cloud server

- Patient chooses low entropy information (ID_p) and password (PD_p) and also takes biometric information (BI_p) and computes $A_p = H1(ID_p \text{ k } PD_p)$, $B_p = H2(BI_p)$. Then, the patient sends information $< ID_p, A_p, B_p >$ to the CSM through private channel.
- On getting registration message, CSM generates a random number but unique, that is, R_p, and maintains a table to store tuple $< ID_p, R_p, B_p >$ for further uses.
- CSM computes $C_p = H_1(R_p \text{k} Y) \oplus A_p$, $D_p = H_1(A_p \text{k} B_p)$ and

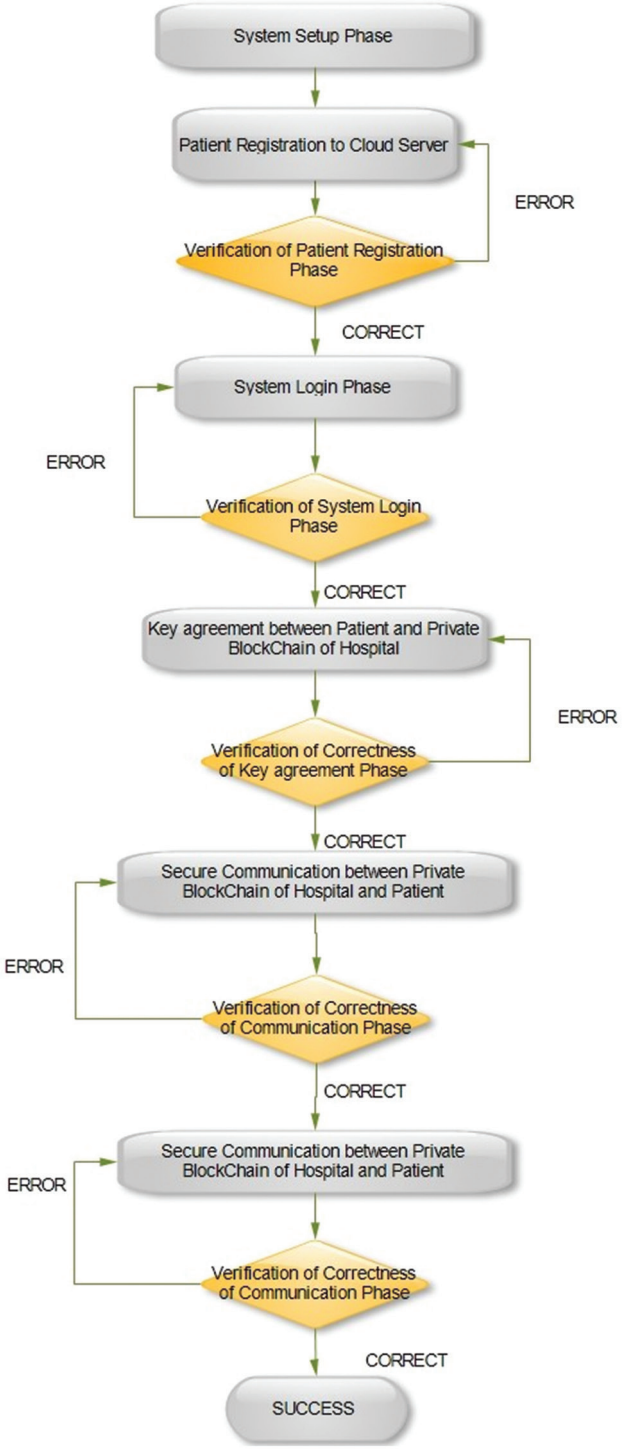

Figure 2: Flowchart

then stores C_p and D_p in the application software (.apk) and then stores in the server. Finally, CSM sends a confirmation message to acknowledge successful registration.

System login phase

- Patient executes the installed application and provides ID_p^0 and PD_p^0 as well as BI_p'. Then, the application first computes $A_p' = H1(ID_p'||PD_p')$, $D_p' = H1(A_p'||B_p')$, where $B_p' = H2(B_p)$. Then, it checks the condition $D_p^0 = ?D_p$; if it holds, patient is authentic, otherwise it rejects the patient.
- Now, the application generates a random number R_a and computes $G_1 = R_a.Z_{sm}$, $G_2 = V + R_a.Z_{sa}$, where V is the random point, that is, $V = (V_x, V_y)$.
- Now, the application computes $K_p = H1(ID_p \text{ k } R_a \text{ k } V_x \text{ k } T_1 \text{ k } ID_h)$; $L_p = ID_p \oplus H1(V_x)$; $M_p = R_a \oplus H1(V_y)$, where T_1 is the timestamp.
- The same software now forwards the message $< G_1, G_2, K_p, L_p, M_p, T_1, Id_h >$ to the private blockchain of hospitals whose identity is ID_h through insecure communication.

