Computer Systems Science & Engineering
DOI: 10.32604/csse.2023.024884
Article

Tech Science Press

Hybrid Smart Contracts for Securing IoMT Data

D. Palanikkumar[1], Adel Fahad Alrasheedi[2], P. Parthasarathi[3], S. S. Askar[2] and Mohamed Abouhawwash[4,5,*]

[1]Department of Computer Science and Engineering, Dr NGP Institute of Technology, Coimbatore, 641048, India
[2]Department of Statistics and Operations Research, College of Science, King Saud University, Riyadh, 11451, Saudi Arabia
[3]Department of Computer Science and Engineering, Bannari Amman Institute of Technology, Sathy, 638401, India
[4]Department of Mathematics, Faculty of Science, Mansoura University, Mansoura, 35516, Egypt
[5]Department of Computational Mathematics, Science, and Engineering (CMSE), Michigan State University, East Lansing, MI, 48824, USA
*Corresponding Author: Mohamed Abouhawwash. Email: abouhaww@msu.edu

Received: 03 November 2021; Accepted: 07 January 2022

Abstract: Data management becomes essential component of patient healthcare. Internet of Medical Things (IoMT) performs a wireless communication between E-medical applications and human being. Instead of consulting a doctor in the hospital, patients get health related information remotely from the physician. The main issues in the E-Medical application are lack of safety, security and privacy preservation of patient's health care data. To overcome these issues, this work proposes block chain based IoMT Processed with Hybrid consensus protocol for secured storage. Patients health data is collected from physician, smart devices etc. The main goal is to store this highly valuable health related data in a secure, safety, easy access and less cost-effective manner. In this research we combine two smart contracts such as Practical Byzantine Fault Tolerance with proof of work (PBFT-PoW). The implementation is done using cloud technology setup with smart contracts (PBFT-PoW). The accuracy rate of PBFT is 90.15%, for PoW is 92.75% and our proposed work PBFT-PoW is 99.88%.

Keywords: PoW; byzantine fault tolerance; IoMT; cloud computing; health care data

1 Introduction

Internet of Medical Things (IoMT) uses smart devices to collect medical data. In the health care system, IoMT plays an important role in providing security, accessing physicians, remote lab access and transmitting health care data electronically. It also provides real time-medical services like consulting physicians, through web and mobile applications. The benefits of IoMT are reducing the cost of health care data, faster decision-making process. Timely responses from the physicians and improvise in quality of health care treatment [1]. In smart health care data management system, real time health data is collected through medical sensors. Physicians can monitor the patient's health status through collected data [2]. Patient's sensitive information are stored in blockchain securely. To provide high dimensional security and transmitting data in a secure manner it needs to detect unauthorized users and prevent them to access the data. It ensures the integrity, validity, authenticity and preserving privacy in health data [3].

Patient's requests are analyzed using a web application. The smart contract is a mediator to transfer health data between physician and patient in a secured manner [4]. A medical data transaction between two or more parties using blockchain in a secure manner without check for validity process is a key concern. In the decentralized blockchain network, each and every node contains copy of medical data and updates the content of nodes in the network [5,6]. Research works have been done in managing of health care data in a secure way. The main drawback of existing algorithm is lower-level security, unscalable, computation time is high. To overcome these issues this paper proposes PBFT-PoW. It gives double layer of security in high level, scalable, faster in access of health data in the blockchain network.

The consensus algorithm is used in open public blockchain technology such as Proof-of-Authority (PoAu), Proof-of-Work (PoW), Byz Coin, Delegated Proof-of-Stake (DPoS), Proof-of-Stake (PoS), Leased Proof-of-Stake (LPoS), Omni Ledger, Elastico, Proof-of-Burn (PoB). The main drawbacks in the open public blockchain are current state value cannot compete with existing system.

Private blockchain is called as permissioned blockchain in which Delegated Practical Byzantine Fault Tolerance (DPBFT), Practical Byzantine Fault Tolerance (PBFT), Proof-of-Elapsed-Time (PoET), Tender mint, RS Coin, Raft consensus protocols and Pore are used. For accessing the medical data this private blockchain network needs permission to access, contribute and transfer the medical data from one node to another node in the blockchain network. It provides higher levels of security, preserving privacy and accessed by authorized users only. They are also highly scalable because it needs only few nodes for managing the medical data. These characteristics makes the private blockchain network as optimal in the IoMT network. In the private blockchain network, parameters such as medical data size, accessing speed, trust preserving privacy, scalability is the much better than public blockchain network [7,8]. The contribution of this work is:

1. To implement consensus algorithm of Practical Byzantine Fault Tolerance with PoW (Proof of Work) (PBFT-PoW) to provide high level security in accessing of health care record in the blockchain network.

2. Evaluate the performance metric measures of Block propagation time, latency, energy consumption and accessing time.

3. Smart contracts are implemented in the verification of health care data to facilitate the identification and authorization of the user.

