Computer Systems Science & Engineering
DOI: 10.32604/csse.2023.024537
Article

Tech Science Press

Proof of Activity Protocol for IoMT Data Security

R. Rajadevi[1], K. Venkatachalam[2], Mehedi Masud[3], Mohammed A. AlZain[4] and Mohamed Abouhawwash[5,6,*]

[1]Department of Information Technology, Kongu Engineering College, Erode, 638060, Tamilnadu, India
[2]Department of Applied Cybernetics, Faculty of Science, University of Hradec Králové, Hradec Králové, 50003, Czech Republic
[3]Department of Computer Science, College of Computers and Information Technology, Taif University, Taif, 21944, Saudi Arabia
[4]Department of Information Technology, College of Computers and Information Technology, Taif University, Taif, 21944, Saudi Arabia
[5]Department of Mathematics, Faculty of Science, Mansoura University, Mansoura, 35516, Egypt
[6]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: 21 October 2021; Accepted: 05 January 2022

Abstract: The Internet of Medical Things (IoMT) is an online device that senses and transmits medical data from users to physicians within a time interval. In, recent years, IoMT has rapidly grown in the medical field to provide healthcare services without physical appearance. With the use of sensors, IoMT applications are used in healthcare management. In such applications, one of the most important factors is data security, given that its transmission over the network may cause obtrusion. For data security in IoMT systems, blockchain is used due to its numerous blocks for secure data storage. In this study, Blockchain-assisted secure data management framework (BSDMF) and Proof of Activity (PoA) protocol using malicious code detection algorithm is used in the proposed data security for the healthcare system. The main aim is to enhance the data security over the networks. The PoA protocol enhances high security of data from the literature review. By replacing the malicious node from the block, the PoA can provide high security for medical data in the blockchain. Comparison with existing systems shows that the proposed simulation with BSD-Malicious code detection algorithm achieves higher accuracy ratio, precision ratio, security, and efficiency and less response time for Blockchain-enabled healthcare systems.

Keywords: Blockchain; IoMT; malicious code detection; security; secure data management framework; data management; PoA

1 Introduction

Healthcare systems offer various services such as exhaustive clinics, emergency centers, reclamation centers, and outpatient care [1]. Medical services are intended for public welfare, and the healthcare system provides extra care to keep patients safe. Health organizations develop a data management system that helps monitor information and keep patient records with increased confidentiality.

In recent years, Internet of Medical Things (IoMT) has become widely used in the medical area. With the help of IoMT, medical data are collected by using various sensor application services. IoMT has many wearable sensors, health monitors that collect and transfer patient data in a secure manner [2]. IoMT has sensor devices such as heartbeat sensors and optimizers. These sensors collect and store patient data in blockchain-enabled systems. IoMT also reduces the treatment costs.

The IoMT systems are used to reduce the travel time and burden of patients and doctors. However, ensuring security for patient data is difficult. Everyone is using technological devices. Cost-effective and secured data transmission characteristics are extremely important requirements for IoMT development. For security purposes, data are encrypted in the IOMT application due to security reasons before transmission to the server. At the same time, clients face several problems [3]. The main cause for these is that the service provider has to perform data computation to respond to client request. Thus, the client must provide the server with the key to decrypt the data before performing the appropriate calculation, affect the cloud data confidentiality.

Patient health records contain assortment of sensitive data that require security potentials. Several intruders may modify data, hijack devices that cause threats to patient life with irrelevant decision of physician. On the other hand, network intruders are probably obtaining access to hospital network that causes threats to IoMT. Despite several cryptographic mechanisms, blockchain has the ability to conquer the hindrance of traditional security issues and privacy.

Blockchain systems consists of several blocks that store the data, each block is connected with the help of nodes, thereby providing data security. Blockchain has secured data structure that connects with blocks. IoMT uses blockchain technology that provides security among the data. This cryptographic technique pays secured way for data transactions and storage. The blockchain technology discards a centralized operating structure for data security and governance. Every transaction in blockchain is cryptographically verified by all nodes in chained blocks. Thus, the IoMT with blockchain-ensured data is highly secured in the network [4].

Consensus algorithms are used to achieve network reliability, and provide fault-tolerant results while performing in the applications. Such algorithm works along with various advanced fields. Security mechanism consensus protocols are used in blockchain-enabled technology. Commonly used protocols are Proof of Work (PoW), Proof of Stake (PoS), Proof of Capacity, and Proof of Elapsed Time (PoET).

