Journal of Information Systems Engineering and Management
2025, 10(18s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Blockchain-Based Secure Multiple Computation Scheme (Bsmpcs) for Preserving and Extraction of Health Care Data

B.Vasantha Rani [1], Dr.Parminder Singh [2]
[1] *Lovely Professional University, pagwara, Punjab; School Of Computer Science and Engineering*
Vignan Institute Of Engineering for Women; Department Of Information Technology
badagalavasantha06@gmail.com
[2]*Lovely Professional University, pagwara, Punjab; School Of Computer Science and Engineering*
Parminder.16479@lpu.co.in

ARTICLEINFO

Received: 21 Dec 2024

Revised: 31 Jan 2025

Accepted: 10 Feb 2025

ABSTRACT

Privacy protection for electronic health records is becoming an issue that the general public is becoming more and more interested in. The increasing use of virtual currencies like Bitcoin has led to the development of blockchain technology, which possesses the qualities of "decentralization" and "immutability." Current EHR management systems priorities safeguarding user privacy information above the security risks that occur when patients engage with several roles. As of right now, there is no sufficient solution to the problem of insurance companies accessing confidential patient information and violating their privacy. As the number of reported data breaches that threaten the current system rises, users' privacy is called into question because of personal data that third parties manage and obtain in large amounts. This study offers a block chain-based solution to all of the aforementioned problems. The paper proposes a blockchain-based framework to address privacy concerns in electronic health record systems. It specifically applies the decentralized, immutable qualities of blockchain to secure data against unauthorized access. The use of smart contracts for EHR management is relatively novel, as it allows interactions with insurance companies without exposing sensitive data. This contribution should highlight why smart contracts are better suited for this use case compared to existing mechanisms. The application of homomorphic encryption ensures that the system can process encrypted data without decrypting it. This allows computations (such as insurance claim verifications) to be performed on encrypted data, preserving privacy. The BSMPCS system is a new framework that could potentially combine these technologies into a unified solution. The paper should emphasize how this is different from existing EHR management systems and what makes it more secure and privacy-preserving. Using Bitcoin smart contract technology and homomorphic encryption, we create the feature with BSMPCS that allows the insurance company to decide whether to execute insurance requests even in the absence of a way to get the ID and the plaintext of the EHR. As a consequence, during communication, no private patient information would be revealed to uninvited parties, improving user data privacy and security.

Keywords: Healthcare,secret sharing, Multiple computation, smart contract, robustness, blockchain,,electronichealthrecords.

INTRODUCTION

The initial purpose of Secure Multiple Computation was to provide a decentralised solution to "The Millionaires' Problem." The two-party calculation was expanded to include many parties in the Goldreich et al. research [1]. A collaborative computing issue that safeguards privacy amongst a collection of untrusted individuals is solved using MPC. In this case, many parties with secret input want to compute a function together and get separate outputs. The intended outcome is the only information the participant receives throughout this process [2].

A variety of health-related data about individuals is collected in Electronic Healthcare Information (EHI). This data includes both medical information (diseases, prescription drugs, medical images, doctor names, hospital names, etc.) and person-specific information (social identity number, patient name, age, gender, address, etc.). Some

patients (individuals) in this data have sensitive values and choose to disclose their identities to the public. Therefore, safeguarding this private information from unwanted access while providing it to insurance companies and researchers is the healthcare system's most important responsibility. The conventional method of storing and managing this electronic medical data via a centralised system has the disadvantage that it is hard to guarantee the data integrity of the EHI. With its evolution, cloud storage has become a reliable third-party service provider for data storage and data transfer [3].

Single points of failure, vulnerability, and inadequate privacy and security characterise cloud-based data systems. Additionally, since third-party services are necessary for cloud-based data sharing, there is a greater chance of data theft, leakage, manipulation, or misuse[4]. While certain cloud-related problems have been resolved by prior cryptography and anonymity solutions, the single point of failure issue still cannot be resolved. On the other hand, access control for electronic health information is often centralised and based on roles. On the other hand, the role-based access control (RBAC) paradigm requires the definition of complex rules in order to restrict access for different types of data users[5]. The process of establishing and modifying rules is especially susceptible to an attack because of the centralised data storage, which might swiftly elevate privileges and get authorization for the whole dataset [6].

Distributed ledger technology, or blockchain, seeks to decentralize data storage while also making it more secure and impossible to mess with. Substituting it for centralized cloud storage solutions might be a smart move [7, 8]. Thanks to the smart contract function in the blockchain ecosystem, players from various organizations, such as policy makers, insurance corporations, and hospitals, may decentrally check requests for data access. To further simplify the setup of data access limitations based on user attributes, the ABAC (attribute-based access control) approach may be used.

To protect the confidentiality of electronic health record data, we propose BSMPCS, a blockchain-based substructure. Before being uploaded to the blockchain, the whole dataset is encrypted using the homomorphic encryption approach. Using this technique for comparisons and other operations only necessitates encryption; decryption is not necessary. On top of that, the owner will have the option to decode the encrypted text in order to get plain text from the generated output. Data that has to be sent between various organizations or in decentralized situations is best protected by this kind of encryption.

The paper is organized with background work in section two which refers how actually technology works and its application in the current work. Literature survey in section three. Proposed work in section four with methodology in section five followed by experiments and results in section six and finally conclusion.

2. BACKGROUND WORK

2.1 BLOCKCHAIN-BASED SECURE MULTIPLE COMPUTATION SCHEME

Many effective secure multiple computing techniques have now been suggested by researchers [5]–[8]. They have finished the secure multiple calculation for function, even in a lab setting [9]. Under the assumption of a semi-honest opponent model, the majority of this study focuses on increasing the efficiency of MPC as much as feasible. In other words, everyone involved in secure multiple computation is sincere; even the corrupted individuals who are targeted are only inquisitive; they merely use the observed message to examine the additional findings without going outside of the established protocol. Regretfully, the present circumstances do not align with this. In actuality, there are malevolent opponents that deliberately alter the protocol's execution in order to achieve the desired attack outcomes. Under the malicious adversary concept, there are also a few secure multiple computation techniques [10–13]. However, two things really continue to occur:

When one party receives findings that are more beneficial to him than to others, he won't disclose them, which prevents other parties from receiving the desired benefits. Attacks by hostile opponents are a persistent source of disruption to the protocol, preventing it from functioning properly. Therefore, in practice, a realistic MPC is also very desired to be resilient (a hostile adversary cannot conduct a "denial of service" against the protocol), fair (either all parties receive output or none), and efficient in addition to privacy[14].

2.2 SMART CONTRACT

A PC convention that meticulously works with, verifies, or executes the arrangement or execution of an agreement is known as a smart agreement. Astute contracts enable confidential conversations and agreements to be carried out between disparate, enigmatic groups without the need for a central authority, comprehensive body of

legislation, or external execution element [15–17]. They provide observable, uncomplicated, and irreversible ALGORITHMS for trades.

2.3 BITCOIN

The Bitcoin distributed computing platform allows users to access the chain and perform smart contract functions. The block chain is available to the public [8]. Each user has access to an authenticated account in order to conduct block chain transactions. All operations and transactions are recorded in terms of units of gas. Every petrol unit may be mined or bought with cryptocurrency. At the moment that a user triggers a transaction, the triggered transaction 's execution cost is added up.

$$PoT=(EC+T\ C)*P \quad (1)$$

Where PoT is the price of a transaction, EC is the Execution cost, TC is the Transaction constant is thepriceof 1gas unit.

2.4 IPFS

IPFS is both a convention and an organization designed to provide a common, substance-addressable method of storing and exchanging hypermedia inside a conveyed record framework [18]. This eats away at the material that it keeps inside the company. Identifiers are generated based on the content of the record, such as an archive, audio file, image, video, or other kind of stored data. The arrangement of these identifiers is merkle dag. PKI-based character is used by IPFS as an organizational model[19]. A programme that can locate, share, and replicate merkledag items is called an IPFS Node. A private key identifies its personality.

$$KeyGen \rightarrow PUKey, PRKey \quad (2)$$

$$NodeId=MultiHash(PUKey) \quad (3)$$

All hashes in IPFS are encoded with multihash, a self-portraying hash design. All IPFS hubs support sha2-256, sha-512, sha3 calculations. The created hash values ought to be deterministic, uncorrelated, special and one-way. The principle usefulness of IPFS relies upon the Content Identifiers which have the accompanying construction <cidv1>::=<multibase-prefix><cid-version><multicode-content-type><multihash-content-address>
where<multibase-prefix>is a code (1 or 2 bytes), to slide encoding CIDs into different squares. <cid-version>is a variant addressing the adaptation of CID for upgradability. <multicode-contenttype>is utilized to address the substance type or organization of the information being tended to<multihash-content-address> addresses the cryptographic hash of the substance being tended to in the arrangement base58(<variant hash work code><variant digest size in bytes><hash work output>).