The paper has been organized as follows: Section 2 describes the review of literature; Section 3 introduces Secure Storage of Patient's Health Care Data Management in IoMT Using Blockchain technology, Section 4 discusses about the experimented results and Section 5 concludes the paper with future directions.

2 Review of Literature

Recently blockchain has been used in various security domains to store and process the data. In the article [9]. blockchain based applications is surveyed and its potentiality is studied briefly. Blockchain has been used in several applications like education, healthcare, share market, stock Exchange etc. Various opportunities and challenges in the block chain at different domains are discussed. The consensus algorithms used in blockchain like proof of work, proof of stack etc., was studied. This article helps to know the future research scope in blockchain security. Block chain characteristics [10] with the benefits are identified in different domains other than bit coin. Technical challenges in consensus protocol like scalability, privacy leakage, security challenges are discussed for proof of work and proof of stack.

The advanced internet communities like smart city, smart nation and smart vehicles etc. IoT devices can be placed in various locations of geographical region. Creation of Block chain, verification of blockchain using consensus algorithm and cryptographic techniques are discussed [11]. Communication support using wireless and wired networks in block chain is studied and 5G support efficiently. Smart home IoT device is rapidly increased due to advancement in internet technology in providing security [12]. Risk assessment on remote data access is focused on this research work. Remote data authentication using blockchain, signatures and authentication secret codes are presented in this article. The secure data communication using grid system based on mutual authentication is discussed in paper [13]. Privacy is ensured using key management in smart meter. In this research they use signature keyless method in blockchain. Result shows cost effective, robust, and scalable in providing security.

Block chain technology in paper [14] used in secured data access of internet of vehicles (IoV). IoV is most significant mobile based application used in real time traffic management, speed control alert, direction alert, accidents etc. Consensus algorithm is used in blockchain for secured transmission. Key distribution technique is used for formation of new nodes in block chain. The resource limitation in IoT is overcome by using outsourcing bilinear pairing with permission blockchain [15]. Major potential of permission blockchain is security, scalability, and availability. The new tactile internet in paper [16] is used for intelligent transport energy trading system. Blockchain was used in providing security of energy trading.

Electrical vehicle uses blockchain for secured energy trading based on the request. SDN architecture is used for effective computation with less latency.

VANET was communicated with environment *via* wireless medium for efficient monitoring technique. Major advantages like weather monitor during emergency, intelligent path management etc. They proposed a blockchain with privacy assistance [17] using authentication technique for vehicle data. It helps to monitor the behavior of vehicle and communication records are traced. Block chain advantages and effectiveness is surveyed in article [18]. It states the importance on consensus algorithm with its principal and performance analysis. Different algorithm on consensus protocol is used to check the performance. Group decision is suggested in reaching consensus was implemented in paper [19]. It initiates and proposes minimum cost soft model in consensus algorithm. it is used in loan problem. The symmetric and asymmetric cryptographic method is used as hybrid scheme in blockchain technology [20]. It combines both techniques to provide efficient security in data storage. The IoT are now days used wide variety applications like nano robots, nano technology etc. internet of nano health care [21,22] applications required high security infrastructure for medical data process.

The limitations of above literature work are still need of additional security and do not support dynamic entry of device in the network. some technology does not support blockchain concepts and some research works are insecure when the devices are stolen.

3 Proposed PBFT-PoW Methodology

Storing of patient's health care data electronically, in the IoMT by using sensor devices, wearable devices status of patient's health details is collected based upon some predefined parametric measures of oxygen saturation, pulse rate, calories, temperature, Blood sugar etc. These data are collected from wearable devices and permanently stored in Ethereum based blockchain technology. All patient's health status is a sensitive information, and it must be kept in safe and more confidential one. This paper proposes Ethereum blockchain technology of smart contracts with various consensus protocols of Practical Byzantine Fault Tolerance, PoW (PBFT-PoW). Fig. 1. shows that architecture of PBFT-PoW.

This PBFT-PoW is composed of sensor and wearable devices that connect with web application as well as mobile application which collects and monitors the patient's health care data.

