DOI: https://doi.org/10.33103/uot.ijccce.21.3.7

Blockchain for Authorized Access of Health Insurance IoT System

Iman Mohammed Hasan[1], Rana Fareed Ghani[2]
[1,2] Computer Science Department, University Of Technology, Baghdad, Iraq.
[1]cs.19.01@grad.uotechnology.edu.iq, [2]110016@uotechnology.edu.iq

Abstract**—** *Today's insurance industry plays a significant role in a variety of fields, particularly in health insurance. As IoT technology advances, health insurers in IoT networks can obtain real-time medical data for individuals and issue individual insurance policies based on a person's lifestyle. However, sharing personal data requires a guarantee of privacy and security. This paper suggests a Blockchain technology to solve this problem. The work presents a novel framework that integrates health insurers, IoT-based networks, and Blockchain technology to implement access control protocol using a smart contract for sharing the financial premium of insureds with the stakeholders as non-participants/authorized parties. The evaluation of the proposal results in authorized access within less time compared to traditional data-sharing systems, and the security analysis shows that proposal can protect data from potential threats.*

Index Terms*— IoT, Blockchain, health insurance, insurer, Smart Contract, PBFT.*

I. INTRODUCTION

During the 1980s, a new technological revolution has occurred, which was the emergence of powerful, low-cost microprocessors and computer network innovation [1]. Computer Networks enabled accessing and transferring data among the connected computer. Networks spread widely to include all aspects of life businesses, schools, industries, healthcare, and more [2]. Also, it expanded to connect various devices and systems that need to work together. This problem led to appear distributed systems.

The distributed systems provide a scalable, open, and accessible environment among logically/geographically pervasive independent components. Distributed systems share the computational operations among the collaborated entities to be executed as a single/centralized system behind the user interface. This collaboration provides exact resource exploit and protects users from the failure of some components [1], [3].

The distributed systems have encouraged the emergence of the concept of the Internet of Things (IoT). IoT networks play an efficient role today in various domains because of their ability to connect different devices. In addition to sensing, sharing, storing, analyzing, and decision making about collected data [4]. However, IoT networks confront challenges related to the security of components and the privacy of data. For preserving these concepts, Blockchain technology is used as a new practical solution [5].

(R. Manyannk et al., 2018) proposed a framework that focused on the performance and security of normal processes in insurance companies [6]. The researchers designed a Blockchain-based system to provide fine-grained access. For each process, they specified a

Received 7/6/2021; Accepted 19l8l2021

 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.21.3.7

smart contract and various sets of endorsers. They used the Hyperledger Fabric platform to implement their insurance Blockchain. However, the results of security analysis are not involved.

(N. Dinh C. et al., 2019) proposed a framework that aims to provide secure sharing for electronic health records (EHRs) that manage participants' access to EHRs system [7]. The researchers combined Blockchain with a Decentralized Interplanetary File System (IPFS) and developed a mobile application to be an interface between participants and the primary cloud. However, the cloud has sent back requested data to the authorized user as a plaintext; this matter increases the risk of data leakage. To evaluate the schema performance, the researchers compared their system with a non-authorization system. The results show slight differences in processing time by 100ms as the worst result. The researchers concerned it as good latency compared to privacy implementation.

(Chen et al., 2019) proposed a Blockchain-based searchable encryption scheme for sharing electronic health records on the cloud, the schema aimed to improve EHRs searchability [8]. The Authors used public Blockchain to store the structure of EHR's indexes. The structure was build using complex logical expressions stored in smart contracts used by authenticated users to search the indexes of the EHRs. Although the schema gains control to the owners of their data access, ensures integrity, and prevents fraudulence, the schema suffers from the time cost spend because of the expression complexity.

(X. Xiang et al., 2020) presented mutual authentication schema called (PBBIMUA) that aims to improve the security of medical data of E-health systems [9]. The researchers used permissioned Blockchain technology to store mutual authentication identities. However, this proposed schema ignores the privacy of health data.

(S. Khalid et al., 2020) suggested a framework called (IoBHealth) that aims to save the privacy of patient data on E-health systems [10]. The researchers combined IoT and Blockchain technologies to store the data. Also, they used smart contracts to manage access permissions that enable healthcare providers to update the EHRs of the patient.

This paper presents a design and an implementation for a healthcare system based on Blockchain that:

- Integrates IoT network with healthcare insurance. Thus, the insurer can issue a health policy for insureds depending on the collected data by IoT networks.
- Enables insureds to control access to their insurance information and determines the access provisionally with keeping privacy and security.
- Enables a non-participant party to verify insurance policy detail under the control of the owner.

The later sections of the paper are organized as follows. Section 2 presents research background include the concepts of the Internet of Things (IoT), Blockchain and healthcare systems. Section 3 describes the methodology of the proposed model. Section 4 shows the experimental results of our proposed model and the security analysis. Finally, section 5 presents the conclusion arrived at in this paper.

II. BACKGROUND

Internet of things (IoT) is an emerging technology that consists of a collection of uniquely addressable objects that able to connect whenever and wherever using internet protocol (IP)

Received 7/6/2021; Accepted 19l8l2021

 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.21.3.7

and produce a scalable worldwide network [11], [12], [13]. Applications of the IoT include all domains of daily operations of individuals, societies, and organizations. The IoT applications aim at the smartness of these domains such as Cities, Lifestyles, Agriculture, industries, Supply chain, Healthcare, User interaction, tourism, Culture, Energy, and Environment [14], [15].