3. RELATEDWORK

Blockchain technology offers a decentralized, immutable network where all nodes may verify transactions using smart contracts and consensus techniques. The blockchain has been employed by a number of healthcare systems [25, 26] because it is a trustworthy way to increase communication security and privacy.

Authors have used smart contracts in [27] to create a system that allows for remote patient monitoring and emergency notifications to medical professionals. Through blockchain, this remote monitoring system ensures the patient's protection and privacy[20]. There are three actors and three functions in the suggested system. The platform's patient and physician registration process is its primary use. They use a smartphone to access it and securely register personal information like name, age, and ID. They are also able to review and amend these records. Data from the IoT sensor will be processed for patient monitoring, and smart contracts on the blockchain will store the processed data. It is now simpler for physicians to monitor their patients in real time thanks to this step. The business and the medical gadgets are the subject of the final function. A smart contract is made between the patient and the corporation at the time of purchase to register the device in his name. The patient's data that the IoT instrument obtained is therefore recorded in the care facility[21–24].

The authors of the study [28] use the concepts of smart contracts and multi-agent systems to oversee and manage pharmaceutical logistics operations. They provide a framework that enables transactions between the various system participants to be stored on the blockchain. These transactions are managed via smart contracts, independent of any other party. As a result, the system is less costly and delivers information more quickly. But in order to assess its effectiveness and performance, a working prototype must be created concurrently with empirical

validation. Gilad Asharov et al. study game theory and safe two-party computation [6]. When a safe two-party system is transformed into a computation protocol, it preserves two sides' privacy, nash equilibrium, accuracy, and security[29].

The stated RMPC is reliant on game theory, which addresses MPC fairness but falls short in addressing robustness issues. The MPC protocols are expressly engineered to provide near-fairness and include a decentralized trusted third-party system, both of which are absent in real-world settings. As a result of the growing demand for block chain technology, which is embodied by Bit Coin [7], Bit Coin's incentive mechanism became inseparable from Game Theory, and academics started incorporating Bit Coin's fail-safe mechanisms into MPC economics. It gives parties a great incentive to take part in MPC processes. Based on the Bit coin network, Marcin Andrychowicz et al.'s work [8], [9] offered a safe two-party lottery mechanism. The parties get economic remuneration in the form of Bit currency or the product.

Multiple rounds of communication with the Bit coin network are required for the startup procedure. Several functions, such as the claim-or-refund functionality, the t (secure computation with penalties functionality), and the q (secure lottery with penalties functionality), were shown by Iddo Bentov and Ranjit Kumaresan [10]. They created the MPC protocol, which requires calling a continuous round. FCR Iddo Bentov and Ranjit Kumaresan conducted more study on using Bit Coin to inspire patients.

obtaining the accurate calculations [11]. Four unique features are included into the work: verifiable computation, fair secure computation, non-interactive reward, and secure computation with limited leakage.

Bit coin is beneficial for building a decentralized poker game, as explained by Ranjit Kumaresan et al. [12]. In 2017, he once again put up an enhanced plan to achieve favorable outcomes.[13]. He discussed the optimization process in this technique to produce a safe computational model. Many of the scientists looked at the bit coin concept in order to fulfil the criteria. To ensure the protocol's resilience, accuracy, and fairness, they made complete changes to the framework. Although there are several implementation restrictions for bit coins and block chains in the real world, scientists' evolving tactics provide successful outcomes in real-world situations. Due to the incompleteness of BitCoin's scripting language, it is limited in its ability to enable complicated tasks that are intricate and challenging to implement. These tactics work well in theory, but they are not recommended for the bit coin's implementation stage.

Global ledger-based multi-party computing protocol developed by A. Kiayias et al. [14]. Three elements are included in their work: 1) UC-Secure; 2) a constant-round resilient multi-party computing protocol; and 3) a frame model to secure multi-party computation with compensation. We developed a novel ideal function for a fair and robust multi-party computing in this study, which we refer to as FRMPC (fair and robust multi-party computation). Then, in order to achieve our objectives of robustness and fairness, an outsourced MPC scheme based on the EOS block chain was put forward. Nowadays, almost all of the top businesses choose and use the OAuth protocol [15] for their proprietary authentication, which functions as a reliable and trustworthy authority. Many researchers have put forward different methods to secure personal data from a security standpoint. Sensitive data in these anonymized datasets has to be protected. Every record at this location can be distinguished from at least k-1 other records [16]. A sufficiently wide range of feasible values of k-anonymity 1-diversity is used to represent the sensitive data. These methods are widely utilised nowadays to show how data sets are employed in our study [19], [20].

Numerous privacy-preserving techniques have differences that cause data exchange to be disrupted [21], and there are questions about how to compute encrypted data. One such method is called Fully Homomorphism Encryption, or FHE for short.[22]. This method's use over encrypted data has a special quality. Although it may be effective in tackling real-world problems, it also has certain drawbacks. Thus, a plethora of alternative methods, such as accountable systems, have been developed as a remedy for this problem. It can safely transmit Bit Coin money between users without requiring a centralised system. Additionally, it has an open ledger and public verification capability. As block chain regulators, all projects are adopting this bit coin 2.0 together. We can accomplish trusted audibility with trusted functions by putting this into practice. Transparency, security, and effective, secure data are the outcomes.

The BiiMed platform was recommended by the authors of [31]. This strategy aims to distribute the patient's electronic health record across many parties. Data interoperability and integrity are provided via the blockchain. The BiiMed blockchain and the health information system (HIS) make up the two halves of the proposed

architecture. Medical data is gathered, stored, and disseminated by the HIS, and shared data is maintained via the BiiMed platform [33]. It is based on smart contracts and the Bitcoin blockchain. Data integrity and interoperability are essential components of electronic medical record interchange. These attributes are guaranteed by the technology built on a decentralized trustworthy network.

4. PROPOSED SYSTEM

The platform that the proposed system, BSMPCS, uses to facilitate the sharing and exchange of patient medical data. Multi-agent systems and blockchain technologies are combined in this approach. Smart contracts and access control (ABAC and RBAC) are used to guarantee the security of the data that is altered by many stakeholders [34–37]. A few conditions must also be met by the system. The identification of those authorized to take part in the electronic medical record management procedure in the blockchain-based healthcare system has to be confirmed. In fact, in order to access resources, participants must verify themselves. Every participant also has a predetermined role in the way the patient file is processed. Actually, all of the resources people need to do their duties are available to them. Scalability is important because of the massive amounts of data that are transferred in the healthcare industry and the way the network grows with each new user. An electronic medical record system should have a flexible user interface that makes resource use simple and effective for all users in order for them to gain from the necessary medical data service. The CIA trifecta (confidentiality, integrity, availability) must be met by the application. To guarantee correctness and dependability, patient data must be shielded against viewing and any unauthorized access or change. Those with authorization who need it may also access it.

As shown in Figure 1 and the EMR system, several agents communicate with one another to share information. They make requests for or supply health information using a web application. They need to authenticate in order to access it. The automated and secure part of this transfer is added by the smart contract, depending on the kind of user. The relevant interface then displays the data that have been recorded on the blockchain. In order to protect patient data from assaults, we attempt to give each user an access role because of the blockchain's transparency and immutability.