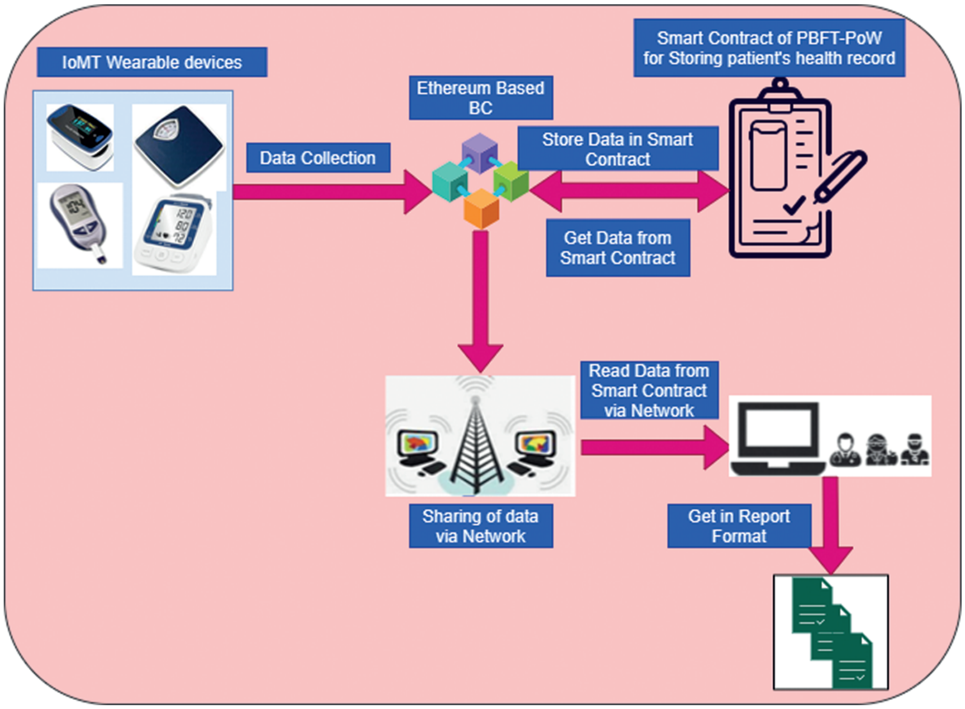
IoMT Wearable devices
Data Collection
Ethereum Based BC
Smart Contract of PBFT-PoW for Storing patient's health record
Store Data in Smart Contract
Get Data from Smart Contract
Read Data from Smart Contract via Network
Sharing of data via Network
Get in Report Format

Figure 1: Architecture of PBFT-PoW

3.1 Wearable Devices

To capture the patient's health care information based on predefined parametric measures of oxygen saturation, pulse rate, calories, temperature, Blood sugar etc. These devices are transforming the collected data with web and mobile applications through ZigBee and Bluetooth.

3.2 Ethereum Based Blockchain

Each and every node in the blockchain represents the physicians, health caretaker etc. In this work we are implementing the Ethereum based blockchain network. It is decentralized ledger in which patient health care data is stored and manage the data through mobile application and web application. For each patient's registration the transaction of health care data is validated and stored in smart contract. Physicians add the patient's health care data in the block of the blockchain.

3.3 Mobile Application and Web Application

The medical data collected from wearable devices are stored in Ethereum based blockchain network. And it is accessed by patient or physicians *via* web application or mobile application. The data is uploaded in the blockchain every three hours or based upon the request.

3.4 Smart Contract with PBFT and PoW Consensus Algorithm

In this proposed work, each patient's health care data is collected from wearable devices and stored in the patient's smart contract. The Ethereum based smart contracts with consensus protocols of practical Byzantine Fault Tolerance, PoW.

3.4.1 Practical Byzantine Fault Tolerance in Smart Contract

Algorithm 1: PBFT in Health Care Data Management

```
Input: Patient (IoMT_patient 1) ; doctor (IoMT_Doctor 1)
Output: Secure or not
Step 1: Send request HCD(Primary_Node)← Patient (IoMT_patient 1)
Step 2: HCD(Secondary_Node)←HCD(Primary_Node) // Primary node send request to
                                                  all back up nodes.
Step 3: For each node ni from HCD // ni is number of nodes
Step 4: Patient (IoMT_patient )←HCD( 〖Primary_Node〗 _i),HCD( 〖Secondary_Node〗 _i)
Step 5: If Patient (IoMT_patient ) ≥M // M is maximum number of faulty nodes
Step 6: Request is Successful.
Step 7: Patient Health care Data Block is safe.
```

PBFT is a distributed system and nodes are arranged in sequential order. It contains only one is called leader node or primary node and remaining other nodes are called as back up nodes or secondary nodes. Through leader node health care data is transferred to back up nodes. If primary node gets fail by using majority rule remaining all honesty nodes helps to reach the state. The malicious nodes of PBFT system must not greater than or equal to one-third of all nodes. If number of nodes increase, then the system gets more secure [23]. The algorithm for PBFT is given above.

3.4.2 PoW Consensus Algorithm in Smart Contract

It provides more secure to the health care data in the blockchain network.

Algorithm 2: PoW in Health Care Data Management

```
While (patient) _iin HCD(patient) do
Select (patient)_i
If (patient)_i∈HCD( (patient)_list)
For eachHCD((data)_i) in IoMT do
If (device)_i select HCD((data)_i) then //Check for validity
Retrieve HCD ((patient)_i, HCD((data)_i))
Store in PBFT-PoW(block_HCD)
Else
Display "Unauthorized User"
End If
  End For
End If
End
```

In the algorithm 2, smart contract act as a finite state machine and executes the instruction in the dynamic form. When data requested from the patient or physician smart contracts monitor authorized user or not and give rights to access it and stored it in block of the blockchain network.

3.5 Smart Contracts Consensus Protocols of PBFT- PoW

To create Ethereum based blockchain this proposed work has two types of consensus protocols and it is used to improve more secure in the storage of health care data in the blockchain this PBFT-PoW consensus algorithm is used. The features of this PBFT-PoW consensus algorithm are given in Tab. 1.

