International Journal of Healthcare Information Systems and Informatics
Volume 16 • Issue 4 • October-December 2021

A Blockchain-Based Distributed Authentication System for Healthcare

Soumyashree S. Panda, International Institute of Information Technology, Bhubaneswar, India
Debasish Jena, International Institute of Information Technology, Bhubaneswar, India
Priti Das, SCB Medical College and Hospital, India

ABSTRACT

The use of digital health records, stricter health laws, and the growing need for health records exchange point towards the need for an efficient security and privacy preserving mechanism. For health insurance management systems, multiple entities exchange health information, which is used for decision making. Since multiple authoritative entities are involved, a secure and efficient information sharing protocol is required as extremely sensitive health information is exchanged among the entities. Hence, this paper aims to put forward a novel a decentralized authentication system based on blockchain known as insurance claim blockchain (ICBChain) system. The proposed system ensures privacy of patients and provides secure information exchange and authentication of entities. An implementation of the proposed system is provided using Ethereum blockchain. The security and performance analysis of the system shows its potential to satisfy healthcare security requirements and its efficiency, respectively.

KEYWORDS

Blockchain, Distributed System, Elliptic Curve Cryptography (ECC), Ethereum, Healthcare, Insurance Claim Processing, Smart Contract, Transaction

INTRODUCTION

The fast evolution of Blockchain is paving the way for a system, where multiple parties who do not know each other or who do not trust each other can work together to achieve consensus. This is the key concept behind the first ever digital currency, Bitcoin (Nakamoto,2018). Conceptually, Blockchain serves as an immutable log of records that allows occurrence of transactions in a decentralized manner. Apart from this, Blockchain is distributed in nature and can eliminate single point of failure (Ali et al., 2018). Business sectors that demand high reliability and honesty can use Blockchain technology to gain popularity. It is widely believed that Blockchain would play an important role in the sustainable development of the global economy, enhancing people's quality of life (Shen et al., 2018). The inherent characteristics possessed by Blockchain makes it pertinent for accomplishing such a vision .This the reason why application of Blockchain technology is not limited to finance sectors anymore. Rather, it has been applied to provide a secure storage and access environment to various other sectors like Healthcare, Transportation, Government, Supply Chain etc. (Aggarwal et al., 2019).

Lately, there has been significant number of research conducted Blockchain and Healthcare in a combined way and the studies can be used to remodel the traditional procedures like health record storage and exchange, end to end drug provenance and traceability, medical claim processing etc. (McGhin et al, 2019; Mohanta et al., 2019b). Now-a-days, easy access of health record as well as

DOI: 10.4018/IJHISI.20211001.oa12

exchange of the same among various Healthcare Providers and Research Centres is being given more importance for better understanding of the clinical records. Considering the fact that health records are very exclusive in nature, it is very much necessary to ensure the security and privacy of the exchanged health information. Blockchain, due to its inherent features like immutability, decentralization, verifiable, etc., is an apt solution for providing a secure storage and access environment for exchange of healthcare information (Fernández et al. 2018). In fact, according to an investigation, more than 70% of industry leader predict that the greatest advantage of Blockchain technology is contributing to manage for the healthcare domain (Guo et al., 2018).The traditional health insurance claim and settlement process can be made more efficient and hassle free using Blockchain technology. Since Blockchain technology is particularly useful when multiple authoritative entities want to work together in a common platform for application development process. Hence, a novel distributed system using Blockchain is being presented where the Health Insurance Providers, Hospitals and the Claimants can come together to a common platform and work towards the management of insurance schemes. The proposed system is entitled as Insurance Claim Blockchain System (ICBChain). This study also proposes a novel protocol that addresses the requirements of Healthcare applications like authentication, privacy of patients and their health records, secure data sharing, interoperability and integrity. The proposed approach ensures that only authorized entities can have access to a patient's health records. This approach also ensures transparency among the entities of the system while sharing information so that any kind of fraud can be avoided. An extensive study of different performance parameters is also provided which proves the efficiency of the proposed system.

The rest of the manuscript is organized as follows. Section 2 describes the existing works in healthcare discipline based on Blockchain technology. Section 3 presents Blockchain technology and its related concepts. Section 4 presents the security requirements of Healthcare domain. After that, in section 5, the proposed distributed model for secure processing of healthcare insurance claims has been presented and described in details. Section 6 presents the implementation details. The formal analysis of the proposed approach is discussed in section 6. Finally, section 5 concludes the paper.

RELATED WORK

Though Blockchain technology initially designed to work as a backbone for crypto currency Bitcoin, but because of its open and decentralized framework, tamper proof and secure environment, Blockchain is gaining considerable amount of attention in other fields like Healthcare, Government, Intelligent transportation system, etc. In case of Healthcare domain, a lot of researches have pointed the capabilities of Blockchain technology to address the existing security related challenges (Ekblaw et al. 2016; Dubovitskaya et al., 2017; Xia et al., 2017; Sun et al., 2018; Griggs et al., 2018; 2018; Pham et al., 2018; Dwivedi et al., 2019). Hence in this section, we have reviewed almost all papers that have intended in integrating Blockchain technology with Healthcare domain to provide the required security and privacy. Ekblaw et al. (2016) presented a decentralized medical record management model where Blockchain technology was the key element. The model ensures secure data sharing, auditability, integrity and authenticity. Yue et al. (2016) proposed a model where patients can manage and control their own healthcare data with required security. An approach to manage and exchange the data of cancer patients using Blockchain technology is described by Dubovitskaya et al. (2017). Their approach provides fine grained access to the records with significantly less time. Simiarly, Xia et al. (2017) proposed a system for secure exchange of medical big data in a trust-less environment. They have developed a system known as "MeDShare" using smart contracts for sharing of data among cloud service providers. Zhao et al. (2017) presented a key management protocol for accessing the healthcare data using Blockchain. They have used Blockchain to store the secret keys of the users to ensure their privacy. Griggs et al.(2018) utilized private Blockchain for secure analysis and management of medical sensors. These sensors combined with IoT smart devices help in monitoring the health condition of a patient from remote locations. Next, Guo et al. (2018) proposed a Blockchain based approach