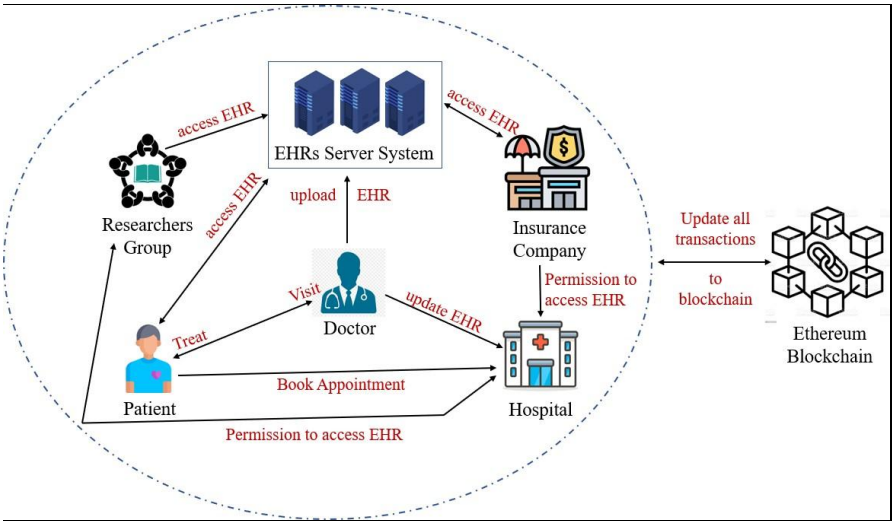

Figure 1 :EHR Privacy Model in Blockchain Model architecture

As shown in figure 1, the entities of our EHR Privacy Model on Blockchain include patients, physicians, insurance companies, research groups, and hospitals. A patient's duties include updating the system with his medical information. The only legitimate form of identification the patient has is his Aadhar card, which is immediately connected to all the information he updates. A doctor's duties include making sure the patients they have registered are being treated[38.39]. The physician obtains authorization to see the patient information stored in the hospital module. The physician establishes a treatment ID for the patient after reviewing the patient's medical data. He administers the precautions to the patient while also keeping an eye on them. The patient information that was registered for insurance is kept up to date by the insurance company. They keep records of information divided into categories, such as drugs that are covered by insurance and those that are not.

As shown in picture 2, The patient compiles all of his medical documents. He creates digitised versions of the medical records. The EHRs are transformed into encoded data. The encoded EHR is created by assembling the encoded components. The blockchain has been updated for these encoded EHRs. The doctor obtains authorization to see the patient's information. The physician generates a treatment ID for further care after reviewing the patient's electronic health record. The patient receives the prescription from the doctor after receiving treatment. The prescription reports are also prepared by the doctor and sent to the insurance company so that they may be included in the database's list of prescribed drugs. The blockchain has been updated with the files in 8 and 9. The doctor sends the papers to the insurance company. In order for patients to register with them, they update the terms and conditions and medication files. The patients sign up with the insurance provider on their own. They produce the medical records that are linked to insurance. The blockchain is updated with these entries. To access the EHRs, the research team asks authorization from the hospital. RG secures the necessary authorizations to carry out different types of analysis on the EHRs.

In order to provide predictions and outcomes, RG analyses and evaluates the EHRs in a variety of ways. All of the produced forecasts and outcomes are updated on the blockchain. The hospital keeps an eye on other organizations and has the authority to grant or revoke them access to patient privacy-protected data.

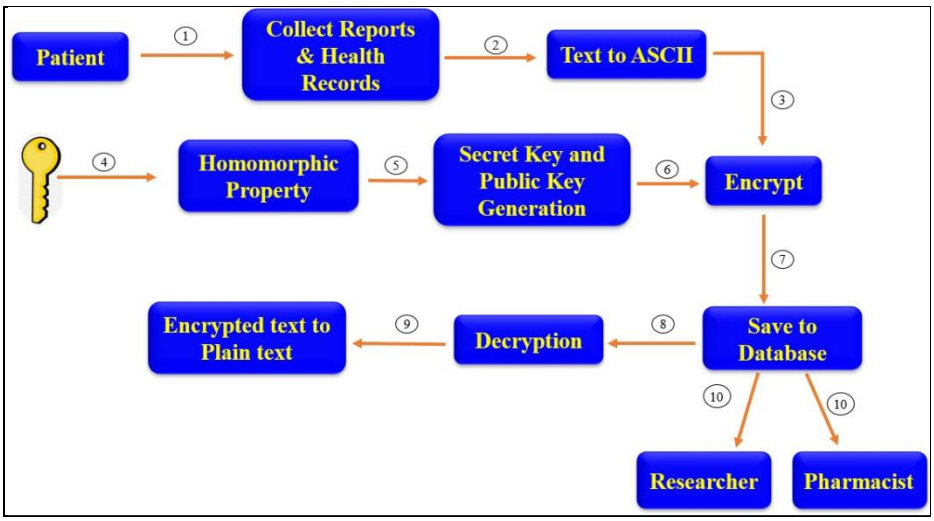

Figure 2: Flow of HomomorphicEncryption process in EHR-PP model

5. METHODOLOGIES

5.1 Homomorphic encryption

The algorithm used for performing homomorphic encryption is “ElGamal”. “In the ElGamal cryptosystem, a cyclic group G of order q with generator g, if the public key is (G, q, g, h), where $h = gx$, and x is the secret key, then the encryption of a message m $\mathcal{E}(m) = (gr, m, hr)$ for some random $r\{0, \dots, q - 1\}$. The homomorphic property is then”

$$\mathcal{E}(m_1) .\mathcal{E}(m_2) = (g^{r}{}_1 ,m_1 .h^{r}{}_1)(g^{r}{}_2,m_2.h^{r}{}_2)= (g^{r}{}_1{}^{+r}{}_2 ,(m_1 .m_2)h^{r}{}_1{}^{+r}{}_2)= \mathcal{E}(m_1 .m_2) \quad (4)$$

$$Y=g^{x} \text{ (mod p)} \quad (5)$$

His public key is(Y,g,p)andhewill send thisto Alice. Alicethencreates amessage(M)andselects a random value (k). She then computes a and g

$$a= g^{k} \text{ (mod p)} \quad (6)$$

$$b = y^{k}M \text{ (mod p)} \quad (7)$$

both then receives these and decrypts with:

$$M=\frac{b}{a}^{x} \text{ (mod p)} \quad (8)$$

This works because $\frac{b}{a^z}(\text{mod } p) = \frac{y^k M}{(g^k)^x}(\text{mod } p) = \frac{(g^z)^k M}{(g^k)^x}(\text{mod } p) == \frac{g^{zk} M}{g^{zk}}(\text{mod } p) = M$ (9)

If we have:

$a_1 = g^{k_1} (\text{mod } p)$ (10)

$a_2 = g^{k_2} (\text{mod } p)$ (11)

$b_1 = y^k M_1 (\text{mod } p)$ (12)

$b_2 = y^k M_2 (\text{mod } p)$ (13)

then we get

$a = a_1 \times a_2 = g^{k_1} \times g^{k_2} = g^{k_1 + k_2}$ (14)

$b = b_1 \times b_2 = y^k M_1 \times y^k M_2$

$$M = \frac{b}{a^x} = \frac{y^k M_1 \times y^k M_2}{g^{k_1 + k_2 z}} \quad (15)$$

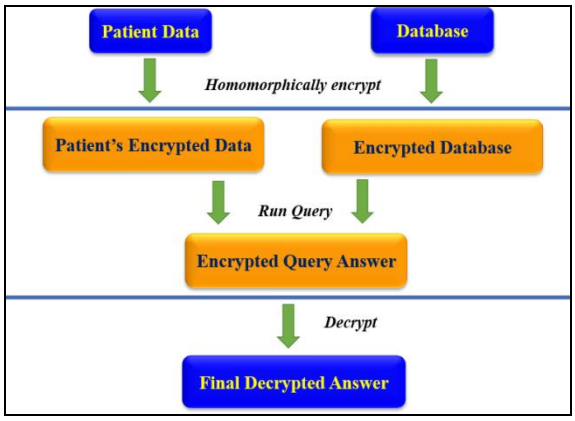

Figure 3: Homomorphic Encryption process in EHR-PP model

5.2 Psudeo Algorithm for Registering Patients

This smart contract is responsible for registering the patients, fetching details of patients and updating the precautions of patientsto the blockchain.

1. Begin

2. P_details [] ← Read patient's details (Aadhar number, Name, address, phone number, blood group, insurance company, emergency contact)

3. if (P_details[aadharnumber].isValid()) then

4. if(P_details[aadharnumber].isAlreadyRegistered) then

5. Display("User already registered")

6. Else

7. Add details to blockchain

8. Else

9. Display (“Please enter valid user details”)

10. End

This function fetches the Aadhar card number of the patient an checks whether he is registered.If the user is patient and already registered then the details will get updated.