In this study, we use the Proof of Activity (PoA) algorithm, which is a hybrid of PoS and PoW protocols. PoA is used for detecting malicious threats found in the data during transactions. In addition, this study uses a downgrade mechanism along with the PoA Protocol to provide data security.

The blockchain-assisted secure data management framework (BSDMF) is mainly used for secured data management. In this study, the roles of BSD–PoA malicious code detection algorithms are as follows.

The BSD-PoA malicious code detection algorithm improves the accessibility of data in the medical field and helps to evaluate the data trustworthiness which is based on blockchain-enabled cloud computing network.

This approach is used for ensuring data security by using nodes.

The malicious code detection mechanism is used for detecting the irrelevant information from the system, and thus protects the data from hackers or intrusion.

In this system, the results enhance the precision value, accuracy level, and trust values.

The rest of the paper is organized as follows. Section 2 consists of a brief study of existing IoMT system and block chain. Section 3 describes the working principal of the proposed model. Section 4 evaluates the result and provides a comparison of the different algorithms. Section 5 concludes the research and states possible future scopes.

2 Related Work

The healthcare system provides various services, such as clinics, emergency centers, renovation centers, and outpatient care. In medical services, curing a disease is the most important factor and treatment is a primary concern. The welfare of society plays a major role in healthcare management.

The system provides different resources to ensure the safety of patients' environment. High-quality medical care is more critical for disease prevention, integrity of all patients, and preserving wellness. Thus, health data management involves developing a system to monitor the access to information over the institutions [5]. Medical records collect secured patient data, testing and tracking these by using blockchain-enabled IoMT devices. The main factor behind such devices is portability; therefore, anyone can use the devices anytime and anywhere [6–8]. IoMT is used for medical devices and as a wireless connectivity to people, thereby allowing access to healthcare data [9]. Such data helps in the diagnosis of diseases via the Internet, especially during the current pandemic that affects patients worldwide.

In healthcare systems, IoMT is used for tracking patient data and to connect with the cloud servers. In the quantitative evaluation, cloud server management measures and stores resources [10–12]. IoMT-enabled blockchain provides the security, transfer, and protection of data through the integration. exchange, and transfer from various healthcare devices [13]. Given the accessibility or usage of data, legal or compliance issues occur and inadequate data protection standards are observed [14].

Blockchain is used as a secure management for data acquisition and cloud connectivity. In the IoMT and Blockchain database, patient data are collected from sensors and stored in blocks. For blockchain safety and security, the system uses smart contracts [15–18]. Blockchain also uses a network of computers, with a framework composed of six layers, namely, data, networking, consensus, incentives, contract, and application [19]. The existing blockchain model combines all transactions with individual time stamping and cryptographic algorithms [20]. However, blockchain quality relies on strong consensus protocol that serves as security in block creation and validation.

The consensus algorithm is a collaborative decision among blockchain nodes for the creation of new ones. The nodes provide permission or compromise to approve trusted entities [21]. Blockchain members negotiate to check if a transaction is valid and synchronized with known accounts. After confirmation by a certain number of nodes, the blockchain allows the data update.

Proof of Work (PoW) mainly uses a filtering spam. The first bitcoin application achieved efficiency in generating blocks using PoW and writing blocks in blockchain. Proof of Stake (PoS) was first implemented by sunny for his peer coin and the number of stakes is used to adjust difficulties in mining. A high number of stakes leads to easier block generation. Later, Larimer developed a delegated PoS (DPos) for the bitcoin project. This DPoS performs a witness election and block generation with the specified time stamp. The main problems in this system are inefficiency and decentralization. In addition, blockchains have higher probability of being a witness and voting for known intruders, leasing to high chance for vulnerability and collision attacks. As a solution, Castro (1999) introduced the Byzantine fault tolerance (PBFT), which works through the principal concept of machine replication.

Tab. 1 shows the various consensus protocols and their advantages and disadvantages.