The IoT includes various enabling technologies that can be categorized into three integrated groups: The first group contains technologies that allow things to gather relevant information. The second supports things to process aggregated data. Finally, the technologies preserve the privacy and security of the collected data at the endpoint and during transmission between generator and receiver [12], [15].

One of the technologies so related to privacy and security is Blockchain technology. A Blockchain is a particular data structure that is a combination of transactions arranged into blocks. Blocks are cryptographically joined to each other to create an increased list. Blockchain is immutable and distributed among the participants in the untrusted network. This technology aims to share replicate of assets and digital files over a peer-to-peer network with forsaking the trust of a third party and a centralized authority. Blockchain enables consensus protocols to control the creation, validation of transactions [16], [17].

Although many countries still use conventional systems to introduce health services, electronic health systems are used by the healthcare industry in other countries, such as the digitalized healthcare system of Denmark that store the information of patients and healthcare providers [18].

Recently, information technology has attracted a great space of research in the healthcare domain in an integrated way, intending to improve health quality and lower costs by providing health information electronically anytime and everywhere on call [19],[20]. However, the data that is stored in the central E-health system is critical. So it needs to protect from unauthorized access and single-point failure. Permissions that control access must be stored in an immutable and auditable database for tracing an unauthorized activity [18].

In [21], the World Health Organization (WHO) aimed to provide the Universal Health Coverage UHC for distance residents and the poor with low-cost using systems to track health expenses that support the budgets. WHO asked the technical parties to collaborate and involve the sciences and technologies (sensors, mobiles, cloud, etc.) to create new solutions that serve their noble objectives.

Health Insurance is defined as coverage of medical treatment expenses that health insurers must pay to/ rather than insured. Today's most employment offers include payment of health insurance for the employees discounted from the employee's salary [22], [23]. Recently, health insurers have begun to integrate with IoT-based healthcare systems. This integration contributes to submit an individual insurance policy for the insured based on lifestyle and medical history. Not only insured benefits from this collaboration but also insurers benefit from it. The insurer can make the right decision about policy issuance and can direct its efforts toward protecting the insured rather than pay claims [24].

III. THE PROPOSED SYSTEM

This section describes the whole proposed system, including the network's general architecture also implementation of fundamental processes.

Received 7/6/2021; Accepted 19l8l2021

 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.21.3.7

A. System Architecture

This section illustrates the general network architecture of the work, as shown in *Fig.* 1, including the components of the network and the system entities.

1) Network Components

The proposed IoT-based network contains the main parts of E-Health systems, including the healthcare insurer, clients, cloud, etc. This section shows the fundamental components of this network, and their roles are as follows:

- **Client:** refers to an employee who is connected to the IoT-based network. Also, the client uses the collected data by IoT network to obtain a convenient health insurance policy by sharing it with the insurer.
- **IoT gateway:** refers to devices that contain applications to execute basic computations and facilitate the connection among sensors and between the sensors and cloud.
- **Healthcare providers**: refers to individuals or organizations that receive the functional information from the IoT gateway. Also, they analyze the health status and provide health services to the clients as need.
- **IoT Cloud**: refers to a remote database where the client's electronic health records are stored persistently.
- **Health Insurer:** refers to the insurance company which is a party in the IoT network. The insurer benefits from the accessible electronic health records of the client on the IoT cloud to issue individual health insurance policies. IoT-based collected data supports insurers to make as accurate a policy as possible.
- **Employer:** is a non-party in the IoT network. The employer already incurs health expenses

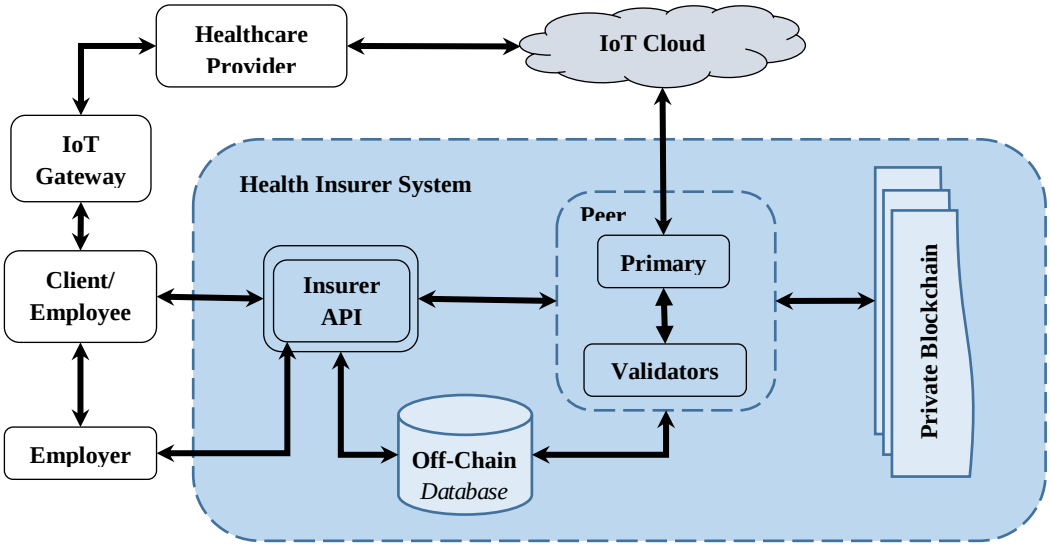

FIG. 1. THE PROPOSED NETWORK ARCHITECTURE

of employee/client in the IoT network. Thus, the employer is interested in verifying the healthcare policy of the employee accurately.