5.3 Pseudo Algorithm for Insurance & Medications

This contract’s responsibility is to maintain the data of the patients who registered for insurance. They also maintain the data of medications that are covered under insurance claim. If any necessary medications were not covered in the list formulated earlier, authorized doctors are given permissions to add the necessary medications to the insurance company data. This function takes in input of medication details. It checks whether the entered medications are covered under insurance or not.

1. Begin

2. Company_details [] ← fetch(company id, name, phone number)

3. If (Company details[id].isNotRegistered) then

4. Add company details to blockchain

5. Else

6. Display (“ID already registered. Please enter a new ID”)

7. End

Medications

1. Begin

2. Medication [] ← fetch(Medication details)

3. UADDRESS←fetch (User Address)

4. if (UADDRESS.isInsuranceCompany) then

5. Medic [] ← fetch (stored medication details)

6. If (Medic. Exists (Medication)) then

7. Display (“Medications not covered under insurance”)

8. Else

9. Display(“Medication covered under insurance”)

10. Else

11. Display (“Only insurance company can do this operation”)

12. End

5.4 Pseudo Algorithm for claim for insurance

This function takes in input of patient’s aadhar card number. It checks whether the entered aadhar number has already claimed for insurance or not.

1. Begin

2. Medication [] ← fetch (Medication details)

3. UADDRESS ← fetch (User Address)

4. if (UADDRESS.isInsuranceCompany) then

5. Medic [] ← fetch (stored medication details)

6. If (Medic. Exists (Medication)) then

7. Display (“Medications not covered under insurance”)

8. Else

9. Display (“Medication covered under insurance”)

10. Else

11. Display (“Only insurance company can do this operation”)

12. End

5.5 Pseudo Algorithm for Doctor

This contract takes care of all the operations performed by the doctor. First a doctor has to register himself with the system in order to perform any operation. The doctor requests permissions for accessing the patient’s medical data. After receiving the required permissions, the doctor creates a treatment id for the patient, treats him and then uploads the prescription & the bill to the blockchain. He also sends a copy of the medication details that are not covered in insurance company’s details to the insurance company for addition.

1.Begin

2. UserDetails [] ← fetch (user details)

3. UADDRESS ← fetch (User Address)

4. if (UADDRESS.isAlreadyRegistered) then

5. Display (“user already registered”)

6. Else

7. Register doctor details to the blockchain

8. End

5.6 Pseudo Algorithm for accessing the Patients data for treatment

This function reads the patient’s Aadhar card number. It creates an OTP for the entered aadhar card number, using which doctor can access the patient’s medical records.

1. Begin

2. Paadhar ← fetch (Aadhar details of the patient)

3. UADDRESS ← fetch (User Address)

4. If (UADDRESS.isDoctor) then

5. OTP ← keccak256 (Paadhar)

6. Update OTP to blockchain

7. Else

8. Display (“Only doctor can get access permissions to patient”)

9. End

5.7 Pseudo Algorithm for treatment and insurance

1. Begin

2. UADDRESS ← fetch (User Address)

3. if (UADDRESS.isDoctor) then

4. Tid ← ((142317 * Paadhar)%1000003)

5. Else

6. Display (“Only doctor can create a treatment id”)

7. End

5.8 Pseudo Algorithm for treating a patient

This function takes in input of patient’s Aadhar card number. It checks whether the entered Aadhar number has already claimed for insurance or not.

1. Begin

2. UADDRESS ← fetch (User Address)

3. if (UADDRESS.isDoctor) then

4. PatientDetails [] ← fetch (stored patients details)

5. If (PatientDetails.Exists) then

6. Prescription ← Create (prescription, bill)

7. PatientDetails.add (Prescription)

8. Display (“Prescription and bill updated to patient”)

9. Update blockchain

10. Else

11. Display (“Register the patient first”)

12. Else

13. Display (“Only doctor can treat a patient”)

14. End

The following modules make up the MPS (multiple computation scheme) Contract, and the following is a detailed description of each module's functions:

1) Register: To become an MPS node, a participant must first register under this contract and pay a minimum deposit. Only once this is done will the participant be eligible to be chosen by the users to provide computing services in exchange for money.

2) Reputation System: According to this contract, every MPS node has a reputation value. The reputation value of the MPS node will rise if it cooperates and does the calculation work successfully; if not, it will fall. The MPS nodes' long-term usefulness is determined by their reputation value.

3) Incentive Mechanism: The MPS node receives revenue from two sources: the price charged to users who use the service, and the penalty imposed on dishonest MPS nodes. The allocation of rewards after the completion of each service is a reflection of the real usefulness of MPS nodes, as determined by the Incentive Mechanism.

4) Choose Quorum: In order to complete the present calculation work, users may choose a quorum of MPS nodes based on their reputation scores and deposit amounts. A low reputation does not guarantee selection, but the likelihood will drop very rapidly as the reputation value drops. The poor players should be given another

opportunity to make up for their previous actions. We must also take a newbie into account. This is in line with what is really true.

5.9 Compute contract

Users that need the multi-party computing service negotiate and implement Compute Contracts into the blockchain network. The Compute Contract contains information about the MPS settings for the present calculation work, the computation scripts for each MPS node that has been chosen, etc. The calculation is done in rounds; each round has a time restriction that participants (Users or MPS Nodes) must accurately provide the data that has to be added to the blockchain during that round. The accuracy of the given data will be confirmed by the smart contract. The smart contract will also determine which member failed to provide the right message at the start of the next round. The blockchain will then decide whether or not the computation may continue. This time restriction may represent the future height of a certain block. To get a quorum of MPS nodes taking part in the present calculation work, it will submit a transaction to MPS Contract in the first phase. Using this contract, users broadcast their shares encrypted using the MPS nodes' public key in the first round and deposit the charge fee. Between the second and penultimate rounds, the MPS nodes broadcast the worthless intermediate value created during the calculation in the same manner. MPS nodes declare and collect fees for their respective production shares in the final round. This contract is a reliable broadcast channel from this angle. This is comparable to the synchronous broadcast channel in some ways.

5.10 MPS protocol

We may make use of some research on current multi-party protocols based on contracts in this section [40]–[42]. Our primary concerns in this research are MPS robustness and fairness. It is beyond the purview of this study to discuss how to build a secure MPS protocol using contracts. The parties calculate hidden shares of the function f's outputs or a pointless intermediate value, as stated in [22]. Thus, upon the completion of each round in the BSMPSS, users and MPS nodes will broadcast the shares to the blockchain. The blockchain platform's Smart Contract automatically executes rewards or punishments. At the conclusion of every cycle, what the Users and MPS nodes must do.

5.11 Fairness & robustness analysis

Blockchain technology and (t, n)-threshold contracts form the foundation of BSMPSS, which operates in rounds. Time stamps on a blockchain may make it possible for protocols to run synchronously. The Smart Contract will identify and eliminate any player who sends an improper message outside of the protocol at the start of the next round. All of this operates automatically in a blockchain context and is visible to the public. This is not feasible in earlier work when there isn't a centralised node. On the blockchain, every member has a unique account and

matching key pairs, making identity theft impossible. The following features primarily demonstrate BSMPSS's robustness:

a) Setup Phase: Each participant's reputation value is publicly maintained by the ledger based on their previous actions. To make selection easier, individuals must build up their reputation values over an extended period of time. In order to prevent "The Sybil Attack," a deposit is required in the contract in order to become an MPS node. In other words, the attacker cannot add additional nodes to break the protocol. The phase may be repeated and a new subset can be chosen to begin with if the procedure is aborted.

b) Phase of Input: When submitting the input, users must pay a certain quantity of coins as the service charge for the current job. The accuracy of the user's input will be verified by the smart contract. The service fee will be charged to the truthful Users if they fail to provide the accurate input within the allotted period. The service price will allow the programme to withstand denial-of-service assaults from users.

c) Compute Phase: The Smart Contract also detects the MPS node's intermediate value. If a valid message is not provided, the node will be transferred to the corruption set at the start of the next round. The protocol will be finalised as long as the number of corrupt participants is less than or equal to n-t.

In conclusion, the Smart Contract will identify any BSMPSS participant who violates the protocol and will prevent them from taking part in the subsequent task. The plan makes use of a (t, n)-theshold secret share, which provides some fault tolerance as long as an appropriate t is specified. Users may choose a new subset to resume the agreement even in the event that the protocol is terminated. As a result, BSMPSS is resilient.