Key agreement between patient and private blockchain of hospitals

- After receiving login message, first check the timestamp. If it is valid, continue the operation, otherwise stops procedures due to some technical issues (such as replay attack). Then, the private blockchain of hospitals computes V using G_1 and G_2, where $V = V_x, V_y$ and retrieves $(ID_p') = L_p \oplus H_1(V_x)$ and $R_a^0 = M_p \oplus H_1(V_y)$ and computes $K_p^0 = H_1(ID_p^0 \text{ k } R_a^0 \text{ k } V_x \text{ k } T_1 \text{ k } ID_h)$ and checks $K_p^0 = ?K_p$. If the condition $K_p^0 = ?K_p$ is correct, the private blockchain of hospitals computes a common key $K_s = H_1(ID_p \text{ k } R_a^0 \text{ k } V_y \text{ k } ID_h)$ and further computes $K_v = H_1(ID_p \text{ k } R_a^0 \text{ k } K_s \text{ k } T_h)$.
- Now the private blockchain of hospitals forwards $< K_v, T_h >$ to the user through insecure channel. On getting message, the application software first checks timestamp verification using the same procedure mentioned above. If the timestamp verification is true, then the software computes $K_s^0 = H_1(ID_p \text{ k } R_a' \| V_y \| ID_h)$, $K_v' = H_1(ID_p \| R_a' \| K_s \| T_h)$ and verifies the condition $K_v' = ?K_v$.
  If the condition $K_v' = ?K_v$ is satisfied, then the common key K_s is verified, and now, this key can be used for secure communication between the patient and private blockchain of hospitals.
- Now, the user will take some query (Q) and encrypts it using K_s with the help of AES and sends cipher text to the private blockchain of hospitals. After getting cipher text, private blockchain of hospitals finds Q after decryption and checks whether the data are present in the database against query Q.

Secure communication between private blockchain of hospitals and consortium blockchain

- The private blockchain of hospitals first generates a random number R_h and computes $A_1 = H_1(ID_h \| ID_{cb} \| R_h \| T_c \| Y_{sm})$, $A_2 = R_h \oplus H_1(Y_{sm}.Z_{sm}).ID_p)$ and then sends A_1, A_2, T_c to the consortium blockchain through secure communication, where T_c is the current timestamp.

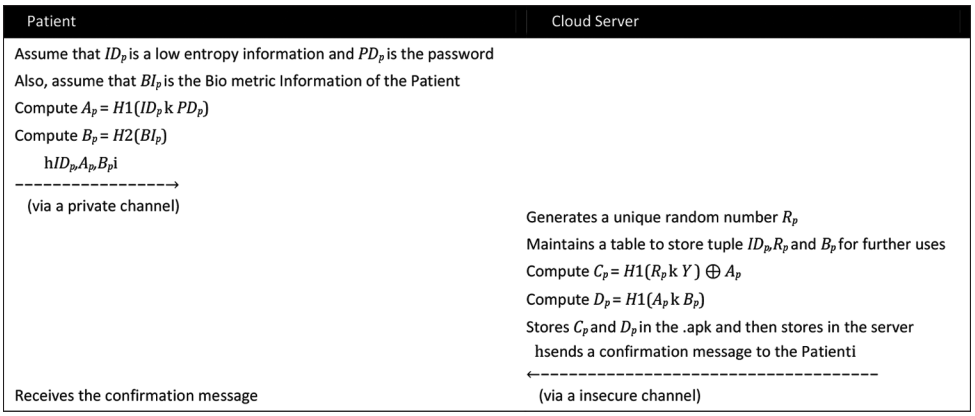

Figure 3: Patient registration to cloud server

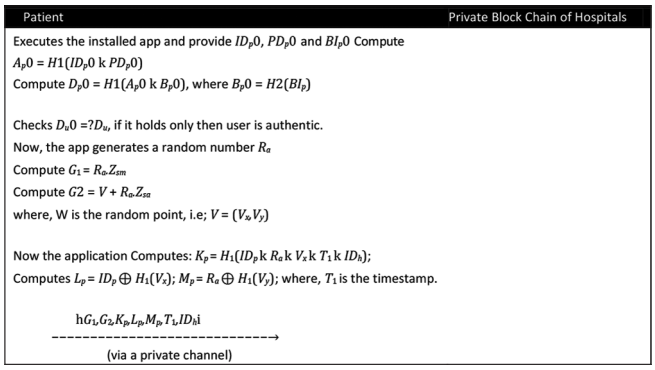

Figure 4: System login phase

- Now, consortium blockchain first receives the message A_1, A_2, T_c and immediately checks the timestamp. If the timestamp condition is successful, the consortium blockchain calculates R_h using A_2 and Y_{sm} and further calculates $A_1* = H_1(ID_h \| ID_{cb} \| R_h \| T_c \| Y_{sm})$ and checks $A_1* = ?A_1$. If the condition $A_1* = ?A_1$ is valid, private blockchain of hospitals is authenticated to consortium blockchain. Now, consortium blockchain computes a common key $K_1 = H_1(ID_h \| ID_{cb} \| R_h \| R_{cb})$, where R_{cb} is the random number, and further computes, $K_{v1} = H_1(ID_h \| Y_{sm} \| K_1)$, $RN_{cb} = R_h \oplus R_{cb}$. Finally, consortium blockchain sends K_{v1}, RN_{cb}, T_c to private blockchain of hospitals through secure communication.
- The private blockchain of hospitals first receives the messages and immediately checks timestamp verification using T_{cb} and then extracts R_{cb} and computes $K_1* = H_1(ID_h \| ID_{cb} \| R_h \| R_{cb})$; $K_{v1}* = H_1(ID_h \| Y_{sm} \| K_1*)$ and checks $K_{v1}* = ?K_{v1}$, where K_1 is the common key used for secure communication between private blockchain of hospitals and consortium blockchain.