Table 1: Various consensus protocol

Various consensus protocol	Pros	Cons
PoA [22]	Efficiency is improved by fairness	Less security on the data
PoB [23]	Efficiency is high	Practically less possible
PoSV [24]	Financial workflow is processed using decentralized rights	More centralized process
PoUW [25]	Good practical approach	Less security

3 IoMT Security Enabled Blockchain Using BSD-PoA Malicious Code Detection Algorithm

3.1 Overview

Given technological progress, many improvements have been developed for the data management of healthcare system, especially computer-based methods for users. The Blockchain-enabled IoMT provides increased security to the data transfer. Maintenance of health data on the daily basis may provide certain features such as new data creation, update records, and provide better security [26–40]. By using electronic healthcare records (EHRs), the system enhances the services for both the public and patients. EHR helps to monitor medical records; and therefore, the organization can easily collect data and diagnose the disease. Blockchain-enabled IoMT systems are well-structured and therefore the data can be stored and shared securely, and be updated in the blockchain with from any Hub. EHRs can also be accessed by the user, thereby providing accessibility. Existing systems use two algorithms, BSDMF and PoA, to detect malicious code using a downgrade mechanism that provides security among the data records. This algorithm provides efficient data communication in blockchain network with high security and large storage. Further improvement is achieved for both computing resources and generated stakes using downgrade technology. The technique for malicious code detection works perfectly through early identification of node attacks and increased security of blockchain and IoMT model. By comparison, the proposed model of BSD-PoA using malicious code detection provides the following:

IoMT-enabled blockchain provides more secured data management for easy data accessibility in healthcare systems.

The security, accuracy value, precision value, trust value, and ratio of response time are increased.

Verification nodes ensure that the interruption node is found and facilitates easy replacement.

This study improves the data security in healthcare systems such that the user can use the IoMT healthcare systems with greater trust.

3.2 Architecture Model

The architecture model shows how the proposed system works with the algorithms. Fig. 1 shows the proposed system workflow.

For data security, a network encryption technology is applied in the system. For medical institutions, data are encrypted as an important security step, and afterwards, are decrypted by the medical authorities.

3.2.1 IoMT Devices

IoMT is an amalgamation of software applications and medical equipment. Sensors are used to collect the user data over the network. Various wearable devices can be used for tracking the healthcare data. For example, smart watch, wearable fitness trackers, wearable monitors, wearable blood pressure monitors, and many biosensors are used in IoMT technology.

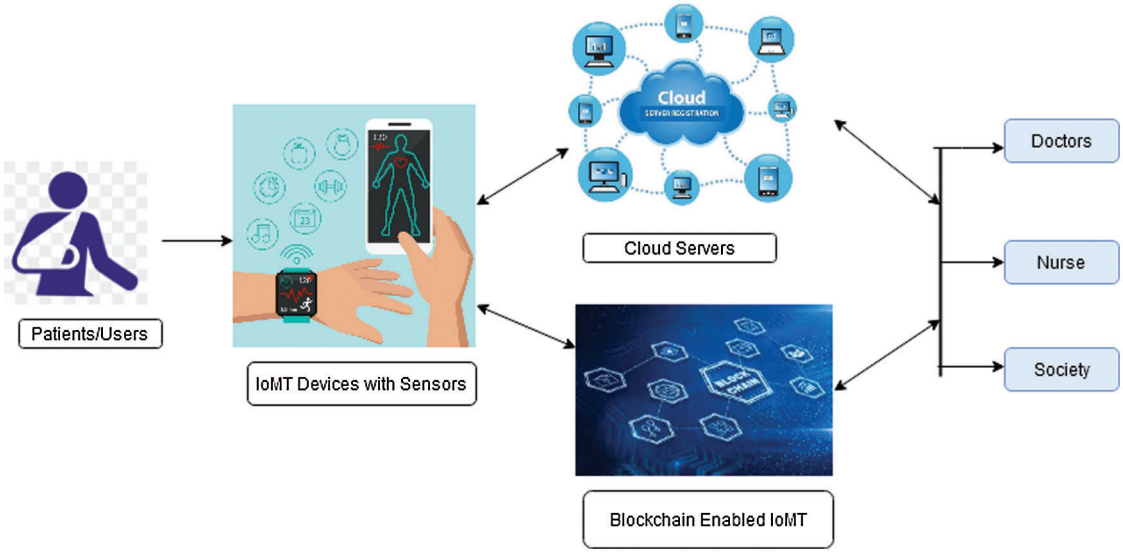

Figure 1: Proposed architecture model

3.2.2 Blockchain-Enabled IoMT System

A blockchain is a decentralized method in IoMT, which handles various issues and provides a sophisticated environment for patients and users. The blockchain consists of several blocks, each connected similar to linked chain. Each block carries another block's node, and thus facilitates data security. Encrypting data is one way to restrict intrusions. IoMT systems are widely used in the medical management. In the context of the pandemic, visiting hospitals for checkups is a challenge. Thus, IoMT plays a huge role in reducing travel, costs, and other affected factors. The patient can use healthcare applications to record their problems, and with the help of Blockchain and cloud servers, the treatments are given to the patient. In this case, the patient has to be aware of healthcare systems, pharmacists, and professionals to contact and directly share their concerns.