A client in the IoT network needs to obtain convenient health coverage based on his/ her IoT data and introduce trusty information about his health insurance premium to his employer.

Received 7/6/2021; Accepted 19l8l2021

 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.21.3.7

Here, the insurer presents a service to the insured employee to control the access to his insurance policy without revealing the other medical information. The authors develop a webpage that allows the insured to give provisional permissions that enable the employer to verify the financial premium of the employee. This scenario keeps the privacy of insureds and the network secure, also come back the benefits to the insurance company.

2) System Entities

This section shows the fundamental entities of the core proposed system, and their roles are as follows:

- **Peers:** refers to the participants in the network that are peer-to-peer connected. Each peer has a replica of the private Blockchain and participates in the consensus mechanism.
- **Off-chain Database:** refers to SQL Server Database that stores authentication information, It defines the authenticated insured and their public keys using database manager.
- **Private Blockchain:** refers to a private distributed ledger among peers. The Blockchain is updated using a specified consensus mechanism.
- **Smart contract:** is a program that is executed automatically. Here, it is used to retrieve the policy related to the client according to the conditions included in the smart contract.
- **Consensus mechanism:** A Blockchain-based system usually uses one of the kinds of consensus mechanism algorithms to guarantee that a transaction is legitimate, as well as, no change may occur unless the consensus and agreement of all the participants. This work uses the Practical Byzantine Fault Tolerant (PBFT) consensus mechanism algorithm to achieve commit among peers.

The PBFT algorithm is excellent for enterprises where the participants are partially trusted and doesn't include rewards. PBFT supposes one of the participants is a primary and others are validators, and number of participants as showed in equation (1):

$$n >= 3f + 1 \quad (1)$$

where n refers to the number of participants in the Blockchain network and f refers to the maximum acceptable fault of participants [25]. When some request reaches the primary and starts consensus in three main phases:

1. **Pre-prepare phase:** The primary creates a Pre-prepare message that contains the requested transaction with a unique number and sends the Pre-prepare to the rest of the validators.
2. **Prepare phase:** A validator receives a Pre-prepare message and matches the included transaction with its replica of Blockchain. If the transaction is valid, the validator sends Prepare message to all participants (including primary).
3. **Commit phase:** A validator receives Prepare message from (2f) of participants (including itself), the validator sends the Commit message to all participants.

Received 7/6/2021; Accepted 19l8l2021

 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.21.3.7

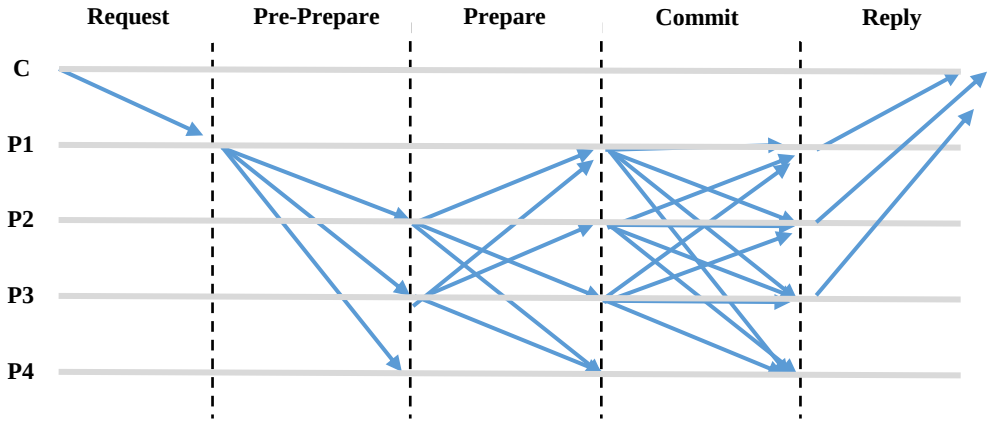

FIG. 2. FLOWCHART OF PBF MECHANISM

Each participant receives Commit messages from (2f+1) of participants (including itself), stores the transaction, and informs the client with a reply message, and *Fig.* 2 shows the main phases [25].

– **Insurer webAPI: is a web page interface that facilitates identifying insureds, submits the permissions, and verifies policy by the authorized party.**

Fig. 3 shows the webAPI and the main processes, and *Fig.* 4 shows the Peers (Primary and Validators).