Secure communication between consortium blockchain and blockchain miners

- The consortium blockchain first generates a random number R_{cb} and computes $B_1 = H_1(ID_{cb} \| ID_{bm} \| R_{cb} \| T_x \| Y_{sm})$, $B_2 = R_{cb} \oplus H_1(Y_{sm}.Z_{sm}).ID_p)$ and then sends B_1, B_2, T_x to the blockchain miner through secure communication, where T_x is the current timestamp.
- Now, blockchain miners first receive the message B_1, B_2, T_x and immediately check the timestamp. If the timestamp condition is successful, the miner calculates R_{cb} using B_2 and Y_{sm} and further calculates $B_1* = H_1(ID_{cb} \| ID_{bm} \| R_{cb} \| T_x \| Y_{sm})$ and checks $B_1* = ?B_1$. If the condition $B_1* = ?B_1$ is valid, the miners are authenticated to consortium blockchain. Now, miners compute a common key $K_2 = H_1(ID_{cb} \| ID_{bm} \| R_{cb} \| R_{bm})$, where R_{bm} is the random number and further computes, $K_{v2} = H_1(ID_{cb} \| Y_{sm} \| K_2)$, $RN_{bm} = R_{cb} \oplus R_{bm}$. Finally, the miners send K_{v2}, RN_{bm}, T_x to consortium blockchain through secure communication.
- The consortium blockchain first receives the messages and immediately checks timestamp verification using T_{bm} and then extracts R_{bm} and computes $K_2* = H_1(ID_{cb} \| ID_{bm} \| R_{cb} \| R_{bm})$; $K_{v2}* = H_1(ID_{cb} \| Y_{sm} \| K_2*)$ and checks $K_{v2}* = ?K_{v2}$, where K_2 is the common key used for secure communication between consortium blockchain and blockchain miners.

Challenges related to real-world implementation

In this section, we would like to highlight certain possible drawbacks or difficulties that this protocol might present in actual healthcare systems in this section. In addition to the difficulties, we have covered the remedies to these difficulties below.

Issues related to legal and compliance standards

Laws vary from nation to nation, and the healthcare industry is heavily controlled. The use of healthcare data may be restricted by legislation such as HIPPA,[18] which was primarily created for US citizens.

To tackle this challenge, we have kept healthcare data protected while sharing and it is suggested to establish clear terms and conditions for data usage.

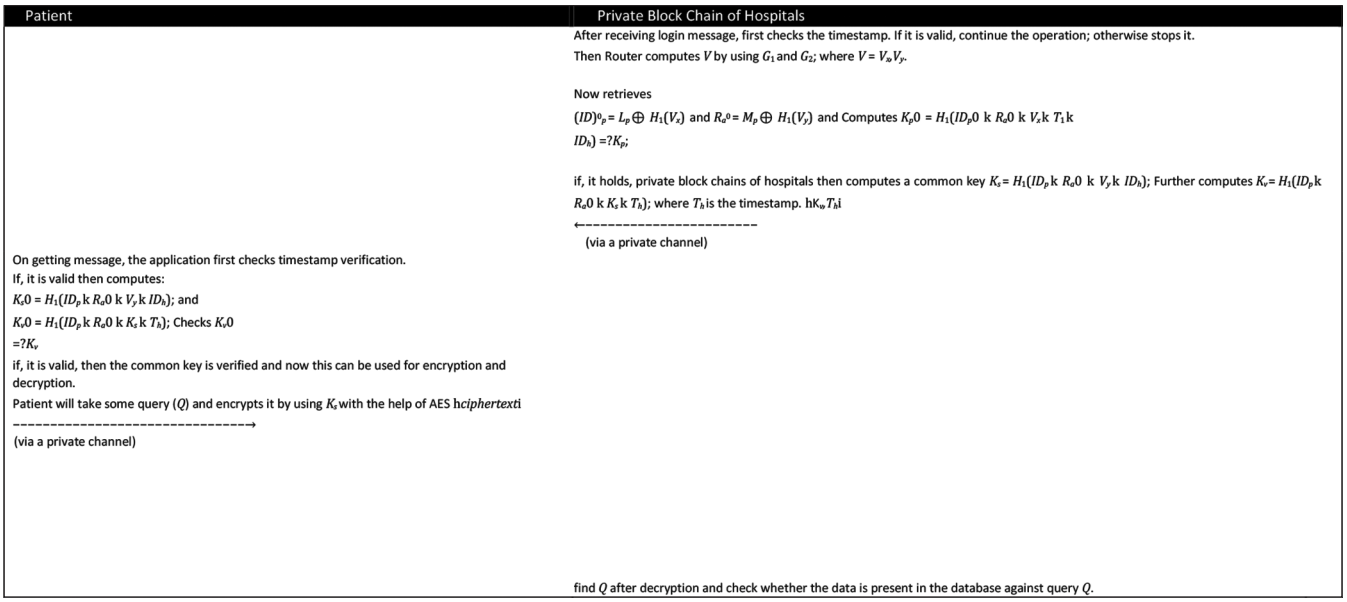

Figure 5: Key agreement phase between patient and private blockchain of hospitals