6. EXPERIMENT & EVALUATION

All things considered, there are six parts to the implementation: IPFS Storage, the insurance company, the pharmacist, the blockchain network, the patient, and the doctor. A Java prototype has been constructed using Geth, which is used to build blockchain technology. The source code for both programs is freely accessible online. Due to the need for on-chain storage space in the blockchain, the CID value (hash value) is kept in the blockchain after being extracted from IPFS version 4, and all of the reports are recorded in IPFS version 4. A network has been established up using IPFS version 4. The computers include Intel Core i5 7th Gen processors with (i) 8 GB RAM and 500 GB local storage based on Windows x64, and (ii) 6 GB RAM and 500 GB local storage based on Ubuntu 16 processors.

It is a well-known fact that the average block creation time of the chosen blockchain determines the computational efficiency of all blockchain-based schemes. For instance, a Bitcoin transaction typically takes ten minutes to execute. The EOS blockchain platform is selected by BSMPCS. BFTDPoS, the current EOS consensus process, can

reliably produce a block every 0.5 seconds. All MPC Contract and Compute Contract activities in BSMPCS are carried out on a chain.

The primary time burden associated with off-chain execution in each round is the PVSS data distribution procedure, which involves sharing the Shamir's secret and carrying out several asymmetric encryption operations. For MPC nodes that choose to take part in the present compute work during the ComputeContract Init phase, their execution duration is mostly determined by the size of the quorum.

We may deduce that, for a given set of MPC nodes in Compute Contract, the cost of time for a BSMPCS round grows exponentially as the size of the quorum rises. This is so that additional asymmetric encryption computations may be performed during each round of computation as MPC nodes are added to a particular workload. Worse, in order to enable secret sharing, a higher power polynomial is required, which means that more bytes are used in the created shares, increasing the size and time required for the asymmetric encryption of the data. We may see that users choosing more MPC nodes to complete a compute work for greater privacy would result in a significant loss of efficiency when the quorum surpasses 40.

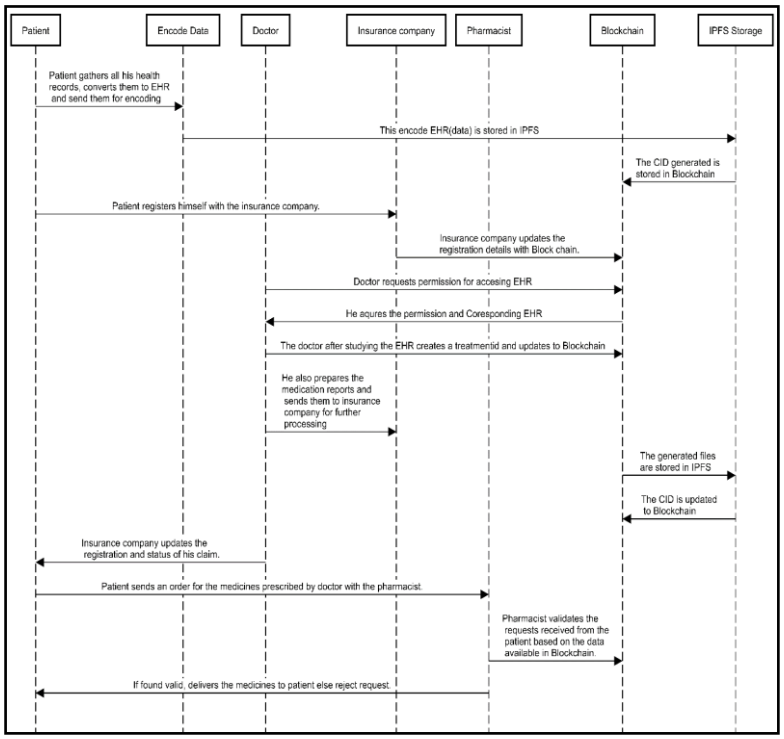

Figure 4: Sequence diagram for EHR report in Healthcare System

This module is in charge of compiling their medical records and forwarding them to the data encoder so that the plain text may be changed to encoded language. These files will eventually be updated to the blockchain and transferred to the IPFS storage system. The upload and download times for various sizes are shown in Fig. 5. The graphs show that the computational cost of uploading a transaction is higher than that of downloading it.

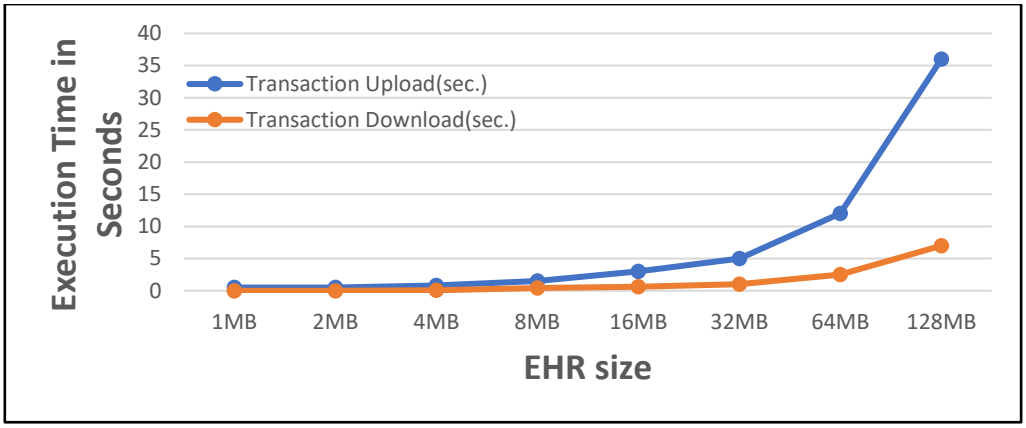

Figure 5: Transaction Upload and Download Execution Time

a) Doctor: When a patient registers with the system, the request is sent to a related doctor. To access the data, he obtains authorization from the blockchain network. In addition, he generates a treatment ID for the ongoing procedure. In addition to recommending certain medications and testing, the doctor uploads the information to the blockchain.

b) Insurance Company: The patients, hospital, and blockchain network are all covered in this module. Depending on the kind of issue and emergency found, the patients register with the insurance provider. The hospital and the doctor confirm the information with the insurance company. If the request is determined to be legitimate, the patient's claim is rejected; otherwise, the information is processed and money is awarded to the patient.

c) Pharmacist: Patients may place online orders for medications from the pharmacy after obtaining prescriptions from their doctors. The blockchain will be updated with the same.

d) IPFS Storage: The peers in the network store all of the reports in IPFS. Every file has a Content Identifier created for it when the reports are uploaded. This serves as a point of reference for network file access. In the blockchain, this produced Content Identifier value will be kept.

e) Blockchain Network: To verify transactions submitted by different participating entities and to construct a block, this module really implements the consensus procedures. A number of blocks containing the data from the participating entities—such as patient and doctor IDs, treatment IDs, insurance company details, etc.—will be formed during the mining process. The observation is that the mining process takes longer than the block creation process. This may be seen in fig. 6.

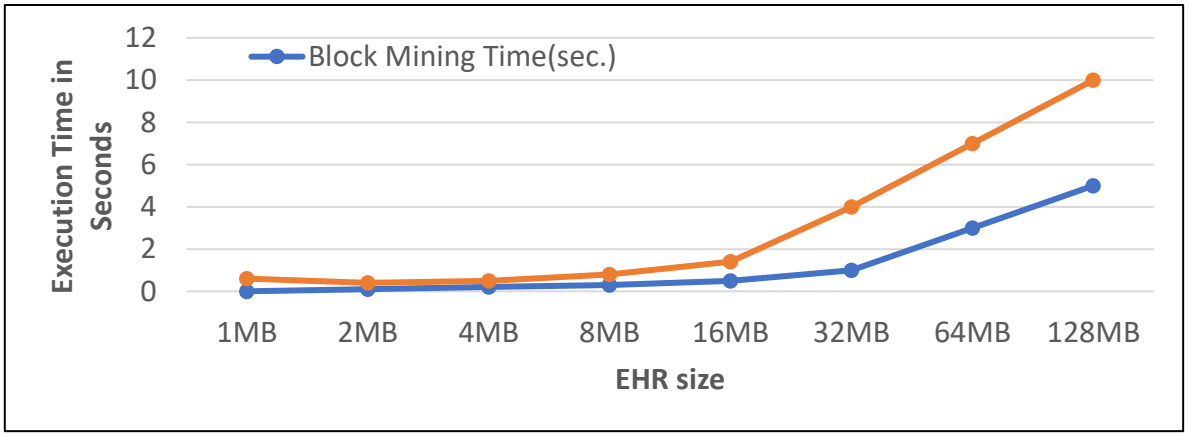

Figure 6: Execution Time for Block Mining and Block Creation

Fig. 7 shows the time it takes peers to access (availability) a transaction for a range of report sizes. It seems sense that the access time would rise as the report's size rose. Furthermore, a transaction takes longer to complete the more peers participate.