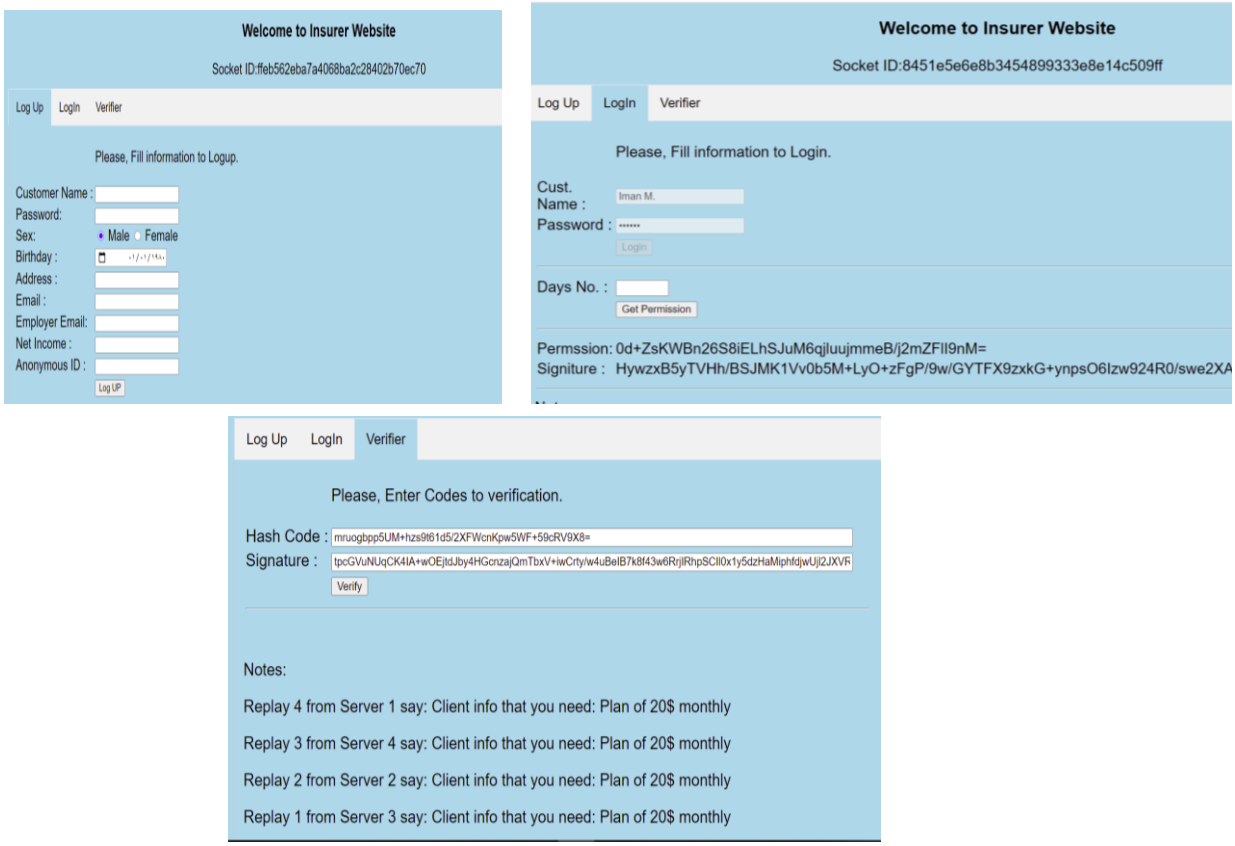

FIG. 3. WEB API DESIGN SHOW MAIN THREE SERVICES

Received 7/6/2021; Accepted 19l8l2021

DOI: https://doi.org/10.33103/uot.ijccce.21.3.7

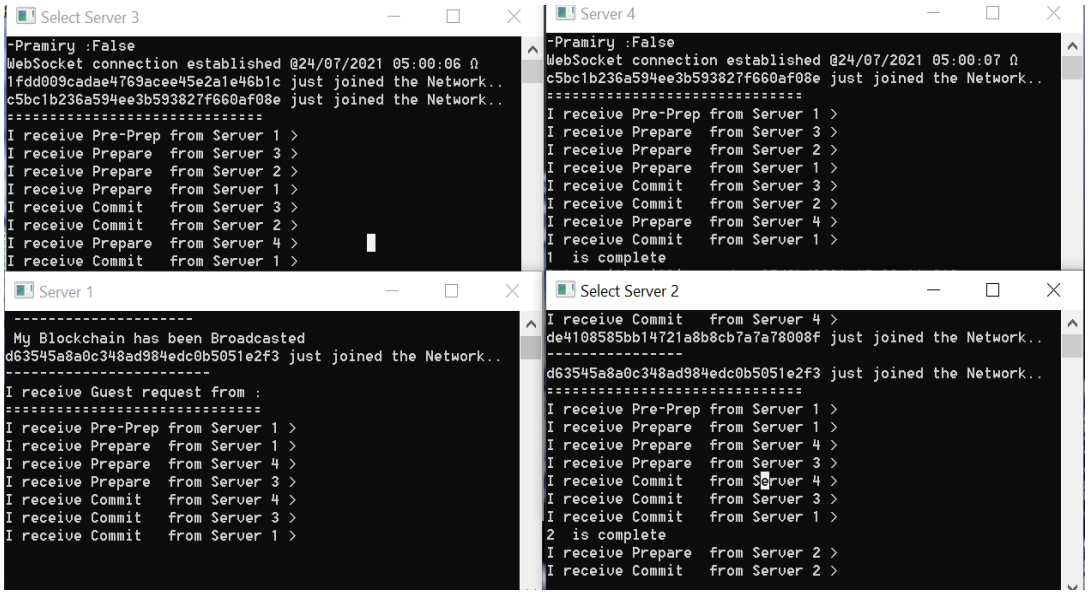

FIG. 4. SHOWS THE PEERS (PRIMARY AND VALIDATORS)

B. Goals of the model

1. Registration of a new insured and issuance of a policy.
2. Log in authenticated insured.
3. Managing access using granted permissions within an expiration time.
4. Verifying service of policies of insured employees by the authorized employer.