to preserve the privacy of patients and to resist collusion attack in a multiple authority healthcare system. They have used attribute based signature with the variant multiple authorities to ensure that only genuine users can access to electronic health records (EHR). However, they have not provided any implementation details of their scheme. Recently, Al et al. (2019) proposed a design for secure storage and access of healthcare data in cloud using Blockchain. According to their design, only the data sender can access to the data stored in the ledger which restricts it from sharing it with others. Most of the works only concentrated on storage of the Healthcare records and access to them. But Healthcare domain has other use cases which are not addressed till now. Therefore, in this paper, the insurance claim processing scenario is considered as the use case.

BLOCKCHAIN

Blockchain, the key element of Bitcoin, has been growing at an unbelievable pace over the last few years and its application is not limited to digital currency anymore. A Blockchain is basically a distributed database used by the interested network elements in a P2P network (Mohanta et al., 2018). The distributed database records the transactions in the blocks of the Blockchain and each block is connected to its previous block through a hash function to maintain the chain (Fernández et al., 2018). The network elements/nodes will receive a pair of public key and private key upon registering to the Blockchain network which can be used for encryption and decryption purpose. In addition to this, the private key also helps to sign transactions in Blockchain network and public key works as a unique identifier for each element. Whenever a node wants to communicate with another node belonging to the same Blockchain network, the source node signs the transaction with its private key and broadcasts it to its peers at one hop distance (Panda et al., 2019b).. Here signing a transaction does not only help in authenticating a valid node but also ensure that integrity of the transactions will be maintained. Once the peers of the source node get the signed transactions, first they verify its authenticity. If it is valid then only the peer nodes will re-transmit it to other peers (Mohanta et al., 2019a). The transactions, which are received by all the nodes of the Blockchain network and are validated, are grouped into a timestamped block by few nodes designated as miners. A consensus algorithm is used to select a block, among the number of blocks created by the miners, which will be added to the Blockchain network.

Key Features

The following features of Blockchain describe how and why Blockchain can be a panacea for all the security issues in a decentralized environment (Panda et al., 2019a).

- Open: It means whatever information that is stored in Blockchain is accessible to all the nodes belonging to the network.
- Distributed Ledger: Blockchain is a distributed ledger, i.e., we are keeping a copy of the public ledger with every individual party who are there, communicating with each other. The underlying platform can be decentralized or distributed based on the nature of the application.
- Verifiable: Every individual belonging to the Blockchain network should be able to check the validity of the information stored in the Blockchain Ledger.
- Permanent: The information that are entering into the Blockchain network that must be persistent. Once entered, information cannot be changed or updated in future.

Types of Blockchain

Blockchain can be public or private. It can also be permission less or permission-based/permissioned at the same time. In case of crypto currencies, the terms public/permission less and private/permission-based can treated as synonyms, but it is not the case with many other applications. As the name

implies, public Blockchain network is open for everyone (Hammi et al., 2018). Anyone can join the network at anytime without registering with any third/central party. Bitcoin, Litecoin, Ethereum are some of the examples of public Blockchain. Private Blockchain somewhat works like a centralized system where a third/central party controls the access to the network. Only a particular set of nodes can act as miners and this type of Blockchain is less time and power consuming as compared to public Blockchain. Private Blockchain can be permission-based or permission less. Examples of permission-based private Blockchain are Hyperledger Fabric, Ripple, etc.

Elliptic Curve Cryptography

Elliptic curve cryptography, a type of Public key cryptography is widely used because of small key size and low computational overhead as compared to RSA (Chen et al, 2010). It is basically based on the algebraic structure of elliptic curves over a finite Galois field (GF) (Miller and V, 1985; Chen et al, 2010).

The encryption and decryption mechanism of ECC is given below.

Encryption

First select an Elliptic group Ep(i, j) and generator point, $G \in Ep(i, j)$. Then select n such that $nG = 0$. Then both the communicates entities (say S and R) chooses a private key, r_S, $r_R < n$ respectively. Then corresponding public keys are computed a Q_S, Q_R, where $Q_S = r_S G$ and $Q_R = r_R G$. Next, message,Msg is mapped in to point $P_{Msg} \in Ep(i, j)$.

Ciphertext will be computed as a point in the curve as, $C_{Msg} = [(KG), (P_{Msg} + KQ_R)]$, where K is a random integer.

Decryption

Receiver calculates the message as follows:

$P_{Msg} \leftarrow (P_{Msg} + r_R KG)$. Since receiver knows his private key $r_{R,}$ he will be able to decrypt the message.

SECURITY REQUIRMENTS OF HEALTHCARE DOMAIN

As per the security and privacy rule of Health Insurance Portability and Accountability Act (HIPAA), the entities belonging to the Healthcare domain must implement security measures to protect their information infrastructure and mechanisms to monitor and control intra and inter-domain information access (Appari et al. 2010). Healthcare system has special requirements related to security and privacy in addition to confidentiality, integrity and availability. Now days, with cloud storage and internet technology, sharing of patient's health records and data have become more widespread (Dinget al., 2016). Since this information is highly sensitive, ensuring security and privacy of this information are a matter of concern (McGhin et al., 2019; Sahi et al., 2017). Thus, this section describes the main security requirements of Healthcare discipline and characteristics that a suitable authentication protocol for Healthcare systems should possess.