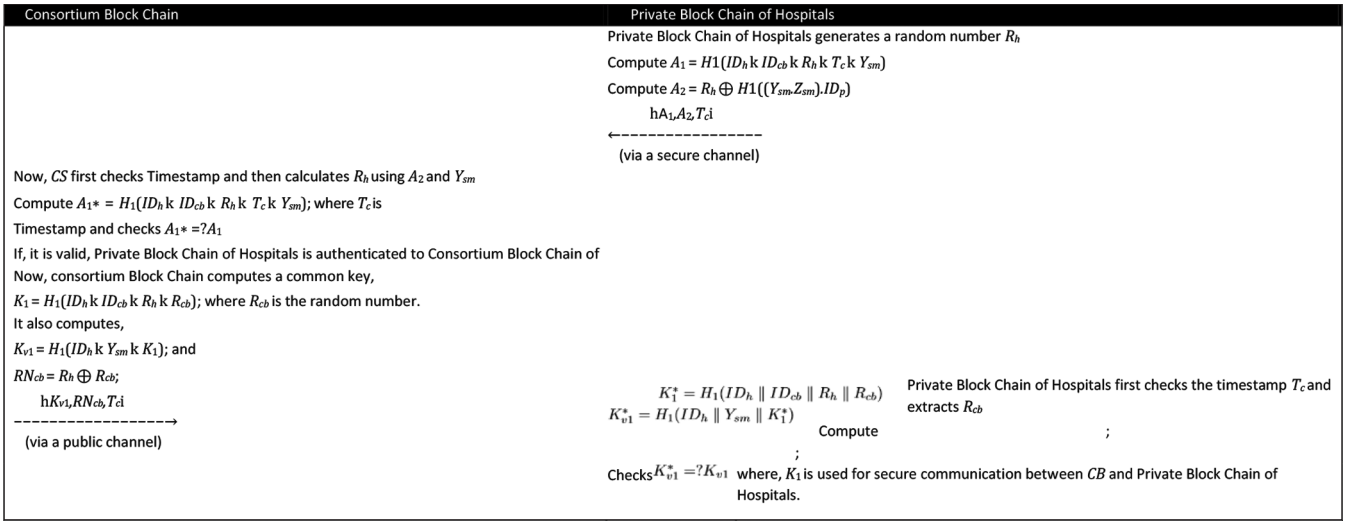

Figure 6: Protocol for secure communication between private blockchain of hospitals and consortium blockchain phase

Issues related to infrastructure and connectivity

It is clear that certain parts of the nation might not have the necessary connectivity and infrastructure to enable blockchain systems.

Given that the proposed protocol is made to function well even in settings with limited bandwidth or connectivity, in the suggested protocol, mobile app usage has also been covered for end users. Thus, consumers can access blockchain-based healthcare system data from even the most remote locations.

Issues related to interoperability and scalability

This problem might complicate data interchange between different blockchain platforms to employ many data standards or formats, particularly when the systems produce enormous volumes of data.

The proposed protocol is based on DPoS. DPoS is a compelling solution for addressing scalability concerns in blockchain systems, enabling faster transaction processing and increased throughput. Common standards for data communication must be adopted to address interoperability-based challenges. Data formats[19] such as Health Level Seven (HL7) and Fast Healthcare Interoperability Resources (FHIR) are available. The developers can use healthcare data more easily thanks to these data formats.

Issues related to computation cost- and resource-intensiveness

It is common knowledge that implementing new blockchain solutions can be more expensive and resource-intensive.

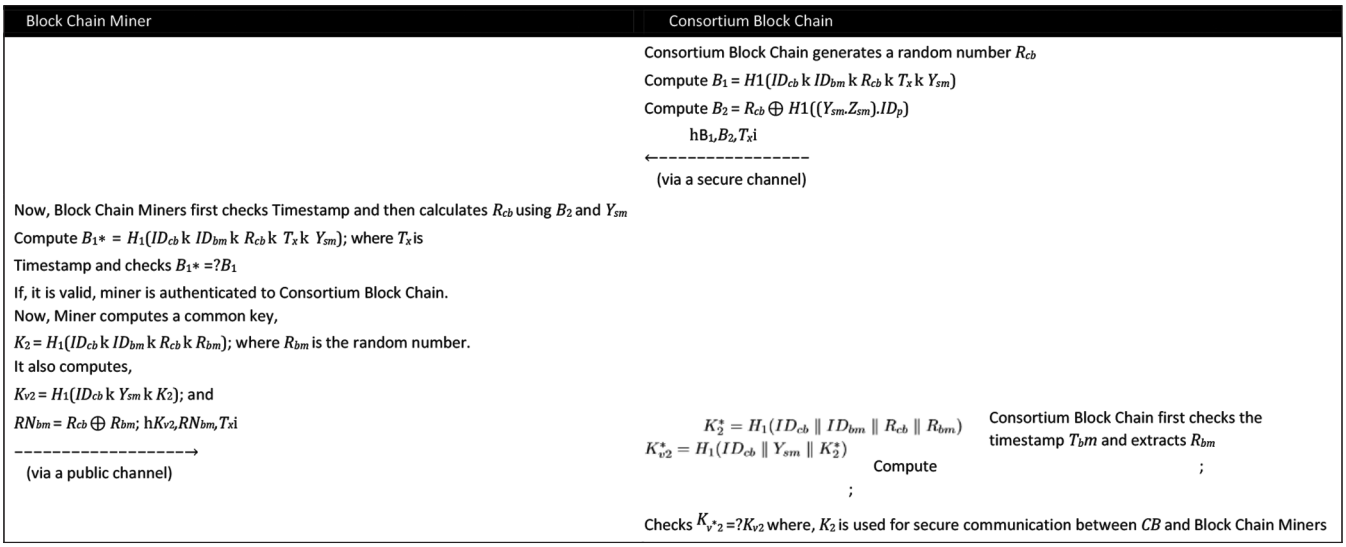

Figure 7: Protocol for secure communication between consortium blockchain and the blockchain miner phase

To address this, we have compared the suggested protocol with a few of the blockchain solutions that are now available and have demonstrated that, in terms of cost and communication, the proposed protocol is comparable and does not require extensive use of resources.

In the subsections below, we have conducted both formal and informal security analyses for issues pertaining to data security and privacy.

Informal security analysis

Proposition 1. *The proposed protocol is secure against offline password guessing attack.*

Proof. An offline password guessing attack involves an attacker attempting to guess user passwords by exploiting compromised password databases, potentially granting unauthorized access to medical data, and compromising patient privacy and confidentiality. In our proposed protocol, for user registration, we take a low entropy *ID* and password *PD* as input which is susceptible to guess attacks from the threat actor. In the registration phase, password and identity are only used to generate C_p and D_p which are sent to the cloud server as well stored in the application, where $C_p = H1(R_p \| Y) \oplus A_p$ and $D_p = H1(A_p \| B_p)$. In equation *Dp, Bp* is the output of the biometric hash of the patient's fingerprint (BI_p).