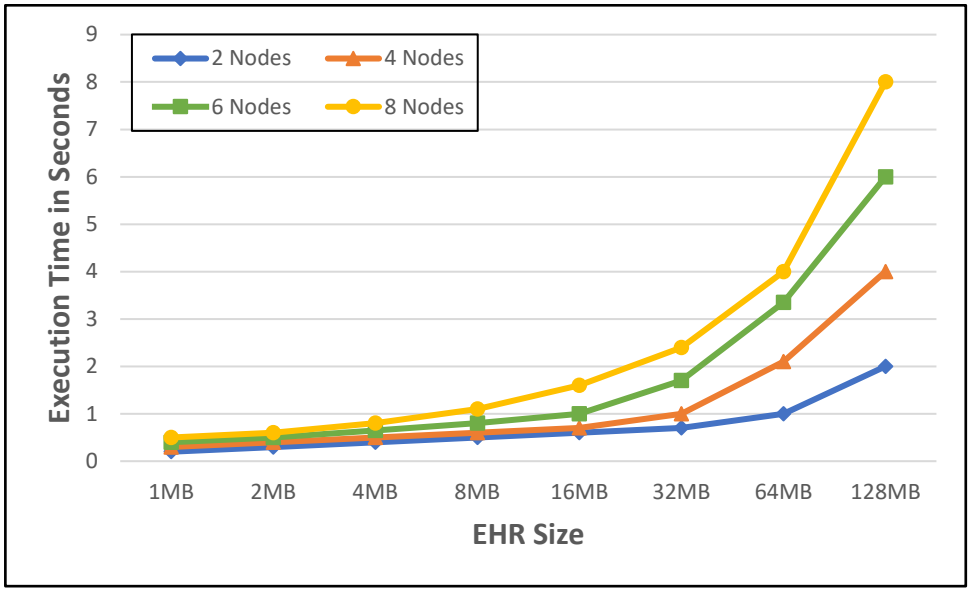

Figure 7: Running Time for Transaction Access by Number of nodes

Comparing the performance of the proposed framework with seven other existing schemes for protecting the privacy of Health Record Information systems is the focus of this section. The schemes include Azaria et al. [26], Omar et al. [24], Li et al. [25], Fan et al. [27], Zhang et al. [28], Shen et al. [29], and Uddin et al. [30]. Seven benchmark privacy and security attributes are taken into consideration in our suggested framework, as shown in the table.

The chart indicates that our suggested architecture has succeeded in achieving both security and privacy features. Notably, our suggested architecture offers the best means of protecting patient privacy and HER security in terms of tamper-proofing, data privacy protection, patient privacy preservation, access control, non-repudiation, access revocation, and block search.

Table 1: Metrics

S.No	Metrics	[J]	[F]	[G]	[K]	[L]	[M]	[N]	Proposed Scheme
1	Tamper – Proof	√	√	√	√	√	√	√	√
2	Privacy Preserving of Patient	×	√	×	√	×	×	×	√
3	Data Privacy(Confidentiality)	×	√	×	×	×	×	×	√
4	Access Control	√	×	×	×	√	√	√	√
5	Non – Repudiation	√	√	√	√	√	√	√	√
6	Access Revocation	×	×	×	×	√	×	√	√
7	Block Search	√	×	×	√	√	√	√	√

6.2 Evaluation

Patients' electronic health records are securely and safely maintained by this application. It includes modules for every aspect of an electronic health care system, including those for physicians, patients, the research team, hospitals, and insurance providers. Ensuring the privacy of data collected and kept in the EHR system is the primary goal of this system. Additionally, the EHR Privacy Model in Blockchain is focused on avoiding data tampering, unauthorised change, and general support for an online electronic health care system. This system uses homomorphic encryption and a novel technology known as blockchain technology to provide data security and

privacy. The smart contracts handle granting permission for data access, other modules, and collaborating entities.

A prototype of the intended system was put into place in order to assess the system's functionality and the degree of privacy and security achieved for the data kept therein. We used the Ethereum blockchain platform, go-Ethereum, version 7.5.4 of npm, and node version 15.8.0 to implement the prototype. Versions 5.1.66 and 6.12.2 of the Solidity Framework and IDE are used to deploy smart contracts, respectively, while version 0.8.1 of the Solidity scripting language is used to develop the contracts. The version of web3js that handles queries between Ethereum [2] nodes is v1.2.0.Six workstations were used to install the blockchain node; each has an Intel CPU with a 2.30GHz core and 8 GB of main memory. A few nodes were set up in different settings, such as Windows 10 and Ubuntu 16. Version 13.2 of Java is utilised to implement the

the encryption and decryption modules of the HME process in the EHR-PP paradigm, and Notepad++ is the editor of choice.

On receiving the search word “Fever” the HME algorithm performs encryption andgeneratesthecode“4zLE9”.Now this encrypted keyword is searched and matched with the values that are already encrypted and stored in the database.