1. Authentication and Access Control: Authentication is the process of verifying one's identity and access control is a way of restricting access to resources. With the transfer of health records from paper to digital data, it requires extra security and only authorized entities should be allowed to access this information to preserve the privacy of the information. For example, electronic health records should be accessed only by those who have the privilege to see them and patient's consent should be taken before sharing his or her health records (Yüksel et al.,2017). Apart from this, stringent access control mechanisms should be employed to reduce the likelihood of tampering or leaking of these records.

2. Data Privacy and Anonymity: As per a survey on Healthcare data, patients strongly believe that their personal information and health record should be shared only with the entities involved in their treatment. Even if, many patients agree to share their health records, they strictly reject to share their personal details. Thus utmost care should be taken while exchanging such sensitive information with anyone.
3. Integrity: It is one of the critical requirements for an approach to ensue both message integrity and data integrity. Maintaining message or transaction integrity means that the communicated message must not be modified during transmission. Data or information integrity means ensuring the consistency of the information throughout its entire lifetime. This can be achieved by allowing only legitimate users to alter the stored information
4. Data Confidentiality: Confidentiality refers to the mechanism through which illegal access to information can be restricted. Since healthcare data are extremely sensitive, so it must be protected from unauthorized access which could be risky to a patient's life.
5. Non-repudiation: Non-repudiation is a property that assures that an entity cannot deny that she has performed an action. For example, a hospital cannot deny having generated a claim request.
6. Data Interoperability: It is one of the major requirements for the Healthcare system. It is the characteristics of a system that allows exchange and use of information among different entities of the system. As in case of conventional Healthcare systems data are stored in a centralized database, it restricts the interoperability of the system. The main issues with centralized storage are slow access to health records, single point failure and availability of health records etc. Thus instead of centralized storage, heath records should be stored in a decentralized or distributed manner to ensure interoperability in the system.
7. Mobility: The movement of patients from one physician to another is also affecting the Healthcare systems as the patients require their health records to be portable enough to support their mobility. In addition to it, as the body sensors, smart devices and other internet enabled devices become more widespread, advanced secure mechanisms should be used to send these real time data from any remote location at any time.

PROPOSED WORK

Our main objective is to design a distributed system for secure and efficient processing of health insurance claims using Blockchain technology. The proposed ICBChain system relies on a public Blockchain where smart contracts are implemented to ensure that only a legitimate entity can access the system. Since private Blockchain works for predefined set of users and adding new users is very difficult, so this type of Blockchain is not used. Patient's personal information is not stored in the Blockchain since this information is not required for insurance claim processing. In this way, privacy of patient will be ensured and storage overhead for Blockchain will also be less.

System Architecture

The working scenario for our ICBChain System is presented in the Figure. 1. The framework has been designed using Blockchain that implements smart contracts. The HIPs are responsible for generating and deploying the ICBChain System Smart Contracts. The entire system consists of the following entities.

Claimant

Claimant is the customer who buys a Health Insurance Scheme (HIS) from a HIP. The Scheme provides coverage for all the medical and surgical expenses incurred by the Scheme holder when he/she is hospitalized. Each claimant needs to register to a particular HIP by providing the required information to purchase a HIS. On successful registration and purchase of a HIS, the concerned HIP will add the claimant to the ICBChain System.

Table 1. Terminology Table

Notation	Description
HIP_i	i^{th} Health Insurance Provider
C_j	j^{th} Claimant
H_k	k^{th} Hospital
$RN.HIP_i$	Unique registration number of HIP_i
$RN.H_k$	Unique Registration number of H_k
$ID.C_j$	Unique health identity of C_j
EA. HIP_i	Ethereum address of HIP_i
$EA.C_j$	Ethereum address of C_j
$EA.H_k$	Ethereum address of H_k
r. HIP_i	Elliptic Curve Private key of HIP_i
Q. HIP_i	Elliptic Curve Public key of HIP_i
r. H_k	Elliptic Curve Private key of H_k
Q. H_k	Elliptic Curve Public key of H_k

Health Insurance Providers (HIP)

Health insurance companies provide insurance that covers risks fully or partly of a person incurring medical expenses. In the proposed ICBChain system, one of the HIPs generates the smart contracts and deploys them in the Blockchain. The HIP is also responsible for publishing the smart contract address to other HIPs, Hospitals and HIS holder so that they can be a part of the system.

Hospitals

A set of recognized Hospitals are preordained by the HIPs of the ICBChain system to be a part of the model. They are treated as a node in the ICBChain model and authorized to intimate claim settlement process directly using smart contracts.