Table 1: Features of PBFT-PoW

Features	PBFT	PoW
Permissioned storage	Yes	No
Public storage	No	Yes
Private storage	Yes	No
Consumption of Energy	Low	High
To create a Block High processing power	No	Yes
Trust Free	Yes	Yes
Transaction time	Very Fast	Slow

Form the Tab. 1, Practical Byzantine Fault Tolerance (PBFT) enhances very fast transactions with low consumption of energy, but it provides high security. It's a private blockchain, to access health care data it needs permission. In the proof of work (PoW) it's a public blockchain network no need to get permission. When executing a node in the blockchain network it accesses the health care data and ether transmit the transaction between physician or patient with network. It takes more time to transmit the data and consumption of energy is also high. To overcome these issues, this proposed work implements the transaction of health care data in the Ethereum blockchain network gives less transaction time, high security. Fig. 2 shows that workflow of PBFT- PoW.

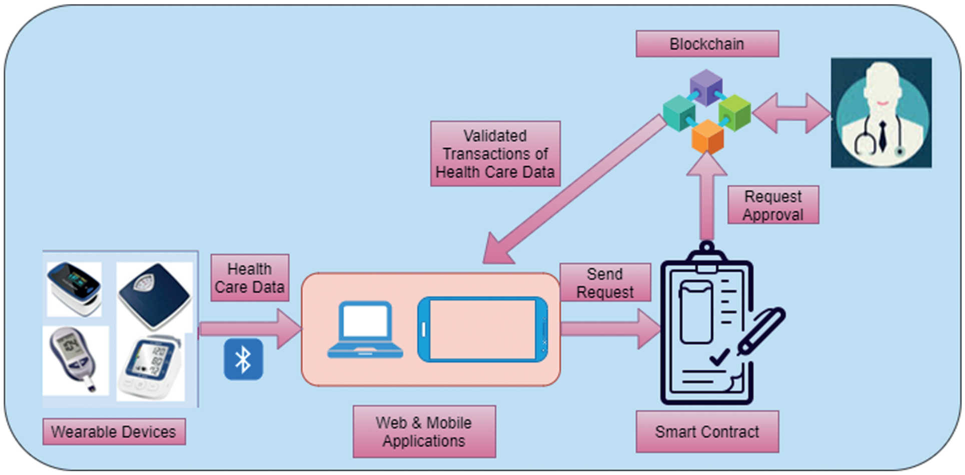

Figure 2: Workflow of PBFT- PoW

This proposed work contains two phases:

Phase 1: Upload Health care Data using PBFT- PoW

Phase 2: Read the Health Care DataPBFT- PoW

3.5.1 PoW Consensus Algorithm in Smart Contract

Algorithm 3: Uploading the health care data using PBFT- PoW

```
Input: Request from smart contract to upload the health care data
Output: E-Health care data is added to the smart contract
Step 1: Using Algorithm 1, ReadPatient (IoMT_patient 1)
Step 2: IF HCD (data)==owner (HCD (data))
Step 3: Check for validity using Algorithm 2
Step 4: Generate health care data of HCD (data)
Step 5: Push HCD (data) into the Blockchain
Step 6: Return HCD (data) is uploaded successfully
Step 7: Else
Step 8: Return unauthorized access of HCD (data)
Step 9: End IF
```

This describes the process of uploading or storing health care data in the Ethereum based blockchain. Data collected from wearable devices and stored it in the blockchain.

In the algorithm 3, get the new patient heath care data from the wearable devices and send it to blockchain and verify by PBFT- PoW consensus algorithm. If it is verified successfully then new health care data (HCD) will be added to the smart contract.

3.5.2 Read the Health Care Data PBFT- PoW

From the Algorithm 4, health care data is stored in the smart contract is accessed by only authorized patients. Request send by the patient *via* web application or mobile application to smart contract. This request will verify by the smart contract and response will be given to the authorized patient only. The algorithm is given below:

Algorithm 4: Reading the health care data using PBFT- PoW

```
Input: Request send to smart contract to read the health care data
Output: Accessing Health care Data
Step 1: If Patient (IoMT_patient 1)∈(list_patient)
Step 2: convert HCD (data) into string
Step 3: Return Patient (IoMT_patient 1)←HCD (data)
Step 4: ElseIf Patient (IoMT_patient 1)∈(list_Dieticians)
```

(Continued)

Algorithm 4 (continued).

```
Step 5: convert HCD (data) into string
Step 6: ReturnPatient (IoMT_patient 1)←HCD ( 〖data〗 _diet)
Step 7: ElseIf Patient (IoMT_patient 1)∈(list_physiotherapist)
Step 8: convert HCD (data) into string
Step 9: ReturnPatient (IoMT_patient 1)←HCD ( 〖data〗 _physio)
Step 10: Else
Step 11: Return Unauthorized access
Step 12: End If
```

In algorithm 4, which checks for the authorized patient are in the list and give rights to access all information data from the block in the blockchain *via* smart contract.