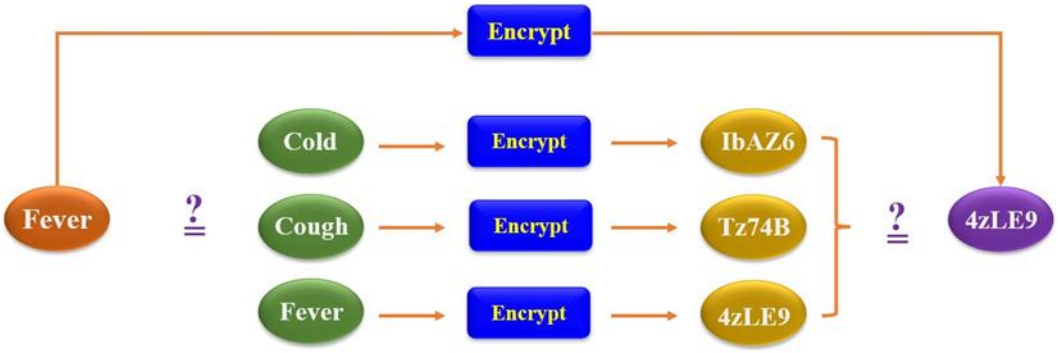

Figure 8: HME working mechanism

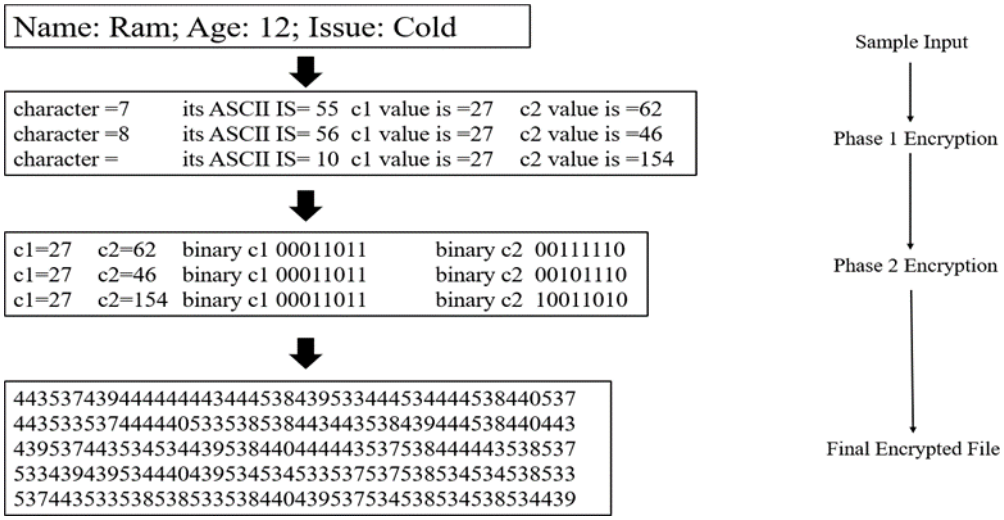

Figure9: Encryptionprocess inElGamalEncryptionAlgorithm

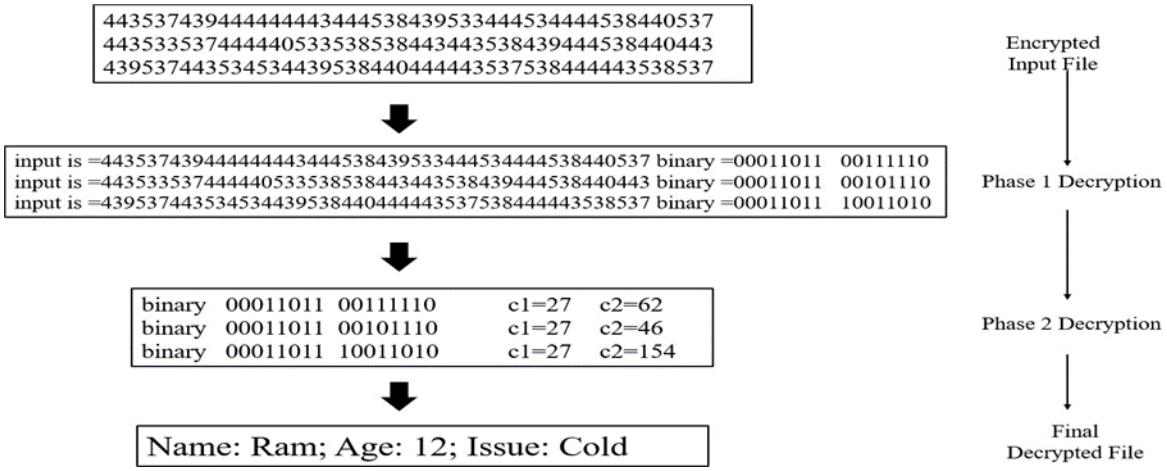

Figure 10: Decryption process in ElGamal Decryption Algorithm

Table 2: Transaction and execution cost

S. No.	OperationPerformed	Transactioncost		Executioncost		Total cost(inether)
		Ingasunits	Inethers	Ingas units	Inethers	
1.	Contract Deployment	1955973	0.2621004	1444301	0.1935363	0.4556367
2.	Addchemist	166589	0.0223229	142821	0.019138	0.0414609
3.	Adddoctor	207754	0.027839	182834	0.0244998	0.0523388
4.	Addinsurance Company	126755	0.0169852	104651	0.0140232	0.0310084
5.	Addpatient	208706	0.0279666	184170	0.0246788	0.0526454
6.	Getpatient Information	29325	0.0039296	7797	0.0010448	0.0049744
7.	UpdatePrecautions	44111	0.0059109	21367	0.0028632	0.0087741
8.	Getchemist	25707	0.0034447	4243	0.0005686	0.0040133
9.	Getinsurance Company	26489	0.0035495	5089	0.0006819	0.0042314
10.	AddMedications Notcoveredininsurance	65770	0.0088132	44114	0.0059113	0.0147245
11.	CreateTreatment-Id	21857	0.0029288	329	0.0000441	0.0029729
12.	TreatPatient	189040	0.0253314	165144	0.0221293	0.0474607
13.	Gettreatment Details	27482	0.0036826	5890	0.0007893	0.0044719
14.	Medication Includedininsurance	53756	0.0072033	31780	0.0042585	0.0114618
15.	Getdoctordetails	24375	0.0032663	2911	0.0003901	0.0036564

Because this experiment involves the deployment or execution of a smart contract, its complexity is measured in terms of gas. The costs associated with each procedure carried out in the experiment are shown in Table 1. Gwei

metrics are used. Total cost is equal to the number of gas units used times the cost per gas unit. To execute the framework, all of the activities in rows 1, 2, 3, 5, 7, 10, 11, 12, 14, and 16 must be completed. Therefore, 0.7274322 ethers are needed to execute this framework overall.

Performance comparison Analysis

In this section, we address the performance assessment of proposed framework with other existing schemes related to privacy preserving of Health Record Information system schemes.

Reference	Access Control	Access Revocation	Privacy Preserving	Access to Patients	Predictive Model	Decision Making
Al-Sumaidaee et al. (2023)	Yes	Yes	No	No	NO	Yes
Egala et al. (2023)	Yes	No	No	Yes	No	No
Abou El Houda et al. (2022)	Yes	No	Yes	Yes	No	No
Proposed Model	Yes	Yes	Yes	Yes	Yes	Yes

7.CONCLUSION

This study presented a blockchain based on a fair and robust MPC scheme to address the needs of robustness and fairness in multi-party computing. The suggested approach maintains a public reputation system in which each participant has a reputation value and a more respectable party has a higher probability of being chosen. The significance of electronic health information in terms of numerous security and privacy issues is covered in this study. After meticulously noting a number of issues, we established a novel architecture to protect and preserve the confidentiality of healthcare data. This is why data is sent and stored in an encrypted manner. With this innovative kind of encryption, users may safely work with encrypted text, ensuring that their data remains private. Consequently, it also reduced the time required to finish several encryption and decryption procedures for every obtained query. We also integrated it with blockchain technology to make it impenetrable. Results from our tests showed that the technology outperformed more traditional forms of encryption and storage. The Smart Contract needs to check the values of the intermediate and final stages of each cycle. When the timer goes off, the smart contract will know that either a message was sent or none was sent. Furthermore, an incentive structure promotes teamwork by all parties involved; those who are truthful will gain more and more, while those who are dishonest will suffer more severe repercussions. Concerns about privacy stem from the fact that blockchain maintains an immutable public record; MPC was developed to tackle this very problem. In future studies, we will look at the potential privacy protection advantages that MPC offers blockchain.

REFERENCES

[1] R. Cleve, “Limits on the security of coin flips when half the processors are faulty,” in Proc. 18th Annu. ACM Symp. Theory Comput. (STOC), 1986, pp. 364–369.
[2] J. Halpern and V. Teague, “Rational secret sharing and multiparty computation: Extended abstract,” in Proc. 36th Annu. ACM Symp. Theory Comput. (STOC), 2004, pp. 623–632.
[3] A. Lysyanskaya and N. Triandopoulos, “Rationality and adversarial behavior in multi- party computation,” in Advances in Cryptology— CRYPTO. Berlin, Germany: Springer, 2006, pp. 180–197.
[4] A. Groce and J. Katz, “Fair computation with rational players,” in Advances in Cryptology—EUROCRYPT. Berlin, Germany: Springer, 2012, pp. 81–98.
[5] M. Nojoumian and D. R. Stinson, “Socio-rational secret sharing as a new direction in rational cryptography,” in Decision and Game Theory for Security. Berlin, Germany: Springer 2012, pp. 18–37.
[6] G. Asharov, R. Canetti, and C. Hazay, “Towards a Game Theoretic View of Secure Computation,” in Advances in Cryptology—EUROCRYPT. Berlin, Germany: Springer 2011, pp. 426–445.