Smart Contracts

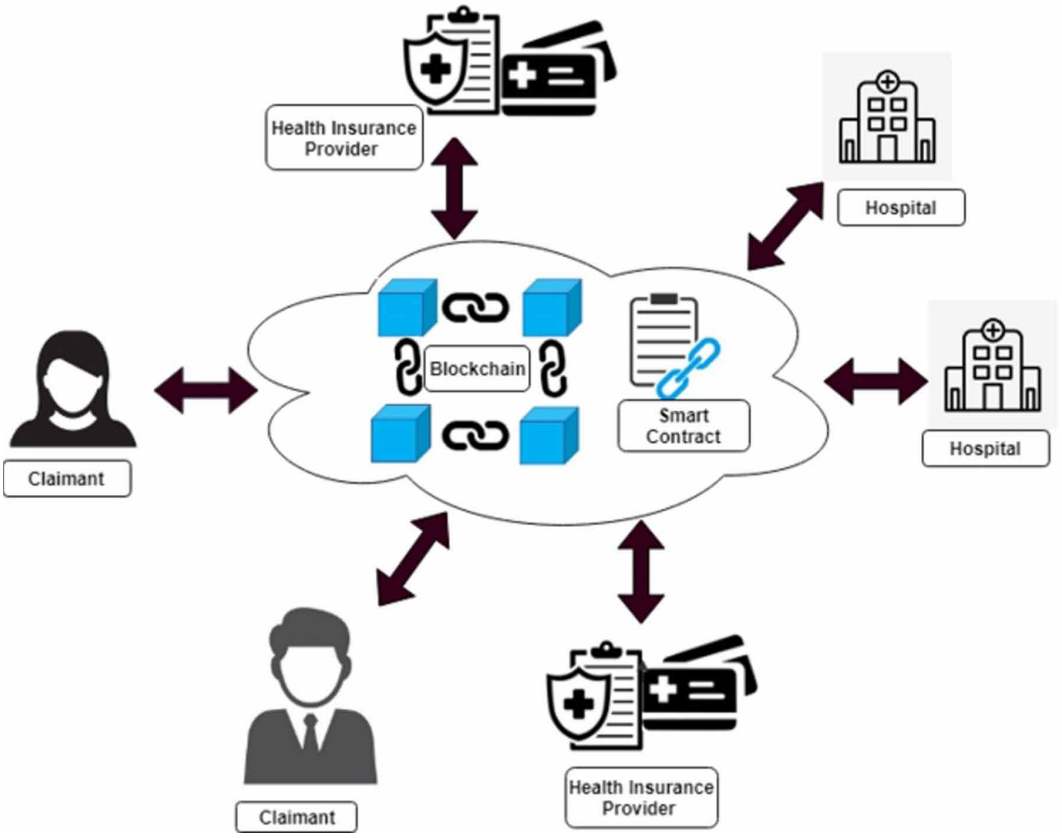
As per the definition of Smart Contract, it helps to develop and deploy agreements among the different entities of the IBS model without the need of a trusted third party (Panda et.,al,2019). The associated codes and data of a smart contract cannot be tampered and can easily be traced. The code or functionalities mentioned in the smart contract are executed automatically when a particular condition is met.

The entire working of the proposed system takes place in three phases which are described below.

Initialization Phase

A claimant needs to buy a health insurance policy by registering to a HIP. The claimant has to provide the required information like name, age, contact details, ID proof, address details, address proof etc and has to choose one of the available insurance schemes. On receiving the purchase request, first the concerned HIP validates the information provided by the claimant and updates the claimant about the payment procedure. On successful purchase of a HIS, a unique health identity will be generated which will be shared with the claimant. The HIP stores all the information provided by the claimant in its database along with the health identity and adds him/her to the ICBChain system by assigning

Figure 1. Architecture of Insurance Claim Blockchain System



the claimant an Ethereum Address. The HIP also shares the smart contract Ethereum address (EA. SC) with the claimant for further communication.

Each networked Hospital has to generate an Elliptic Curve private/public key pair for encryption/decryption.

Registration Phase

Each and every HIP needs to register the claimants in the ICBChain who have already gone through the pre-registration phase using the defined smart contract. Only a HIP can invoke this smart contract to add a claimant by using its Ethereum address (EA.C) and health identity. As a part of the registration process, the smart contract stores the association of the claimant with the HIP in the Blockchain for future reference. In a similar manner, all the Hospitals associated with each of the HIPs are added to the ICBChain network by host HIP by providing them with Ethereum addresses. Hospital registration smart contract has been used for the same.

Claim Settlement Phase

This phase consists of three parts 1) Claimant Authentication and Request Initiation, 2) Claim Settlement and Payment and 3) Update claim status

1. Whenever a registered claimant admitted to a hospital and provides the health identity, the hospital first verifies this proof using Authentication Smart Contract. A request token will be generated if and only if the identity is registered with a HIP and stored in the Blockchain.
2. This activity is carried out outside the Blockchain network since a number of documents need to be verified before doing the payments.
3. Once the request is resolved, the HIP updates the same in the Blockchain so that everyone can validate that.

Smart Contracts of ICBChain System

The proposed system depends on four smart contracts which are Manage Claimant Smart Contract, Manage Hospital Smart Contract, Authentication Smart Contract and Update Claim Status Smart Contract.

1. Manage Claimant Smart Contract (MCSC): The functions included in RSC are as follows:

`Add_Claimant (EA.C, ID.C and RN.HIP)`

This function can only be executed by a Health insurance Provider to add claimants to the Blockchain network.

`View_Claimant (EA.C, ID.C)`

This function can be executed by the Health insurance Providers, Hospitals and claimants belonging to the system.

`Delete_Claimant (EA.C, ID.C and RN.HIP)`

A HIP can only invoke this functionality. It takes EA.C, ID.C and RN.HIP where RN.HIP is the identity of the HIP who is invoking the function. The function executes successfully if and only if the input RN.HIP matches with the RN.HIP stored corresponding to the ID.C in the Blockchain. This ensures that a particular HIP can only delete its own customers.