4 Result Analysis

This blockchain based secure storage of patient's health care data management in IoMT is implemented by using PBFT-PoW. It's a double layer concept of providing security. In the blockchain technology set of blocks which contains patient's health care data in a secure manner. Fig. 3 shows that performance analysis of energy consumption using various algorithms.

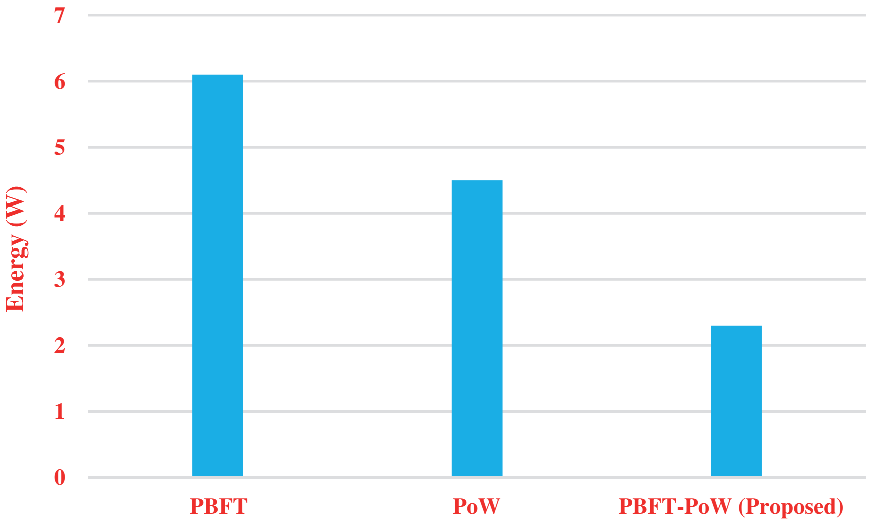

Figure 3: Energy consumption

In the Fig. 3. shows that our proposed work got low energy consumption compared it with other existing algorithms of PBFT and PoW. Tab. 2 shows the comparison of PBFT-PoW with parametric attributes with our proposed work.

Table 2: Comparison of PBFT-PoWin terms of characteristics

Attributes	Ying Z. et al. [24]	Ramani V. et al. [25]	Xia Q.I. et al. [26]	Liang X. et al. [27]	PBFT-PoW
Health care data in Privacy	Yes	Yes	Yes	Yes	Yes
Availability of data	No	No	Yes	Yes	Yes
Integrity of data	Yes	Yes	Yes	Yes	Yes
Authentication	Yes	Yes	Yes	No	Yes
Decentralized access	No	Yes	Yes	Yes	Yes
Flexibility of data	No	No	No	Yes	Yes

From the Tab. 2, our proposed work PBFT-PoW supports with all attributes of blockchain based IoMT compared it with other existing work, and it offers promising solution in Health care data management [28–36]. The blockchain with decentralized security model using smart contracts enable to manage the patients' health care data. This PBFT-PoW work is evaluated using following performance parameter.

4.1 Latency

Latency in PBFT-PoW has been calculated by analyzing the time taken to access a patient health care data. The latency for PBFT-PoW is represented in Tab. 3.

Table 3: Latency for PBFT-PoW

Number of users request	Latency (Sec)
10	88.23
20	120.54
40	232.67
60	320.98
80	480.21
100	625.89

In the observation of Latency in Tab. 3, if user's request increases to access the of patient health care data latency time also increases.

4.2 Throughput

In this performance parameter, it is the rate at which valid transactions of IoMT medical data are committed by the blockchain as per Eqs. (1), (2) AND Eq. (1).

$$transaction\ per\ block = (blocksize)/(average\ transactionsize) \tag{1}$$

$$fraction\ of\ block\ per\ second = 1/(blocktimeinseconds) \tag{2}$$

$$transaction\ per\ block = transcation\ per\ block * fraction\ of\ block\ per\ second \tag{3}$$

This throughput parameter is compared with Blockchain with decentralized storage, and PBFT-PoW. Fig. 4 shows the comparison of throughput for Blockchain with decentralized using smart contract and PBFT-PoW using smart contract.