[7] S.Nakamoto.(2008).Bitcoin:A Peer-to-Peer Electronic Cash System. [Online]. Available: https://bitcoin.org/bitcoin.pdf
[8] M. Andrychowicz, S. Dziembowski, D. Malinowski, and Ł. Mazurek, "Fair two-party computations via Bitcoin deposits," in Financial Cryptography and Data Security. Berlin, Germany: Springer, 2014, pp. 105–121.
[9] M. Andrychowicz, S. Dziembowski, D. Malinowski, and L. Mazurek, "Secure multiparty computations on Bitcoin," in Proc. IEEE Symp. Secur. Privacy, May 2014, pp. 443–458.
[10] I. Bentov and R. Kumaresan, "How to Use Bitcoin to design fair protocols," in Advances in Cryptology—CRYPTO. Berlin, Germany: Springer, 2014, pp. 421–439, 2014.
[11] R. Kumaresan and I. Bentov, "How to Use Bitcoin to incentivize correct computations," in Proc. ACM SIGSAC Conf. Comput. Commun. Secur. (CCS), 2014, pp. 30–41.
[12] R. Kumaresan, T. Moran, and I. Bentov, "How to use Bitcoin to play decentralized poker," in Proc. 22nd ACM SIGSAC Conf. Comput. Commun. Secur. (CCS), 2015, pp. 195–206.
[13] R. Kumaresan, V. Vaikuntanathan, and P. N. Vasudevan, "Improvements to secure computation with penalties," in Proc. ACM SIGSAC Conf. Comput. Commun. Secur. (CCS), 2016, pp. 406–417.
[14] A. Kiayias, H.-S. Zhou, and V. Zikas, "Fair and robust multi-party computation using a global transaction ledger," in Advances in Cryptology— EUROCRYPT. Berlin, Germany: Springer, 2016, pp. 705–734.
[15] Juan Perez. Facebook, google launch data portability programs to all, 2008.
[16] Latanya Sweeney. k-anonymity: A model for protecting privacy. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 10(05):557–570, 2002.
[17] Ashwin Machanavajjhala, Daniel Kifer, Johannes Gehrke, and Muthu ramakrishnan Venkita subramaniam. l-diversity: Privacy beyond k-anonymity. ACM Transactions on Knowledge Discovery from Data (TKDD), 1(1):3, 2007.
[18] Ninghui Li, Tiancheng Li, and Suresh Venkatasubramanian. t-closeness: Privacy beyond k-anonymity and l-diversity. In ICDE, volume 7, pages 106–115, 2007.
[19] Arvind Narayanan and Vitaly Shmatikov. How to break anonymity of the netflix prize dataset. arXiv preprint cs/0610105, 2006.
[20] Yves-Alexandre de Montjoye, Cesar A Hidalgo, Michel Verleysen, and ´ Vincent D Blondel. Unique in the crowd: The privacy bounds of human mobility. Scientific reports, 3, 2013.
[21] Cynthia Dwork. Differential privacy. In Automata, languages and programming, pages 1–12. Springer, 2006.
[22] Craig Gentry. Fully homomorphic encryption using ideal lattices. In STOC, volume 9, pages 169–178, 2009.
[23] Soujanya, D. and Ramana, K.V., 2021. Secured Surveillance Storage Model Using Blockchain. In Evolving Technologies for Computing, Communication and Smart World (pp. 249-263). Springer, Singapore
[24] Al Omar, A.; Rahman, M.S.; Basu, A.; Kiyomoto, S. MediBchain: A blockchain based privacy preserving platform for healthcare data, Security, Privacy, and Anonymity in Computation, Communication, and Storage, Guangzhou, China, 12–15 December, 2017; Wang, G., Atiquzzaman, M., Yan, Z., Choo, K.K., Eds.; Springer: Cham, Switzerland, 2017.
[25] 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, 1–13.
[26] Azaria, A.; Ekblaw, A.; Vieira, T.; Lippman, A. MedRec: Using blockchain for medical data access and permission management. In Proceedings of the 2016 2nd International Conference on Open and Big Data (OBD), Vienna, Austria, 22–24 August 2016; pp. 25–30.
[27] Fan, K.; Wang, S.; Ren, Y.; Li, H.; Yang, Y. MedBlock: Efficient and Secure Medical Data Sharing Via Blockchain. J. Med. Syst. 2018, 42, 1–11.
[28] Zhang, A.; Lin, X. Towards Secure and Privacy-Preserving Data Sharing in e-Health Systems via Consortium Blockchain. J. Med. Syst. 2018, 42, 1–18.
[29] Bingqing Shen , Jingzhi Guo and Yilong Yang, MedChain: Efficient Healthcare Data Sharing via Blockchain, Journal of Applied Science (MDPI), Volume 9(6), 1207, https://doi.org/10.3390/app9061207, 2019.
[30] Uddin, M.; Memon, M.S.; Memon, I.; Ali, I.; Memon, J.; Abdelhaq, M.; Alsaqour, R. Hyperledger Fabric Blockchain: Secure and Efficient Solution for Electronic Health Records. CMC Comput. Mater. Continua. 2021, 68, 2377–2397
[31] Peng, Z.; Xu, C.; Wang, H.; Huang, J.; Xu, J.; Chu, X. P2b-trace: Privacy-Preserving Blockchain-Based Contact Tracing to Combat Pandemics. In Proceedings of the 2021 International Conference on Management of Data, Xi'an, China, 20–25 June 2021; pp. 2389–2393.

[32] Alrebdi, N.; Alabdulatif, A.; Iwendi, C.; Lian, Z. SVBE: Searchable and verifiable blockchain-based electronic health records system. Sci. Rep. 2022, 12, 266. [CrossRef] [PubMed]
[33] Mondal, S.; Shafi, M.; Gupta, S.; Gupta, S.K. Blockchain Based Secure Architecture for Electronic Healthcare Record Management. GMSARN Int. J. 2022, 16, 413–426.
[34] Alrebdi, N.; Alabdulatif, A.; Iwendi, C.; Lian, Z. SVBE: Searchable and verifiable blockchain-based electronic health records system. Sci. Rep. 2022, 12, 266. [CrossRef] [PubMed]
[35] Mondal, S.; Shafi, M.; Gupta, S.; Gupta, S.K. Blockchain Based Secure Architecture for Electronic Healthcare Record Management. GMSARN Int. J. 2022, 16, 413–426.
[36] Cerchione, R.; Centobelli, P.; Riccio, E.; Abbate, S.; Oropallo, E. Blockchain's coming to hospital to digitalize healthcare services: Designing a distributed electronic health record ecosystem. Technovation 2023, 120, 798–805. [CrossRef]
[37] Chatterjee, A.; Pahari, N.; Prinz, A. HL7 FHIR with SNOMED-CT to Achieve Semantic and Structural Interoperability in Personal Health Data: A Proof-of-Concept Study. Sensors 2022, 22, 3756. [CrossRef] [PubMed]
[38] Jayabalan, J.; Jeyanthi, N. Scalable blockchain model using off-chain IPFS storage for healthcare data security and privacy. J. Parallel Distrib. Comput. 2022, 164, 152–167. [CrossRef]
[39] Ruan, P.; Dinh, T.T.A.; Lin, Q.; Zhang, M.; Chen, G.; Ooi, B.C. Revealing Every Story of Data in Blockchain Systems. ACM SIGMOD Rec. 2020, 49, 70–77. [CrossRef]
[40] Tith, D.; Lee, J.S.; Suzuki, H.; Wijesundara, W.M.A.B.; Taira, N.; Obi, T.; Ohyama, N. Application of blockchain to maintaining patient records in electronic health record for enhanced privacy, scalability, and availability. Healthc. Inform. Res. 2020, 26, 3–12.
[41] Mani, V.; Manickam, P.; Alotaibi, Y.; Alghamdi, S.; Khalaf, O.I. Hyperledger Healthchain: Patient-Centric IPFS-Based Storage of Health Records. Electronics 2021, 10, 3003. [CrossRef]
[42] Chenthara, S.; Ahmed, K.; Wang, H.; Whittaker, F.; Chen, Z. Healthchain: A novel framework on privacy preservation of electronic health records using blockchain technology. PLoS ONE 2020, 15, e0243043. [CrossRef] [PubMed]
[43] Sun, J.; Yao, X.; Wang, S.; Wu, Y. Blockchain-based secure storage and access scheme for electronic health records in IPFS. IEEE Access 2020, 8, 59389–59401. [CrossRef]
[44] Verdonck, M.; Poels, G. Decentralized Data Access with IPFS and Smart Contract Permission Management for Electronic Health Records. In International Conference on Business Process Management; Springer: Cham, Switzerland, 2020; pp. 5–16.
[45] Ashizawa, N.; Yanai, N.; Cruz, J.P.; Okamura, S. Eth2Vec: Learning contract-wide code representations for vulnerability detection on ethereum smart contracts. Blockchain Res. Appl. 2022, 1, 100101.
[46] Chelsey C. Y. Hang, M. Batumalay, T D Subash, R. Thinakaran and B. Chitra, "Blockchain-based and IoT-based Health Monitoring App: Lowering Risks and Improving Security and Privacy" International Journal of Advanced Computer Science and Applications(IJACSA), 15(6), 2024. http://dx.doi.org/10.14569/IJACSA.2024.01506103
[47] Daraghmi, E.-Y.; Daraghmi, Y.-A.; Yuan, S.-M. MedChain: A Design of Blockchain-Based System for Medical Records Access and Permissions Management. IEEE Access 2019, 7, 164595–164613. [CrossRef]