C. Processes Implementation

This section illustrates how to implement the fundamental processes as registration into insurer, grant permission, and verifying, as follows:

1) Registration and Issuance of an Insurance Policy

This process enables the client in the network needs to register an account and obtain an insurance policy. So From the webpage, the client fills the required personal information form and submits the form for the registration process and for issuing the individual offer as following protocol:

Phase 1: Initialization by API Agent:

The Agent collects client information like (Name, Birthday, Gender, Contacts, Public Key, and his/her Reference pointer of EHRs on the cloud). Then Agent designs and sends a registration request to the primary peer.

Phase 2: Issuance an Insurance Policy by the Primary Peer:

The primary peer receives a request for registration and an insurance policy. The primary peer checks the information and the authentication requirements. Then it retrieves the electronic health records of the client from the cloud. It calls the Policy_Generator function to generate an individual policy, fill a contract copy of policy status, and spreads the new policy transaction to the rest of the validators.

Phase 3: Add a New Policy to the Blockchain

The primary enables the PBFT algorithm to append the transaction of policy to the Blockchain. In another word, the PBFT consensus ensures that all validators commit to add the new policy on replicas of validators in the network and reply to the Agent.

Phase 4: Inform the Client of Policy's Status by the API Agent

The Agent receives responses of successful acceptance from validators then it informs the client on the webpage. Algorithm 1 illustrates the phases of the process.

Received 7/6/2021; Accepted 19l8l2021

DOI: https://doi.org/10.33103/uot.ijccce.21.3.7

Algorithm 1

```
Input: client_informaion, EHRs reference pointer , client_PK;
Output: Policy_status;
Begin (by API Agent)
1: Read client_information (Name, birth, gender, IoT_ID, Signature,
   client_PK);
2: Sends (client_informaion, Agent_address) → primary peer;
Issuance of the Policy: (by the primary peer)
3: If client_information and signature is verified Then
   a. Public_ID ← Register (client_PK, client_informaion); // by Off-Chain
   Database manager;
4: EHRs ← Retrieve(EHR_reference pointer); //from the cloud
5: Policy_Status ← Policy_Generator(EHRs);
6: Contract_policy ← Fill(Public_ID, Policy_Status);
7: Broadcast(contract_policy) → rest validators
Add contract_policy to the Blockchain (by Validators))
8: If contract_policy is valid and agreed Then  // based on PBFT Alg.
   a. Add smart_contract_policy to the replica of Blockchain;
   b. Reply Policy_status to the API_Agent;
   End;
Return Result (by Agent)
9: Receive a response from validators;
Return Policy_status to the client,
```

2) Grant Access Permission

This process enables the insured employee to grant permission for his/her Employer to access financial premiums of the health insurance policy in a fixed time without revealing the personal health information. The insured submits a request that includes expiring time of permission, as the following protocol:

Phase 1: Initialization by API Agent

The client enters the ID and Password, then the Agent queries the off-chain database manager to validate the authentication and retrieve the related identifier. Then Agent allows for the client to determine the expiring time of required permission. The Agent collects the client's identifier and sends a transaction of permission request to the primary peer.

Phase 2: Add Permission to Blockchain by Peers

The primary peer receives a request from the Agent then it creates a transaction to add permission. The transaction already includes the insured identifier and expiring time. The primary peer enables the PBFT algorithm to append the permission's transaction to the Blockchain. When all the validators consent on the validation and addition, they reply to the Agent with HashCode of transaction that contains permission.

Phase 3: Computing of Permission Keys by API Agent

The Agent receives HashCode from the validators, next it allows the client to sign HashCode using his/her secrete key. The client obtains key pair (HashCode, Signature) to be shared with the employer. Algorithm 2 illustrates the process (Grant Access Permission).

Received 7/6/2021; Accepted 19l8l2021

DOI: https://doi.org/10.33103/uot.ijccce.21.3.7

Algorithm 2

Input: *ID*, Password,*Expire_Time*, *Secret_Key*;
Output: HashCode; Signature;
Begin(by API Agent)
1: Send (ID, Password)→ off_chain database manager
2: Public_ID ← Verify (ID, Password) // by Off_Chain database manager
3: Read permission_requirements(public_ID, Expire Time,signature);
4: Send permission_requirements → Primary peer;
Verification (by Primary)
5: *If Verify (*permission_requirements,Public_Key)→ True Then
a. Contract_Permission ← Fill(public_ID, Expire Time);
b. Broadcast the Contract_Permission → rest validators;
End;
Add Contract_Permission *to Blockchain (by validators)*
6: If Contract_Permission is valid and agreed Then; // based on PBFT Alg.
a. Add Contract_Permission to the replica of Blockchain;
b. Reply(HashCode) → API_Agent; //HashCode of the Permission's transaction
End;
Return Result (by API Agent)
7: Receive HashCode from validators;
8: signature ← Sign(Hashcode,Secret_Key)
Return: HashCode, Signature;

3) Verification Service for Authorized Employer

This process enables an external party, as an employer, to verify the insurance policy of his employee. The employer needs to have authorization permission keys from the insured client as following protocol:

Phase1: Initialization by API Agent

The Employer/ Verifier enters the mutual keys HashCode along with Signature into webAPI. The Agent collects keys, creates a request, and sends it to the primary.