The following description will prove the resilience of the above attack.

- The parameter C_p is quite secure as it is generated using hash function. From C_p, it is very difficult to generate A_p as there are unknown parameters such as R_p. Even if the attacker finds A_p, he will not be able to extract password because of the security provided by the hash function. And furthermore, as randomness is added using R_p, the guessing of password from A_p is a very herculean task.
- The parameter D_p is also protected by the hash function. Hence, it is difficult to extract A_p using D_p. If the attacker wants to guess the password using A_p, then he has to guess three unknown parameters at a time.
- The objective of the protocol is to not use the password directly rather use it as a hash in login as well as authentication phases.

Proposition 2. *The proposed protocol is secure against offline identity guessing attack.*

Proof. An offline identity guessing attack occurs when an attacker attempts to deduce user identities by exploiting unauthorized access to sensitive identity information and posing risks to privacy and security. In our proposed protocol, we take three user inputs and as such like password even identity can be considered a candidate for guessing attacks. Just like password, it is a low entropy information.

- The parameter $D_p = H1(A_p \| B_p)$ can be used to guess ID_p, where $A_p = H1(ID_p \| PD_p)$. The threat actor cannot use A_p as it is hash-protected; however, if he tries to guess, he will have to guess ID_p and PD_p at the same time which is difficult to achieve in polynomial time.
- In the login message parameters, K_p and L_p are using ID_p, where $K_p = H1(ID_p \| R_a \| V_x \| T1 \| ID_h)$ and $L_p = ID_p \oplus H1(V_x)$. The parameter K_p is difficult to decode as it is hash-protected; however, trying to guess, it is also not feasible because of the random variables used in it but there is a slight probability, however, small it may be to find ID_p using L_p. All the attacker needs to know is V_x where V is random point in a vector and V_x is the x-coordinate of the same random point which is very difficult to find through guess work.

- In key agreement phase between patient and hospital private blockchain, the parameter K uses ID_p, which is protected by the hash function where $K = H1(ID_p \| R_a 0 \| V_y \| ID_h)$. Due to the non-existence of a inverse of a hash function, it is a herculean task for the attacker to find IDp using K.

Proposition 3. *The proposed protocol is secure against insider attack.*

Proof. An insider attack involves unauthorized or malicious activities perpetrated by individuals who have authorized access to sensitive systems or data, potentially compromising data integrity, confidentiality, and overall system security. An insider attack is the one where the user of the system tries to gain access to data he is not authorized with. It can be through gaining access to the administrator account using privilege escalation.

It is normal for a patient or another user to use passwords that are not that hard to crack even with the issued security guidelines. To mitigate this loophole, our proposed protocol can be efficient, as the user info such as password and identity are not used beyond login process. During the registration phase, $A_p = H1(ID_p \| PD_p)$ is sent over the private network.

Hence, it is very difficult for the attacker to extract password from A_p due to hardness of the hash function.

Proposition 4. *The proposed protocol is secure against user impersonation attack.*

Proof. A user impersonation attack involves an adversary fraudulently masquerading as an authorized user, gaining unauthorized access to sensitive resources, manipulating data, and posing threats to system integrity and security. User impersonation is the process where the attacker tries to act like the user to gain entry into the system. For this, he may need user credentials as such he may spy on the user (who he wants to impersonate) login activities.

$< G1; G2; K_p; L_p; M_p; T1; ID_h >$ where $K_p = H1(ID_p \| R_a \| V_x \| T1 \| ID_h)$ and $L_p = ID_p \oplus H1(V_x)$ and

$M_p = R_a \oplus H1(V_y)$

- To compute parameter G2 where the attacker needs to guess random variable R_a where $G2 = V + R_a * Z_{sa}$ and $G1 = R_a * Z_{sm}$. The attacker can generate G1 as Z_{sm} is public information and he only needs to guess R_a. However, the attacker may need to compute G1 which is very infeasible to calculate due to Elliptic curve discrete logarithm problem (ECDLP).
- Whereas, if the attacker targets parameter K, he needs valid $< ID_p, R_a, V_x >$. Similarly, the attacker needs $< V_x; ID_p >$ to compute parameter L_p, which already mentioned is a herculean task.

Thus, attacker cannot create a valid login message and is secure against this attack.

Proposition 5. *The proposed protocol is secure against blockchain miner impersonation attack*

Proof. A blockchain miner impersonation attack involves an adversary fraudulently assuming the identity of a legitimate miner in a blockchain network, aiming to exploit the system by controlling the mining process, tampering with transactions, or distorting the integrity of the blockchain ledger. And, like Proposition 4, the actor may attempt to impersonate as a valid consortium blockchain miner.

- It is possible if the attacker can compute valid message $< B1, B2, T_x >$ forwarded by the consortium blockchain to the miner, where $B1 = H1(ID_{cb} \| ID_{bm} \| R_{cb} \| T_x \| Y_{sm})$ and $B2 = R_{cb} \oplus H1(Y_{sm} * Z_{sm}) * ID_p)$
- To compute valid parameter Kv_2, the attacker needs valid ID_{cb}, Y_{sm} common key of the protocol K2 which is very difficult to calculate using protocol description. Further, the attacker will be hard bound to find a random number using public information due to hardness of XOR operation.

Hence, the proposed protocol is secure against the mentioned attack.