2. Manage Hospital Smart Contract (MHSC): The smart contract includes the following functions:

`Add_Hospital (EA.H, RN.H, RN.HIP)`

This function can only be executed by a HIP to add the authorized Hospitals to the system.

`View_Hospital (EA.H and RN.H)`

This function can be executed by the Health Insurance Providers and Hospitals. Hospitals use this function to check their own information.

`Delete_Hospital (EA.H, RN.H and RN.HIP)`

A HIP can only invoke this functionality. It takes EA.H, RN.H and RN.HIP where RN.HIP is the identity of the HIP who is invoking the function.

3. Authentication Smart Contract (ASC): The main functions of ASC are as follows:

`Authenticate_Claimant (EA.C, ID.C and RN.HIP):`

This function can be accomplished by the health Insurance Providers and the Hospitals to authenticate a claimant. If the given input matches with the stored one, then a Request_token will be generated as an output. This Request_token will be used by the Hospital who has invoked this function for the off chain claim settlement process.

4. Update Claim Status Smart Contract (UCSSC): The smart contract includes the following functions:

`UpdateClaim_Status (EA.C, ID.C, Request_token, RN.H and Signature)`

This function can only be executed by Hospital to update the status of the claim as "Approved" or "Rejected". The Smart Contract first checks whether the function has been invoked by an authorized Hospital by checking the signature. If yes, then it verifies the validity of the Request_token. If valid then updates its status and stores the same in the Blockchain. This way a Hospital cannot deny later that it has not received the payment.

`ViewClaim_Status (RN.HIP, EA.C and Request_token)`

The claim status can be viewed by all the entities of the system i.e. the Health Insurance Providers, the Hospitals and the Claimants.

System Functioning in Steps

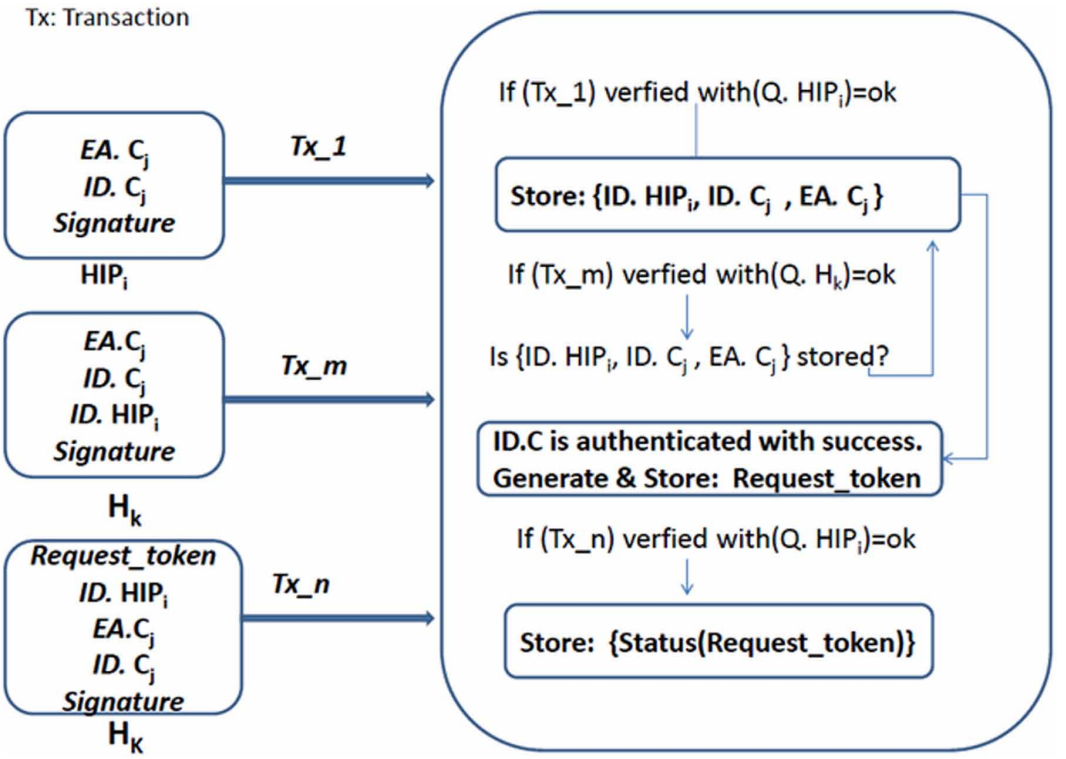
On Chain Activities

1. The first transaction represents registration of claimant Cj in the system by HIPi. The sent message contains EA.Cj, ID.Cj, Encrypted data of Cj and is signed with the HIPi's private key i.e. r.HIPi.
2. When MCSC receives the transaction, it first verifies the integrity of the message by checking the signature with HIPi public key i.e. Q.HIPi. If it is valid, then the association < RN.HIPi, EA. Cj , ID. Cj > is stored in the Blockchain.
3. Whenever H_K initiates a claim request for its patients, a transaction takes place in the Blockchain network to verify the authenticity of the patient which contains (a) ID.HIPi, (b) ID. Cj and (d) the signature using r.HIPi.
4. On receiving the transaction, ASC verifies the validity of the signature using Q.HIPi. If the signature is valid, then it checks if the ID. C_j is stored in the Blockchain and associated with ID.HIP_i sent in the transaction.
5. If the association is stored, then C_j will be authenticated. The smart contract also generates a structure known as Request_token which will be used by H_k for off chain claim settlement process. It is a very lightweight proof that contains a) Request_no, b) $E_{Q.HIPi}$ {ID. C_j || Disease Details} and c) signature
6. This Request_token will be broadcasted to all the entities of ICBChain system as per concept of Blockchain. (For this reason, to ensure the privacy of the claimant disease details are encrypted so that only the concerned entity can decrypt it.)