Phase2: Verification by validators

First, the primary peer receives an access request. Next, it broadcasts to the rest of the validators in the system based on the PBFT algorithm. Each validator participates in agreement, calls the smart contract that verifies access request, and informs the system of its agreement. Then, if the validators consent on authorized access permission, they retrieve relevant insurance policy detail and set the Result. Otherwise, the access request is ignored and sets the Result with False. Finally, Agent receives the result value and shows it to the end-user. Algorithm 3 illustrates the process (Verification Service).

Algorithm 3

Input: HashCode, Signature;
Output: insurance_policy_detail;
Begin: (by API Agent)
1: Read pair of keys (HashCode, Signature);
2: Send verification_request(HashCode, Signature)→ Primary peer;
Validation of the request (by Primary)
3: Primary receives the request(HashCode, Signature);
4: If the request → valid Then
Primary broadcasts request to rest validators;
Verification (by validators)
5: If HashCode is available Then
6: call smart_contract_verification
7: begin //smart contract for verifying permission
a. Pubic_ID, TimeExpire ← Contract_Permission(HashCode);

Received 7/6/2021; Accepted 19l8l2021

 ISSN (Print) 1811-9212 *ISSN (Online) 2617-3352*

DOI: https://doi.org/10.33103/uot.ijccce.21.3.7

```
   b.  If permission's TimeExpire > current date;
   c.  Public_Key ← retrieve_Keys(Public_ID) // by Off_Chain database manager
   d.  If verify (HashCode, Signature, Public_key)= True Then: Continue;
   e.  Else: Exit;
8: End;                          //End of smart
9: If permission is agreed then                  // based on PBFT Alg.
   Result ← retrieve the associated policy_status;
   Else: Result ← "Invalid Access Permission"
   EndIf
10: Send Reply(Result) to API Agent
Reply (by API Agent)
11: Agent receives Result;
Return Result to Employer;
```

IV. RESULTS

The proposed system is implemented and discussed using VS.net 2019. The frontend web page is implemented using HTML, CSS, and JS. The backend is implemented using ASP.net and C# to make peer-to-peer communication among four sockets on the laptop computer. Laptop features are: (ci4-4th, ram 4GB, Hard SSD, and Windows 10). The Blockchain is implemented using SQL Server Management Studio 2019. The dataset of IoT electronic health records is available online [26]. Using these settings, the proposed system is executed to evaluate the efficiency by measuring the performance; and analyze the security.

A. Performance Results

Two experiments are implemented to measure the performance of the proposed system. First, an experiment in a traditional system is used to measure multiple access requests of employers simultaneously without consensus. Next, an experiment in the authorized system is used to measure the spent time on Blockchain consensus processing for multiple access requests of employers simultaneously (*Fig.* 5*)*.

In the experiment of the authorized system, the spent time represents the period time of synchronized requests from arrival time at the primary peer until leave time from the validators nodes. This proposal includes four peers that are connected by p2p way. While a minimum number of validators that are required for validating any request is 2f+1, then the proposal achieves consensus with 1 fault and 3 acceptances. for testing the efficiency, the experiment sends (1, 10, 50, 100, 150, 200, 250, and 300) of synchronized requests and registers the spent time.

FIG. 5 shows that the authorized access spent time is longer than traditional access request processes. The maximum number of synchronized requests (300) synchronized requests spend (0.767sec) in an unauthorized system and spend (12.751sec) in the proposed authorized system. However, this increase resulted from the multiple iterations of the PBFT algorithm and Asymmetric authentication processes that confirm agreement and authorization processes. In real-time experiments, the period of 12 seconds is considered as an accepted delay compared to achieve an authorized environment.