Proposition 6. *The proposed protocol is secure against man-in-the-middle (MITM) attack.*

Proof. It is very common in the security field to encounter malicious actors who intercept messages from the sender, modifies them, and forwards the modified message to the receiver. This is known as man-in-the-middle attack. In Proposition 4, we have already demonstrated that the protocol can withstand user impersonation attacks as well as the protocol provides strong protection against impersonation of the blockchain miners (as in Proposition 5).

Thus, we can conclude that the protocol will protect against man-in-the-middle attack as well.

Proposition 7. *The proposed protocol is secure against replay attack*

Proof. In replay attack, the attacker intercepts the message from the sender and forwards an identical message to the receiver.

No cryptographic mechanism is able to defend against a replay attack. To tackle the replay attack, we have used the timestamp verification technique. In our protocol,

when a certain entity such as patient, blockchain, or cloud receives a message, they first verify the timestamp, if they seem correct; then, the authenticity of the user is checked. As, in every phase of the protocol, we have implemented this technique; so, it is very difficult to execute the replay attack.

As the proposed protocol can foil replay attacks, it can even protect against DoS attacks as well.

Formal security analysis

In this section, we have performed a formal security analysis. For a formal security analysis, we have initially gone through two of the most common tools for inspecting our proposed protocol, namely AVISPA and Scyther. AVISPA was basically for automatically verifying any Internet security protocol. Scyther also has the same feature but with an added advantage of being the fastest among the two. Scyther is used when there are nonce's and sessions. Although Scyther poses many advantages, when it comes to Diffie–Hellman exponentiation, the tool has its limitations and, in that case, AVISPA would be an appropriate choice.[20]

Results and Discussion

Scyther being a user-friendly and easier to understand as its syntax looks very similar to that of C or Java. Though Scyther is case-sensitive, and it is known by the name of.spdl (security protocol description language), it requires the security protocols to provide claims else if no claims are provided, it automatically takes certain claims into considerations. After the protocol is converted into a proper.spdl code, we can press F1 or the verify option from the menu bar which will show the result that the protocol is attack-free or not. If any attack is possible, it will indicate beside the claim, which can be further clicked to find which attacks are possible. This is very useful to identify any security loopholes in the protocol, which can be considered and evaluated to build a secure protocol.

Figure 8a shows the initial setup code, Figure 8b shows the patient's role in Scyther, Figure 8c shows the CSM's role, and Figure 8d shows the consortium blockchain's role. The final results are shown in Figure 9.

Performance evaluation

This section deals with the computation cost and the communication cost of our protocol and comparisons of few related protocols. Our protocol is based on the latest cryptographic methods which is known to be the most secure in today's world. This type of cryptographic method is known as ECC that is based on algebraic elliptic curves based on finite fields.

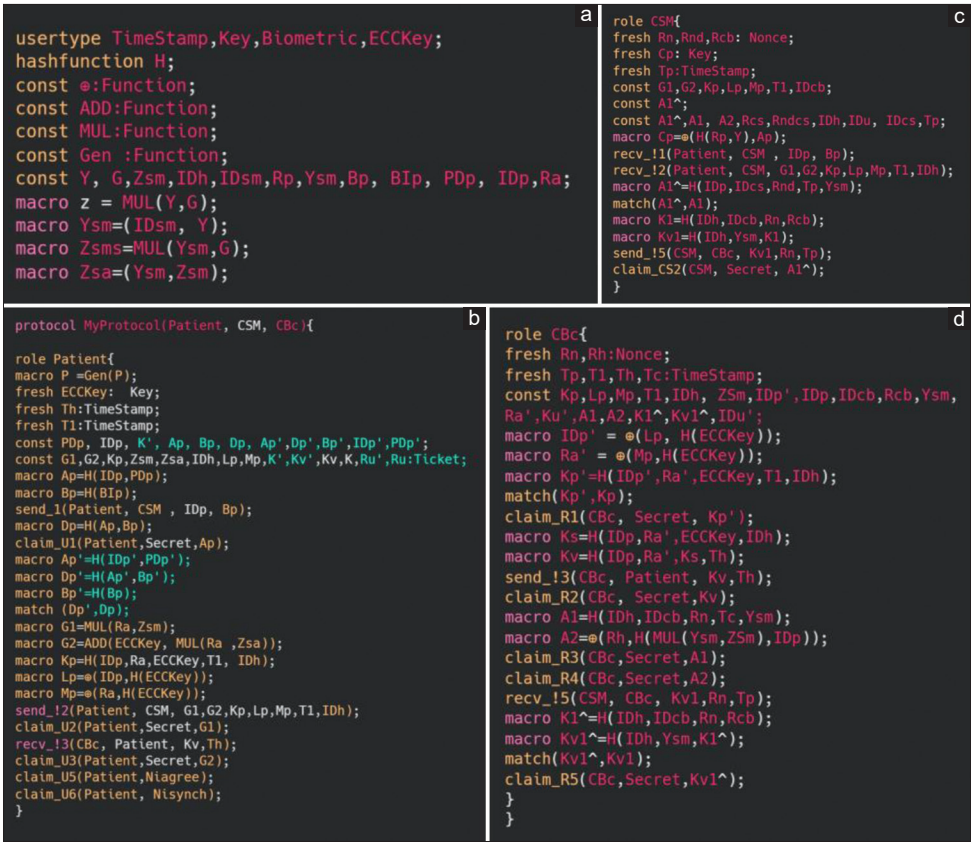

Figure 8: (a) Initial setup code, (b) patient's role in Scyther, (c) cloud system manager's role, and (d) consortium blockchain's role

As XOR operation and the concatenation operations take almost negligible amount of time, we have not considered them during our further cost calculations. We have taken each and every aspect of the model in very detail.