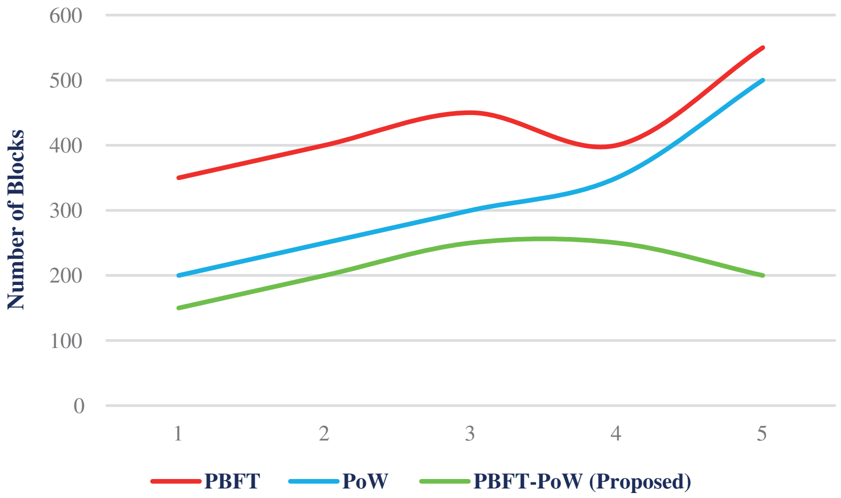

Figure 4: Throughput

In the Fig. 4, If the number of blocks increases within certain period of time, our proposed work gives prominent result.

4.3 Block Propagation Time (BPT)

It is a time taken to distribute the new block with the majority set of nodes in the cloud network. After verification process taken place using algorithm 2, the propagation time for each block is given in Fig. 5.

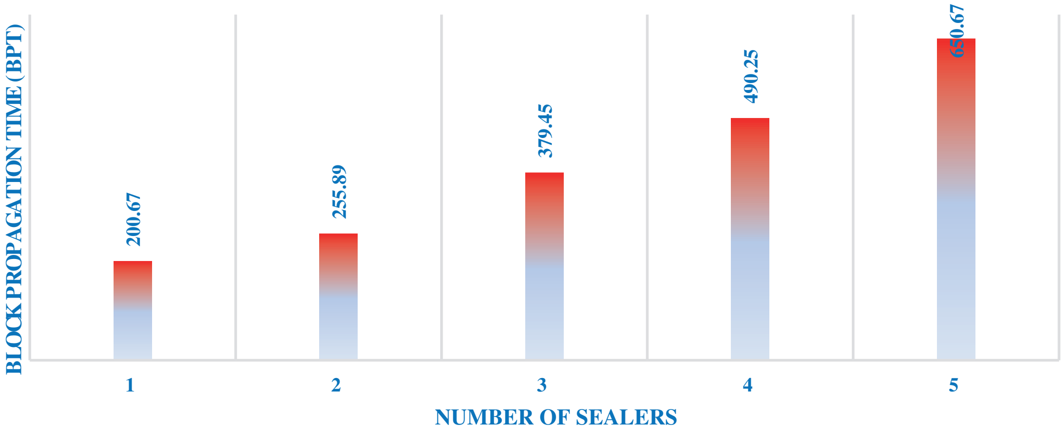

Figure 5: Block propagation time

Form the Fig. 5. BPT is calculated by number of sealers in the network. If number of sealers increases in the network, then synchronization issues occur. It leads to higher propagation delay in the network. Health care data is accessed from blockchain network in IoMT produces the optimized accessing time of medical records. Additionally, number of user's requests increases will lead to average response time also increases. Tab. 4 shows the result obtained by using proposed work (PBFT-PoW)

Table 4: Result obtained by proposed method (PBFT-PoW)

Average access time(ms)			
Total request	PBFT	PoW	PBFT-PoW
1	31.06	35.76	15.87
10	235.02	278.45	175.67
20	375.61	445.23	225.13
50	467.08	578.78	313.56
100	874.12	957.38	763.13

From the observation of Tab. 4. our proposed work produces better result in accessing time of health care records from the decentralized blockchain network. Fig. 6 shows that accuracy rate of executing these consensus algorithms.

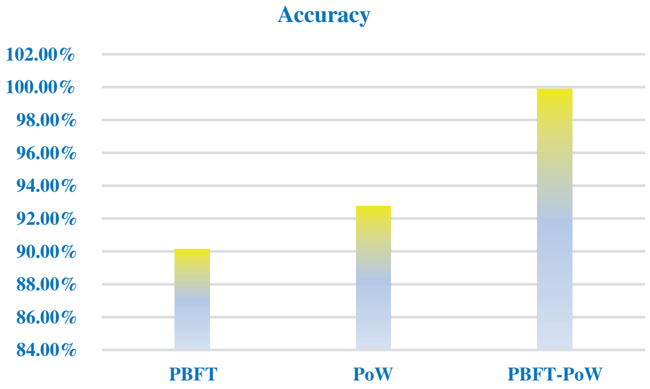

Figure 6: Accuracy rate

From the observation of Fig. 6 shows that our proposed algorithm gives better accuracy rate in the execution of algorithm as well as gives the prominent result.

5 Conclusion

This paper proposes PBFT-PoW using smart contract in health care data are stored in the cloud network, where data collected from wearable devices. Health care data is stored in decentralized and provides security, scalability, preserve privacy and effectively. The experimental results show that PBFT-PoW achieves transmitting of health care data between physician/user. This PBFT-PoW of HCD access control system protects patient health care data from external attacks. Our proposed work requires minimum consumption time when it is compared with existing algorithm. This PBFT-PoW is a decentralized storage of data and which preserves data privacy. In order to get the optimized solution for PBFT-PoW number of sealers should be less than nodes in the network. It minimizes the delay in synchronization and propagation. The accuracy rate of PBFT is 90.15%, for PoW is 92.75% and our proposed work PBFT-PoW is 99.88%. In future this PBFT-PoW will be improving in terms of reducing number of replicas, involving various protocols.