Received 7/6/2021; Accepted 19l8l2021

 ISSN (Print) 1811-9212 *ISSN (Online) 2617-3352*

DOI: https://doi.org/10.33103/uot.ijccce.21.3.7

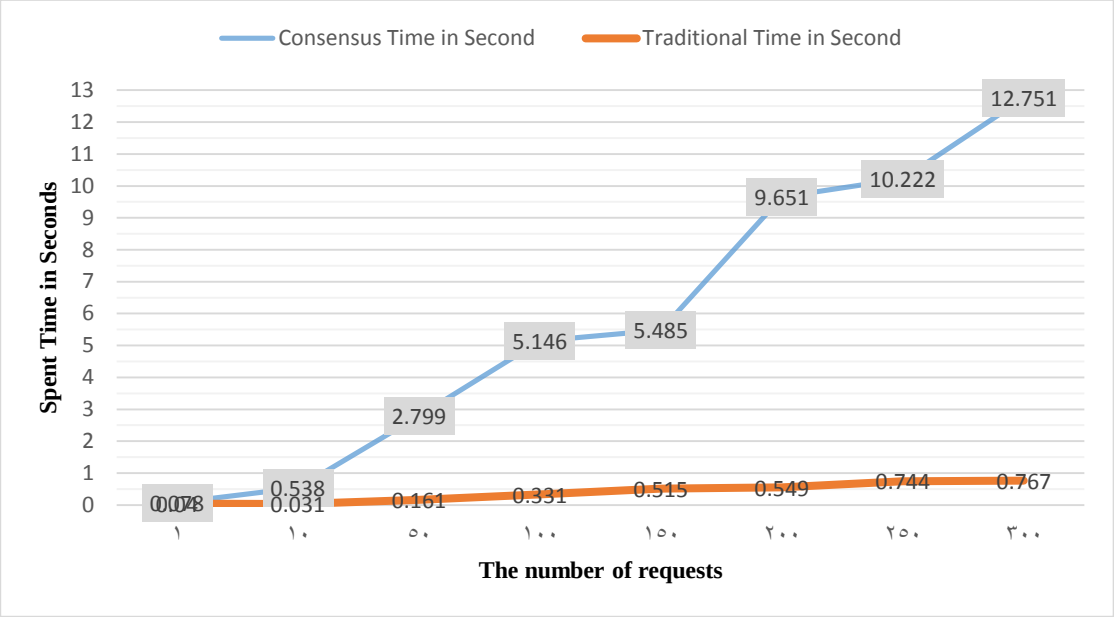

FIG. 5. SPEND TIME OF AUTHORIZATION PROCESSES ON BLOCKCHAIN FOR MULTIPLE REQUESTS

B. Security Analysis

This section presents the performance analysis of the proposed design from a security aspect. Also, Table1 presents the comparison with other relevant works that shows our scheme meets the known security requirements in the fields of Blockchain-based networks. The proposal system provides various security solutions to protect personal data on the system, as follows.

1. **Integrity**: The proposed system uses an SHA-256 algorithm that results in a unique hash value stored in the Blockchain. So the proposal system can ensure the integrity of transactions by re-computing transaction and comparing to a stored hash value.
2. **Authentication**: our system uses asymmetric encryption to ensure that only authenticated validators and insureds can enter the system.
3. **Non-repudiation**: Gain access permission must be signed with the secret key and verified with the public key to ensure that the requester of permission is the real owner of data.
4. **Single Point failure**: the distributed nature of Blockchain avoids the problem of single-point failure.
5. **Privacy**: our system provides access permission fully controlled by the owner/insured. The financial premiums are separate from medical information. Also, an unauthorized access request will be discovered by the system using a smart contract.

Received 7/6/2021; Accepted 19l8l2021

DOI: https://doi.org/10.33103/uot.ijccce.21.3.7

TABLE. 1- COMPARISON OF FUNCTIONALITY FEATURES

Feature	**[6]**	**[7]**	**[9]**	**[10]**	**[8]**	**Our**
Flexibility	✓	✓	X	X	X	✓
Single Point Of Failure	✓	✓	X	X	X	✓
Integrity	X	✓	✓	✓	✓	✓
Privacy	X	X	X	✓	X	✓
Authentication	✓	✓	✓	✓	✓	✓
User Anonymity	X	X	✓	X	X	✓
Grant and revoke permission	X	X	X	✓	X	✓
Interoperability	X	X	X	✓	✓	✓
Non-repudiation	✓	✓	✓	X	✓	✓

V. CONCLUSION

In this paper, a data-sharing system based on Blockchain has been proposed and implemented. The proposal aims to achieve authorized access controlled by the data owner without revealing medical information. A web API has been designed that facilitates the communication between the user side and the system. The experimental results of the system produced authorized access in an accepted spent time. The security analysis displayed the proposal's ability to protect data security and integrity and avoid potential threats.

REFERENCES

[1] M. van Steen and A. S. Tanenbaum, *Distributed Systems*, 3rd ed., vol. 02. Leiden, The Netherlands: Maarten van Steen, 2018.

[2] A. S. Tanenbaum and D. J. Wetherall, *Computer Networks*, 5th ed. 2011.

[3] D. T. Patel, "Distributed Computing for Internet of Things (IoT)," in *Computational intelligence in the internet of things*, IGI Global, 2019, pp. 84–109.

[4] IoTNews, "What is IoT and why does it matter? - IoT Tech Expo | Internet of Things," Aug. 23, 2019. https://www.iottechexpo.com/2019/08/iot/what-is-iot-why-does-iot-matter/ (accessed Feb. 26, 2021).

[5] M. Dakhel and S. Hassan, "A Secure Wireless Body Area Network for E-Health Application Using Blockchain," in *Communications in Computer and Information Science*, vol. 1174 CCIS, no. January, Springer, Cham, 2020, pp. 395–408.

[6] M. Raikwar, S. Mazumdar, S. Ruj, S. Sen Gupta, A. Chattopadhyay, and K.-Y. Lam, "A Blockchain Framework for Insurance Processes," in *9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), IEEE*, 2018, pp. 1–4, doi: 10.1109/NTMS.2018.8328731.