In Table 2, we have calculated the communication cost of our proposed protocol and compared it with that of other related schemes. We have again taken state-of-the-art uniform values[23] for all the functions taken into consideration while calculating the computation cost. We have taken user information T_u, hash functions T_h, timestamps T_c, and any type of symmetric encryption and decryption T_s. For calculating the total communication cost, we have to multiply the above parameters with 160. Practically, our proposed protocol has six steps; so, it should take some extra bits but at the same time it should be comparable with the related schemes. Figure 10 shows the graphical comparison of our protocol with the communication cost of the related schemes.

In Table 3, we have calculated the computation cost of our proposed protocol and compared the same with that of ours by taking a uniform state-of-the-art values[21] for different functions. We have taken hash functions T_h as 0.0005 sec, point multiplication T_m as 0.063075 sec, point addition T_a as 0.009 sec, and for any kind of symmetric encryption and decryption T_s as 0.0087 sec. Computation cost of our protocol takes the least time in seconds than the other protocol taken into considerations. Figure 11 demonstrates the graphical comparison of our proposed protocol with the computation cost of the related schemes.

Conclusion

In conclusion, our research has resulted in the development of a robust protocol that ensures secure storage and sharing of medical records through the integration of blockchain technology, patient biometric information, and robust cryptographic algorithms (ECC and AES). The protocol comprehensively addresses all aspects, including system setup, user registration, login mechanisms, key exchange between users and blockchain, inter-blockchain communication, and communication with multiple miners. To assess its performance, we conducted an evaluation that compared the protocol's communication and computation costs with existing blockchain-based schemes. Moreover, a thorough analysis of the protocol demonstrated its

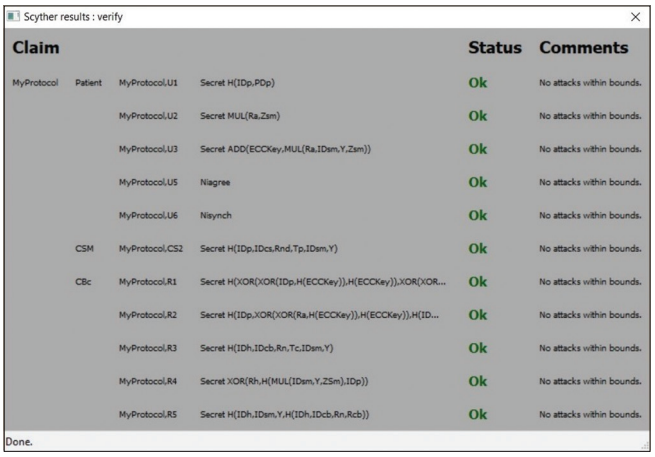

Figure 9: Scyther result

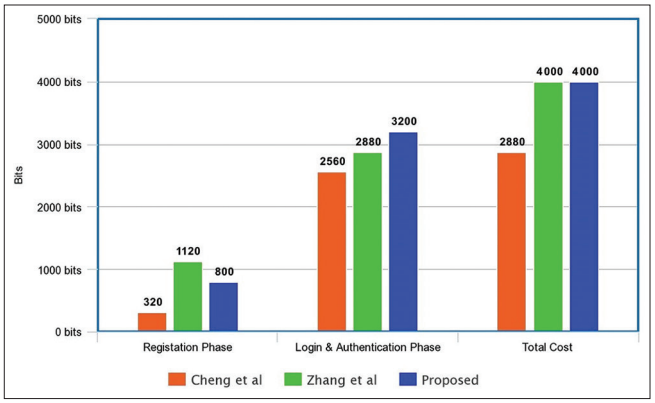

Figure 10: Communication cost comparison

Table 2: Communication cost (bits) comparison of the proposed scheme with the related Schemes

Schemes	Proposed Protocol	Ref. 16	Ref. 23
T1	$5T_h$	$7T_h$	$1T_h+1T_u$
T2	$13T_h+3T_u+4T_c$	$13T_h+2T_s$	$8T_h+5T_c+3T_s$
T3	$18T_h+3T_u+4T_c$	$23T_u+2T_s$	$9T_h+1T_u+5T_c+3T_s$
T4	4000	4000	2880

T1: communication cost for registration phase; T2: communication cost for login phase and authentication phase; T3: total communication cost for registration, login, and authentication phases; T4: total cost (×160)

Table 3: Computation cost comparison of the proposed scheme with the related schemes

Schemes	C1	C2	T_c
Proposed Protocol	$5T_h+3T_m$	$13T_h+5T_m+T_a$	$18T_h+5T_m+T_a$=0.333 seconds
Ref.[15]	$7T_h+5T_m$	$16T_h+5T_m+7T_a+T_s$	$23T_h+10T_m+7T_a+T_s$=0.721 seconds
Ref.[22]	T_h+3T_m	$8T_h+9T_m+2T_a+2T_s$	$9T_h+12T_m+2T_a+2T_s$=0.796 seconds

C1: registration phase; C2: login phase and authentication phase; TC: total computation cost

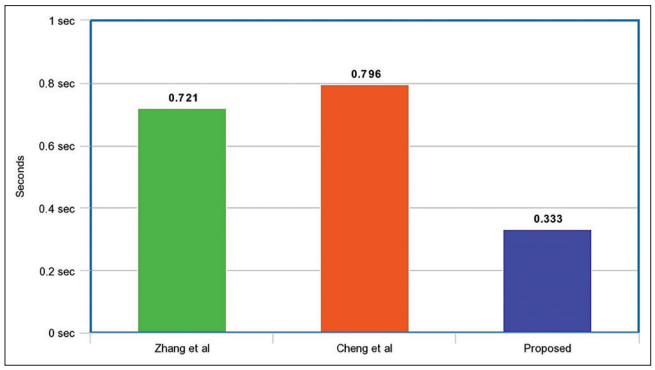

Figure 11: Computation cost

resilience against various attacks commonly encountered by medical institutions. We further validated the protocol's security by subjecting it to formal simulation using the Scyther tool, which confirmed its attack-free nature.