Acknowledgement: Research Supporting Project number (RSP-2021/323), King Saud University, Riyadh, Saudi Arabia.

Funding Statement: This project is funded by King Saud University, Riyadh, Saudi Arabia.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] N. Garg, M. Wazid, A. K. Das, D. P. Singh, J. J. Rodrigues *et al.,* "BAKMP-IoMT: Design of blockchain enabled authenticated key management protocol for internet of medical things deployment," *IEEE Access*, vol. 8, pp. 95956–95977, 2020.

[2] G. G. Dagher, J. Mohler, M. Milojkovic and P. B. Marella, "Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology," *Sustainable Cities and Society*, vol. 39, no. 1, pp. 283–297, 2018.

[3] W. Sun, Z. Cai, Y. Li, F. Liu, S. Fang *et al.,* "Security and privacy in the medical internet of things: A review," *Security and Communication Networks*, vol. 2018, no. 5, pp. 1–9, 2018.

[4] M. Vaishnnave, K. S. Devi and P. Srinivasan, "A survey on cloud computing and hybrid cloud," *International Journal of Applied Engineering Research*, vol. 14, no. 2, pp. 429–434, 2019.

[5] S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han *et al.,* "Blockchain-enabled smart contracts: Architecture, applications, and future trends," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 49, no. 11, pp. 2266–2277, 2019.

[6] F. Restuccia, S. D. Kanhere, T. Melodia and S. K. Das, "Blockchain for the internet of things: Present and future," Arxiv Preprint Arxiv:1903.07448, 2019.

[7] S. Rouhani and R. Deters, "Performance analysis of ethereum transactions in private blockchain," in *Proc. 2017 8th IEEE Int. Conf. on Software Engineering and Service Science (ICSESS)*, Beijing, China, IEEE, pp. 70–74, 2017.

[8] J. Liu, X. Li, L. Ye, H. Zhang, X. Du *et al.,* "BPDS: A blockchain based privacy-preserving data sharing for electronic medical records," in *Proc. 2018 IEEE Global Communications Conf.*, Abu Dhabi, UAE, IEEE, pp. 1–6, 2018.

[9] A. A. Monrat, O. Schelén and K. Andersson, "A survey of blockchain from the perspectives of applications, challenges, and opportunities," *IEEE Access*, vol. 7, pp. 117134–117151, 2019.

[10] Z. Zheng, S. Xie, H. N. Dai, X. Chen and H. Wang, "Blockchain challenges and opportunities: A survey," *International Journal of Web and Grid Services*, vol. 14, no. 4, pp. 352–375, 2018.

[11] S. Aggarwal, R. Chaudhary, G. S. Aujla, N. Kumar, K. K. R. Choo *et al.,* "Blockchain for smart communities: Applications, challenges and opportunities," *Journal of Network and Computer Applications*, vol. 144, no. 5, pp. 13–48, 2019.

[12] C. Lin, D. He, N. Kumar, X. Huang, P. Vijayakumar *et al.,* "Homechain: A blockchain-based secure mutual authentication system for smart homes," *IEEE Internet of Things Journal*, vol. 7, no. 2, pp. 818–829, 2019.

[13] H. Zhang, J. Wang and Y. Ding, "Bloc kchain-based decentralized and secure keyless signature scheme for smart grid," *Energy*, vol. 180, no. 2, pp. 955–967, 2019.

[14] X. Wang, P. Zeng, N. Patterson, F. Jiang and R. Doss, "An improved authentication scheme for internet of vehicles based on blockchain technology," *IEEE Access*, vol. 7, pp. 45061–45072, 2019.

[15] C. Lin, D. He, X. Huang, X. Xie and K. K. R. Choo, "Blockchain-based system for secure outsourcing of bilinear pairings," *Information Sciences*, vol. 527, no. 4, pp. 590–601, 2020.

[16] R. Chaudhary, A. Jindal, G. S. Aujla, S. Aggarwal, N. Kumar *et al.,* "BEST: Blockchain-based secure energy trading in SDN-enabled intelligent transportation system," *Computers & Security*, vol. 85, no. 1, pp. 288–299, 2019.

[17] Q. Feng, D. He, S. Zeadally and K. Liang, "BPAS: Blockchain-assisted privacy-preserving authentication system for vehicular ad hoc networks," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 4146–4155, 2019.

[18] A. Jindal, G. S. Aujla and N. Kumar, “Survivor: A blockchain based edge-as-a-service framework for secure energy trading in SDN-enabled vehicle-to-grid environment,” *Computer Networks*, vol. 153, no. 1, pp. 36–48, 2019.