Off Chain Activities

1. After all the procedural treatment is completed, H_k sends the Request_token received from the Blockchain network, the bills and other supporting documents to HIP_i. H_k encrypts ID.C and the documents using the EC public key (Q. HIPi). So Hk sends ID. Hk , H (Request_token), $E_{Q.HIPi}${Docs} and signature where Docs represents the bills and supporting documents and H= SHA256 Hash function.
2. On receiving the message, HIPi verifies the signature to ensure its integrity and to verify the authenticity of Hk. If valid, then it decrypts the Request_token and cross checks the parameters of the received token from both ASC and the Hk. If matches, then only it decrypts to find out the documents needed for decision making. It then verifies all the received documents which, if, is as per the requirements, and then it is approved and vice versa.
3. Then H_K stores the status of the Request_token in the Blockchain along with the corresponding claimant's identity and payment details. For this, it initiates a transaction which contains ID.C, Request_token, ID.H, status and signature. On receiving this input, UCSSC verifies the signature,

Figure 2. Transactions in the Proposed System



if valid, and then stores this information on the Blockchain so that the concerned claimant can be notified about the same.

IMPLEMENTATION

In this section, a detailed description of how the proposed ICBChain system is implemented using Smart Contracts. The experimental set up consists of 5 laptops, out of which two laptops are designated as two different HIPs, two laptops are used to represent two claimants and one is used to represent a hospital. Descriptions of the laptops are provided in Table 2. As mentioned, Ethereum is used as the Blockchain to realize ICBChain system. Smart Contracts that serve as the core of the proposed system are developed using Solidity language. These smart contracts are implemented and verified using Remix IDE (Remix, 2018) before deploying them in Blockchain platform. In fact, Ropsten Testnet is being used, which is an Ethereum tool for testing and development purposes. We have used ECC for ensuring the confidentiality and integrity of the communicated messages.

RESULT ANALYSIS

In this section, the proposed scheme has been analysed thoroughly in terms of security and performance.

Security Analysis

This section shows how the proposed ICBChain meets the security requirements of a Healthcare domain as presented above.

Table 2. System Specification

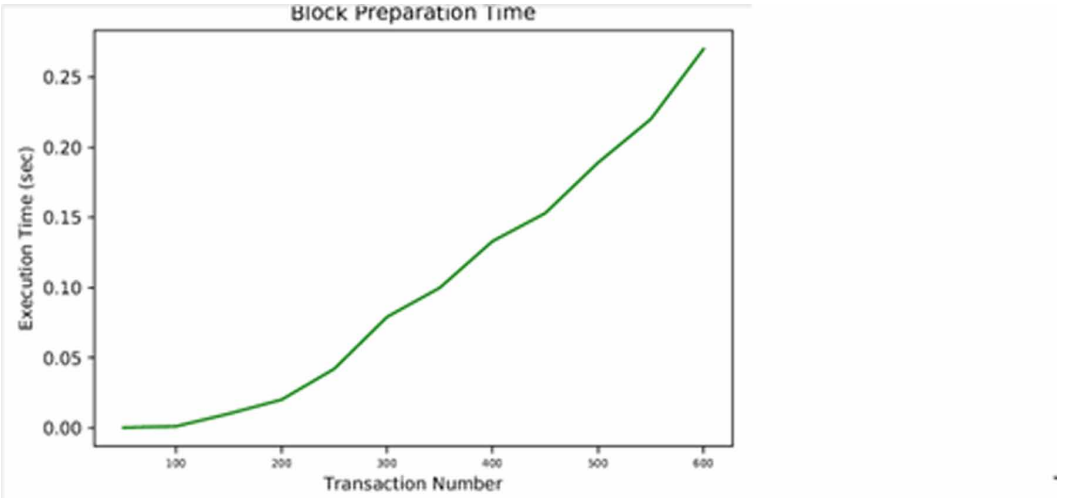
System Number	Designation	Specification
1	Health Insurance Provider 1	Intel(R) Core(TM) i5, CPU-3.30 GHz, 8 GB of RAM, Win 8, 64-bit OS
2	Health Insurance Provider 2	Intel(R) Core(TM) i5, CPU-3.30 GHz, 8 GB of RAM, Win 8, 64-bit OS
3	Hospital 1	Intel(R) Core(TM) i5, CPU-2.20 GHz, 8 GB of RAM, Win 8, 64-bit OS
4	Hospital 2	Intel(R) Core(TM) i5, CPU-2.20 GHz, 8 GB of RAM, Win 8, 64-bit OS
5	Claimant	Intel(R) Core(TM) i3, CPU-2.00 GHz, 8 GB of RAM, Win 8, 64-bit OS

1. Authentication and Access Control: Every time a HIP adds a new claimant to the system, it stores the association with them in the Blockchain which is used to authenticate the claimants. The HIPs are responsible for properly verifying the personal details of the claimants in the pre-registration phase, so that any malicious user can not have access to the system.
2. Integrity: All the messages exchanged between different entities of the proposed system are signed with the sender's private key using ECDSA. This signature ensures both authentication of entities and integrity of the messages.
3. Anonymity and Data Privacy: Data privacy is ensured in the proposed system by not storing the sensitive personal and healthcare data in the Blockchain. This ensures that a claimant's personal information cannot be accessed by any of the entities of the system except the authorized ones. In fact, only minimal information of the claimants is stored in the Blockchain which will be required for decision making. All the messages exchanged during off chain activities are also encrypted to ensure the privacy of the data. Ethereum addresses and a unique health-ID are used in place of real identities so that the claimants will not be identified by any entities during transaction.
4. Data Confidentiality: Confidentiality is ensured since all the sensitive information is encrypted using the EC public key of the receiver.
5. Scalability: The use of public Blockchain for realizing the proposed ICBChain system solves the scalability issue. In fact, since we are not keeping the records of all the claimants in the Blockchain, the storage overhead is also reduced.
6. Non-repudiation: The messages contained in each transaction are signed using the private key, which is only known to its owner. Thus, it cannot deny the fact of signing a message or sending it.