Based on our findings, we are confident in recommending the real-time implementation of this protocol in healthcare settings. By utilizing blockchain technology, patient biometric information, and robust cryptographic algorithms (ECC and AES), the protocol provides a secure framework for safeguarding sensitive medical data at every step of the process. Its comprehensive design and proven security measures make it a valuable solution for ensuring data integrity and privacy within the healthcare industry.

Ethical consideration

The study was obtained from Dr. Raj Raval Sir, Doctor, Gujarat, and Pulmonary and Critical Care Medicine, Ahmedabad, India, for their participation.

Acknowledgement

We thank the National Forensic Sciences University, Gandhinagar, NIT, Jamshedpur, and Indrashil University for the collaboration and support.

Financial support and sponsorship

Nil.

Conflicts of interest

There are no conflicts of interest.

References

1. Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. Decentralized business review. 2008.
2. Saha A, Amin R, Kunal S, Vollala S, Dwivedi SK. Review on "Blockchain technology based medical healthcare system with privacy issues". Secur Priv 2019;2:e83.
3. Esposito C, De Santis A, Tortora G, Chang H, Choo KK. Blockchain: A panacea for healthcare cloud-based data security and privacy? IEEE Cloud Comput 2018;5:31-7.
4. Dubovitskaya A, Xu Z, Ryu S, Schumacher M, Wang F. Secure and trustable electronic medical records sharing using blockchain. InAMIA annual symposium proceedings. American Medical Informatics Association 2017;2017:650.
5. Zhang A, Lin X. Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain. J Med Syst 2018;42:140.
6. Kaur H, Alam MA, Jameel R, Mourya AK, Chang V. A proposed solution and future direction for blockchain-based heterogeneous medicare data in cloud environment. Journal of medical systems. 2018;42:1-1.
7. Al Omar A, Rahman MS, Basu A, Kiyomoto S. Medibchain: A blockchain based privacy preserving platform for healthcare data. In: Security, Privacy, and Anonymity in Computation, Communication, and Storage: SpaCCS 2017 International Workshops, Guangzhou, China, December 12-15, 2017, Proceedings 10. Springer International Publishing; 2017. p. 534-43.
8. Li H, Zhu L, Shen M, Gao F, Tao X, Liu S. Blockchain-based data preservation system for medical data. J Med Syst 2018;42:1-3.
9. Fan K, Wang S, Ren Y, Li H, Yang Y. Medblock: Efficient and secure medical data sharing via blockchain. Journal of medical systems 2018;42:1-1.
10. Azaria A, Ekblaw A, Vieira T, Lippman A. Medrec: Using blockchain for medical data access and permission management. In: 2016 2nd international conference on open and big data (OBD). IEEE; 2016. p. 25-30.
11. Xia Q, Sifah EB, Smahi A, Amofa S, Zhang X. BBDS: Blockchain-based data sharing for electronic medical records in cloud environments. Information 2017;8:44.
12. Xia QI, Sifah EB, Asamoah KO, Gao J, Du X, Guizani M. MeDShare: Trust-less medical data sharing among cloud service providers via blockchain. IEEE Access 2017;5:14757-67.
13. Ji Y, Zhang J, Ma J, Yang C, Yao X. BMPLS: Blockchain-based multi-level privacy-preserving location sharing scheme for telecare medical information systems. J Med Syst 2018;42:1-3.
14. Zhou L, Wang L, Sun Y. MIStore: A blockchain-based medical insurance storage system. J Med Syst 2018;42:149.
15. Yang H, Yang B. A blockchain-based approach to the secure sharing of healthcare data. InProceedings of the norwegian information security conference. Oslo, Norway: Nisk J 2017. p. 100-111.
16. Uddin MA, Stranieri A, Gondal I, Balasubramanian V. A patient agent to manage blockchains for remote patient monitoring. Stud Health Technol Inform 2018;254:105-15.
17. Sun Y, Yan B, Yao Y, Yu J. DT-DPoS: A delegated proof of stake consensus algorithm with dynamic trust. Procedia Comput Sci 2021;187:371-6.
18. Assistance HC. Summary of the Hipaa Privacy Rule. Office for Civil Rights; 2003.
19. Bender D, Sartipi K. HL7 FHIR: An Agile and RESTful approach to healthcare information exchange. In: Proceedings of the 26th IEEE international symposium on computer-based medical systems. IEEE; 2013. p. 326-31.
20. Cremers CJ. The Scyther Tool: Verification, Falsification, and Analysis of Security Protocols: Tool Paper. International conference on computer aided verification. Berlin, Heidelberg: Springer Berlin Heidelberg 2008. p. 414-8.
21. Amin R, Kunal S, Saha A, Das D, Alamri A. CFSec: Password based secure communication protocol in cloud-fog environment. J Parallel Distrib Comput 2020;140:52-62.
22. Cheng X, Chen F, Xie D, Sun H, Huang C. Design of a secure medical data sharing scheme based on blockchain. J Med Syst 2020;44:52.
23. Amin R, Islam SH, Biswas GP, Khan MK, Kumar N. An efficient and practical smart card-based anonymity preserving user authentication scheme for TMIS using elliptic curve cryptography. J Med Syst 2015;39:1-8.