[19] D. Mingxiao, M. Xiaofeng, Z. Zhe, W. Xiangwei and C. Qijun, “A review on consensus algorithm of blockchain,” in *Proc. 2017 IEEE Int. Conf. on Systems, Man, and Cybernetics*, Banff Center, Banff, Canada, IEEE, pp. 2567–2572, 2017.

[20] H. Zhang, G. Kou and Y. Peng, “Soft consensus cost models for group decision making and economic interpretations,” *European Journal of Operational Research*, vol. 277, no. 3, pp. 964–980, 2019.

[21] D. Rathee, K. Ahuja and A. Nayyar, “Sustainable future IoT services with touch enabled handheld devices,” *Security and Privacy of Electronic Healthcare Records: Concepts, Paradigms and Solutions*, vol. 131, pp. 131–152, 2019.

[22] P. K. Pramanik, D. Solanki, A. Debnath, A. Nayyar, A. El-Sappagh *et al.,* “Advancing modern healthcare with nanotechnology, nano biosensors, and internet of nano things: Taxonomies, applications, architecture, and challenges,” *IEEE Access*, vol. 8, pp. 65230–65266, 2020.

[23] O. Onireti, L. Zhang and M. A. Imran, “On the viable area of wireless practical byzantine fault tolerance (PBFT) blockchain networks,” in *Proc. 2019 IEEE Global Communications Conf. GLOBECOM*, Waikoloa, Hawaii, USA, IEEE, pp. 1–6, 2019.

[24] Z. Ying, L. Wei, Q. Li, X. Liu and J. Cui, “A lightweight policy preserving EHR sharing scheme in the cloud,” *IEEE Access*, vol. 6, pp. 53698–53708, 2018.

[25] V. Ramani, T. Kumar, A. Bracken, M. Liyanage and M. Ylianttila, “Secure and efficient data accessibility in blockchain based healthcare systems,” in *Proc. IEEE Global Communications Conf. GLOBECOM*, Abu Dhabi, UAE, pp. 206–212, 2018.

[26] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du *et al.,* “MeDShare: Trust-less medical data sharing among cloud service providers via blockchain,” *IEEE Access*, vol. 5, pp. 14757–14767, 2017.

[27] X. Liang, J. Zhao, S. Shetty, J. Liu and D. Li, “Integrating blockchain for data sharing and collaboration in mobile healthcare applications,” in *Proc. 2017 IEEE 28th Annual Int. Sym. on Personal, Indoor, and Mobile Radio Communications, PIMRC*, Montreal, QC, Canada, pp. 1–5, 2017.

[28] M. AbdelBasset, N. Moustafa, R. Mohamed, O. Elkomy and M. Abouhawwash, “Multi objective task scheduling approach for fog computing,” *IEEE Access*, vol. 9, no. 2, pp. 126988–127009, 2021.

[29] R. Swathy, B. Vinayagasundaram, G. Rajesh, A. Nayyar, M. Abouhawwash *et al.,* “Game theoretical approach for load balancing using SGMLB model in cloud environment,” *PLoS One*, vol. 15, no. 4, pp. e0231708, 2020.

[30] K. Venkatachalam, P. Prabu, A. Almutairi and M. Abouhawwash, “Secure biometric authentication with de-duplication on distributed cloud storage,” *PeerJ Computer Science*, vol. 7, no. 3, pp. e569, 2021.

[31] M. Abdel Basset, D. El-Shahat, K. Deb and M. Abouhawwash, “Energy-aware whale optimization algorithm for real-time task scheduling in multiprocessor systems,” *Applied Soft Computing*, vol. 93, no. 12, pp. 1–15, 2020.

[32] M. Abdel Basset, R. Mohamed, M. Abouhawwash, R. K. Chakrabortty and M. J. Ryan, “EA-MSCA: An effective energy-aware multi-objective modified sine-cosine algorithm for real-time task scheduling in multiprocessor systems: Methods and analysis,” *Expert Systems with Applications*, vol. 173, no. 3, pp. 1–15, 2021.

[33] M. Abouhawwash and A. Alessio, “Develop a multi-objective evolutionary algorithm for pet image reconstruction: Concept,” *IEEE Transactions on Medical Imaging*, vol. 40, no. 8, pp. 2142–2151, 2021.

[34] M. Abouhawwash, “Hybrid evolutionary multi-objective optimization algorithm for helping multi-criterion decision makers,” *International Journal of Management Science and Engineering Management, Taylor& Francis*, vol. 16, no. 2, pp. 94–106, 2021.

[35] S. Maheswaran, B. Vivek, P. Sivaranjani, S. Sathesh and K. Pon Vignesh, “Development of machine learning based grain classification and sorting with machine vision approach for eco-friendly environment,” *Journal of Green Engineering*, vol. 10, no. 3, pp. 526–543, 2020.

[36] M. Shanmugam and R. Asokan, “A machine-vision-based real-time sensor system to control weeds in agricultural fields,” *Sensor Letters*, vol. 13, no. 6, pp. 489–495, 2015.