PERFORMANCE ANALYSIS

In this section, we analyze the Block preparation time in terms of transaction number of the proposed ICBChain system. The ability to record transactions in an efficient, light-weight, and scalable manner is the main concern. Fig. 4 plots the Block preparation time. The preparation time increases exponentially with the growth of transaction number. The preparation time slowly increases before 200 transactions. Preparation time over 0.1 s when transaction bigger than 400. Finally, preparation time reaches 0.275 s when there are 600 transactions.

Figure 3. Block



CONCLUSION

Security and privacy of patients in Healthcare systems is a matter of growing since multiple entities (patients, hospitals and health insurance providers) exchange health information between themselves for decision making. It must be ensured that only valid users can access and exchange this extremely sensitive health information among them.

The paper presented a secure and efficient system for health insurance claim processing. All the entities of the proposed ICBChain system communicate in a secure way. Issues related to security and privacy in Healthcare domain has been discussed. The security analysis depicts compliance to all such issues. Performance evaluation revealed that the proposed ICBChain system runs satisfactorily. For future research, the authors will try a) to address the mobility of different entities of a healthcare system (e.g. clinical research centre, patients, insurance providers, hospital etc.) across the network and b) to address the problem of secure management of the secret keys of the entities of the system.

REFERENCES

Aggarwal, S., Chaudhary, R., Aujla, G. S., Kumar, N., Choo, K. K. R., & Zomaya, A. Y. (2019). Blockchain for smart communities: Applications, challenges and opportunities. *Journal of Network and Computer Applications*, *144*, 13–48. doi:10.1016/j.jnca.2019.06.018

Al Omar, A., Bhuiyan, M. Z. A., Basu, A., Kiyomoto, S., & Rahman, M. S. (2019). Privacy-friendly platform for healthcare data in cloud based on blockchain environment. *Future Generation Computer Systems*, *95*, 511–521. doi:10.1016/j.future.2018.12.044

Ali, M. S., Vecchio, M., Pincheira, M., Dolui, K., Antonelli, F., & Rehmani, M. H. (2018). Applications of blockchains in the Internet of Things: A comprehensive survey. *IEEE Communications Surveys and Tutorials*, *21*(2), 1676–1717. doi:10.1109/COMST.2018.2886932

Appari, A., & Johnson, M. E. (2010). Information security and privacy in healthcare: current state of research. *International Journal of Internet and Enterprise Management, 6*(4), 279-314.

Chen, T. H., Chen, Y. C., & Shih, W. K. (2010, October). An Advanced ECC ID-Based remote mutual authentication scheme for mobile devices. In *2010 7th International Conference on Ubiquitous Intelligence & Computing and 7th International Conference on Autonomic & Trusted Computing* (pp. 116-120). IEEE. doi:10.1109/UIC-ATC.2010.18

Ding, D., Conti, M., & Solanas, A. (2016, April). A smart health application and its related privacy issues. In 2016 Smart City Security and Privacy Workshop (SCSP-W) (pp. 1-5). IEEE. doi:10.1109/SCSPW.2016.7509558

Dubovitskaya, A., Xu, Z., Ryu, S., Schumacher, M., & Wang, F. (2017). Secure and trustable electronic medical records sharing using blockchain. *AMIA ... Annual Symposium Proceedings - AMIA Symposium. AMIA Symposium*, *2017*, 650. PMID:29854130

Dwivedi, A. D., Srivastava, G., Dhar, S., & Singh, R. (2019). A decentralized privacy-preserving healthcare blockchain for iot. *Sensors (Basel)*, *19*(2), 326. doi:10.3390/s19020326 PMID:30650612

Ekblaw, A., Azaria, A., Halamka, J. D., & Lippman, A. (2016, August). A Case Study for Blockchain in Healthcare:"MedRec" prototype for electronic health records and medical research data. In *Proceedings of IEEE open & big data conference* (Vol. 13, p. 13). IEEE.

Fernández-Caramés, T. M., & Fraga-Lamas, P. (2018). A Review on the Use of Blockchain for the Internet of Things. *IEEE Access : Practical Innovations, Open Solutions*, *6*, 32979–33001. doi:10.1109/ACCESS.2018.2842685

Guo, R., Shi, H., Zhao, Q., & Zheng, D. (2018). Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems. *IEEE Access : Practical Innovations, Open Solutions*, *6*, 11676–11686. doi:10.1109/ACCESS.2018.2801266

Hammi, M. T., Hammi, B., Bellot, P., & Serhrouchni, A. (2018). Bubbles of Trust: A decentralized blockchain-based authentication system for IoT. *Computers & Security*, *78*, 126–142. doi:10.1016/j.cose.2018.06.004

Jiang, S., Cao, J., Wu, H., Yang, Y., Ma, M., & He, J. (2018, June). Blochie: a blockchain-based platform for healthcare information exchange. In *2018 IEEE International Conference on Smart Computing (SMARTCOMP)* (pp. 49-56). IEEE. doi:10.1109/SMARTCOMP.2018.00073

McGhin, T., Choo, K. K. R., Liu, C. Z., & He, D. (2019). Blockchain in healthcare applications: Research challenges and opportunities. *Journal of Network and Computer Applications*, *135*, 62–75. doi:10.1016/j.jnca.2019.02.027

Miller, V. S. (1985, August). Use of elliptic curves in cryptography. In *Conference on the theory and application of cryptographic techniques* (pp. 417-426). Springer.