[7] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Blockchain for Secure EHRs Sharing of Mobile Cloud Based E-Health Systems," *IEEE Access*, vol. 7, pp. 66792–66806, 2019, doi: 10.1109/ACCESS.2019.2917555.

[8] L. Chen, W.-K. Lee, C.-C. Chang, K.-K. R. Choo, and N. Zhang, "Blockchain based searchable encryption for electronic health record sharing," *Futur. Gener. Comput. Syst.*, vol. 95, pp. 420–429, Jun. 2019, doi: 10.1016/j.future.2019.01.018.

[9] X. Xiang, M. Wang, and W. Fan, "A Permissioned Blockchain-Based Identity Management and User Authentication Scheme for E-Health Systems," *IEEE Access*, vol. 8, pp. 171771–171783, Sep. 2020, doi: 10.1109/access.2020.3022429.

[10] K. Salah, P. P. Ray, D. Dash, and N. Kumar, "Blockchain for IoT-Based Healthcare: Background, Consensus, Platforms, and Use Cases," *IEEE Syst. J.*, pp. 1–10, Jan. 2020, doi: 10.1109/jsyst.2020.2963840.

[11] E. Schneider, "Internet Of Things (IoT) Technology, Economic View And Technical Standardization," *Inst. Luxemb. la Norm.*, vol. 1.0, no. July, p. 108, 2018, [Online]. Available: https://portail-qualite.public.lu/dam-assets/publications/normalisation/2018/white-paper-iot-july-2018.pdf.

Received 7/6/2021; Accepted 19l8l2021

DOI: https://doi.org/10.33103/uot.ijccce.21.3.7

[12] K. K. Patel, S. M. Patel, and P. G. Scholar, "Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges," *Int. J. Eng. Sci. Comput.*, vol. 6, no. 5, 2016, doi: 10.4010/2016.1482.

[13] A. Salman Dawood, "Internet of Things (IoT) and its Applications: A Survey," *Int. J. Comput. Appl.*, vol. 175, no. 21, pp. 975–8887, 2020, doi: 10.5120/ijca2020919916.

[14] S. A. Alshammari and S. A. Hosseini Seno, "A Cooperation of Fog Computing and Smart Gateways in a Secure and Efficient Architecture for IoT-Based Smart Homes," *Eng. Technol. J.*, vol. 37, no. 7 A, pp. 290–301, 2019, doi: 10.30684/etj.37.7A.10.

[15] M. S. Mahdi, N. F. Hassan, and G. H. Abdul‐Majeed, "An improved chacha algorithm for securing data on IoT devices," *SN Appl. Sci.*, no. August 2020, 2021, doi: 10.1007/s42452-021-04425-7.

[16] G. Hileman and M. Rauchs, *2017 Global Blockchain Benchmarking Study*. Cambridge Centre for Alternative Finance, 2017.

[17] J. Owens, *Blockchain 101 For Governments*, no. October. Vienna: Wilton Park, 2017.

[18] T. Mikula and R. H. Jacobsen, "Identity And Access Management With Blockchain In Electronic Healthcare Records," in *Proceedings - 21st Euromicro Conference on Digital System Design, DSD 2018*, Aug. 2018, pp. 699–706, doi: 10.1109/DSD.2018.00008.

[19] Z. Suhiar Mohammed and R. Abdul Monem Saleh, "Healthcare System Technology using Smart Phones and Web Apps (Case Study Iraqi Environment)," *Int. J. Eng. Manuf.*, vol. 7, no. 3, pp. 1–7, May 2017, doi: 10.5815/ijem.2017.03.01.

[20] R. S. Abd-ali, S. M. Al-qaraawi, and M. S. Croock, "Web Based E-Hospital Management System," *Iraqi J. Comput. Commun. Control Syst. Eng.*, vol. 18, no. 1, pp. 11–28, 2018, doi: 10.33103/uot.ijccce.18.1.2.

[21] World Health Organization, "Thirteenth General Programme Of Work 2019–2023," 2019. Accessed: Mar. 02, 2021. [Online]. Available: https://www.who.int/about/what-we-do/thirteenth-general-programme-of-work-2019---2023.

[22] R. E. Berchick, J. C. Barnett, and R. D. Upton, "Health Insurance Coverage in the United States: 2018," *U.S. Gov. Print. Off. DC*, no. September, pp. 60–267, 2019, [Online]. Available: https://www.census.gov/content/dam/Census/library/publications/2019/demo/p60-267.pdf.

[23] "Health Insurance Definition." https://www.investopedia.com/terms/h/healthinsurance.asp (accessed Mar. 02, 2021).

[24] A. Silvello and A. Procaccini, "Connected Insurance Reshaping the Health Insurance Industry," in *Smart Healthcare*, IntechOpen, 2020.

[25] I. M. Al-Joboury and E. H. Al-Hemiary, "Consensus Algorithms Based Blockchain of Things for Distributed Healthcare," *Iraqi J. Inf. Commun. Technol.*, vol. 3, no. 4, pp. 33–46, 2020, doi: 10.31987/ijict.3.4.116.

[26] "Quantitative Dehydration Estimation," *PhysioNet*. https://physionet.org/content/qde/1.0.0/ (accessed Mar. 06, 2021).

Received 7/6/2021; Accepted 19l8l2021