Mohanta, B. K., Jena, D., Panda, S. S., & Sobhanayak, S. (2019a). Blockchain Technology: A Survey on Applications and Security Privacy Challenges. *Internet of Things*, 100107.

Mohanta, B. K., Panda, S. S., & Jena, D. (2018, July). An overview of smart contract and use cases in blockchain technology. In *2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT)* (pp. 1-4). IEEE. doi:10.1109/ICCCNT.2018.8494045

Mohanta, B. K., Panda, S. S., Satapathy, U., Jena, D., & Gountia, D. (2019b, July). Trustworthy Management in Decentralized IoT Application using Blockchain. In *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)* (pp. 1-5). IEEE.

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. Academic Press.

Panda, S. S., Mohanta, B. K., Satapathy, U., Jena, D., Gountia, D., & Patra, T. K. (2019b, October). Study of Blockchain Based Decentralized Consensus Algorithms. In TENCON 2019-2019 IEEE Region 10 Conference (TENCON) (pp. 908-913). IEEE.

Panda, S. S., Satapathy, U., Mohanta, B. K., Jena, D., & Gountia, D. (2019a, July). A Blockchain Based Decentralized Authentication Framework for Resource Constrained IOT devices. In *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)* (pp. 1-6). IEEE.

Pham, H. L., Tran, T. H., & Nakashima, Y. (2018, December). A secure remote healthcare system for hospital using blockchain smart contract. In 2018 IEEE Globecom Workshops (GC Wkshps) (pp. 1-6). IEEE. doi:10.1109/GLOCOMW.2018.8644164

Qian, Y., Jiang, Y., Chen, J., Zhang, Y., Song, J., Zhou, M., & Pustišek, M. (2018). Towards decentralized IoT security enhancement: A blockchain approach. *Computers & Electrical Engineering*, *72*, 266–273. doi:10.1016/j.compeleceng.2018.08.021

Remix. (2018). *Remix description*. Available: http://remix.ethereum.org

Sahi, M. A., Abbas, H., Saleem, K., Yang, X., Derhab, A., Orgun, M. A., Iqbal, W., Rashid, I., & Yaseen, A. (2017). Privacy preservation in e-healthcare environments: State of the art and future directions. *IEEE Access : Practical Innovations, Open Solutions*, *6*, 464–478. doi:10.1109/ACCESS.2017.2767561

Shen, C., & Pena-Mora, F. (2018). Blockchain for Cities—A Systematic Literature Review. *IEEE Access : Practical Innovations, Open Solutions*, *6*, 76787–76819. doi:10.1109/ACCESS.2018.2880744

Soumyashree S. Panda received her Bachelor's degree from Siksha O Anusandhan University and Masters degree from IIT Dhanbad. Presently she is pursuing Ph.D. in IIIT Bhubaneshwar, Odisha, India. Her research focus areas are IoT Security, and Blockchain.

Sun, Y., Zhang, R., Wang, X., Gao, K., & Liu, L. (2018, July). A decentralizing attribute-based signature for healthcare blockchain. In *2018 27th International Conference on Computer Communication and Networks (ICCCN)* (pp. 1-9). IEEE. doi:10.1109/ICCCN.2018.8487349

Xia, Q. I., Sifah, E. B., Asamoah, K. O., Gao, J., Du, X., & Guizani, M. (2017). MeDShare: Trust-less medical data sharing among cloud service providers via blockchain. *IEEE Access : Practical Innovations, Open Solutions*, *5*, 14757–14767. doi:10.1109/ACCESS.2017.2730843

Yue, X., Wang, H., Jin, D., Li, M., & Jiang, W. (2016). Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control. *Journal of Medical Systems*, *40*(10), 218.

Yüksel, B., Küpçü, A., & Özkasap, Ö. (2017). Research issues for privacy and security of electronic health services. *Future Generation Computer Systems*, *68*, 1–13.

Zhao, H., Zhang, Y., Peng, Y., & Xu, R. (2017, March). Lightweight backup and efficient recovery scheme for health blockchain keys. In *2017 IEEE 13th International Symposium on Autonomous Decentralized System (ISADS)* (pp. 229-234). IEEE.

Debasish Jena, PhD., received his B Tech degree in Computer Science and Engineering, his Management Degree and his M.Tech Degree in 1991, 1997 and 2002 respectively. He got his Ph.D degree from NIT Rourkela in 2010. He is currently working as Associate Professor in IIIT Bhubaneshwar. In addition to his responsibility, he was also IT, Consultant to Health Society, Govt. of Orissa for a period of 2 years from 2004 to 2006. His research areas of interest are Information Security, Cloud Security, IoT Security and Blockchain. His professional memberships include IEEE, ACM, ISTE, IACSIT, MIE (I), CSI, and OITS.

Priti Das, PhD., is an MBBS and M.D. in Pharmacology from VSS Medical College, Burla. She is presently working as Associate Professor at SCB Medical College Cuttack. She has more than 20 years of experience in medical teaching.