Fig. 2 shows the workflow of blockchain in the healthcare systems. Data is managed with the help of cryptography, which provides more facilities to the user for easier access to the IoMT-enabled systems.

3.2.3 Proposed BSD-PoA Malicious Code Detection Algorithm

Data accuracy in medical devices allows doctors in practices to know a patient's history, dynamics, previous complications, current conditions, and likely responses. In turn, patients can be treated as quickly as possible. Academics, medical practitioners, insurance undertakings, and stock dealers use homogeneous IoMT probability for making decisions in cases of uncertainty. Probability theory is used in the epidemiology for health risks. The proposed system uses the probability mechanism to reduce the risks to the data.

3.2.4 Node Selection

A blockchain node is selected based on the tasks allocated in its function. Each node has a task to perform. In the consensus algorithm, the three types of nodes are trading, consensus, and malicious.

3.2.5 Trading Nodes

This type of node helps to perform the data transaction method.

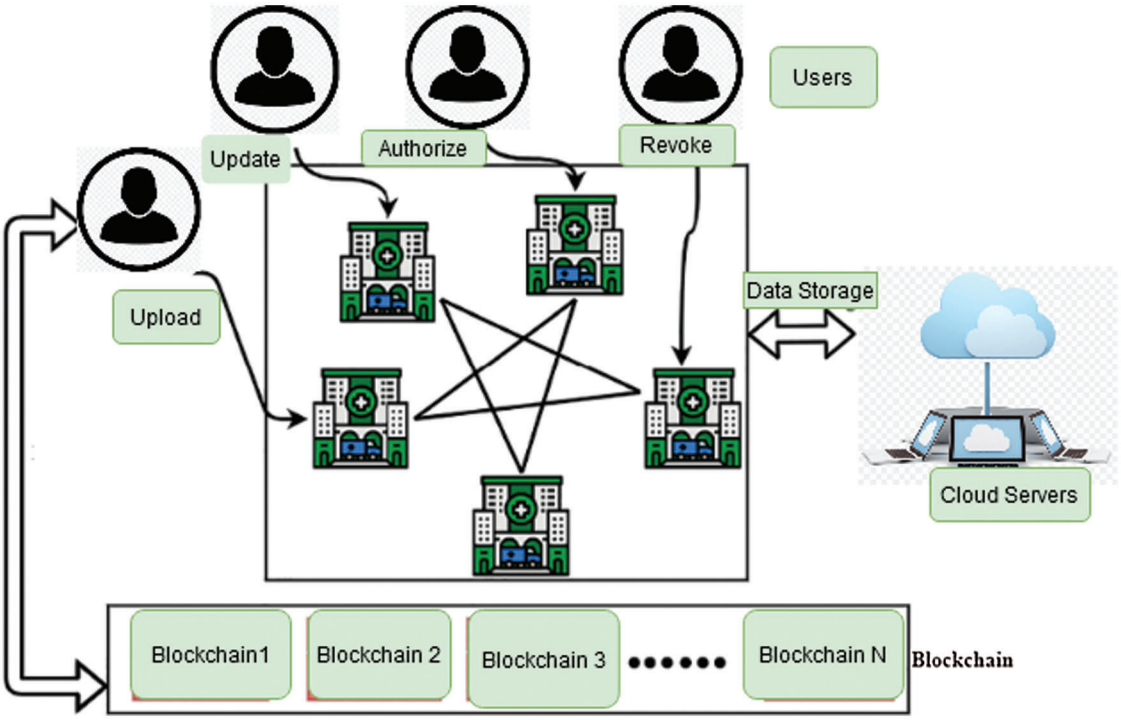

Figure 2: Blockchain-enabled IoMT in the healthcare systems

3.2.6 Consensus Node

This node is used to perform the verification and validation of the task. In addition, consensus nodes can help detect malicious ones.

3.2.7 Malicious Code Detection

A malicious code detection algorithm is planned to automate a static analysis that can distinguish and classify the character of, but not run, the file itself. The system receives all the files as input data, including the malicious code, traditional file, and supply file. In blockchain-enabled IoMT systems, the main issue is data security, and malicious code detection algorithm is used as a solution. The algorithm detects unwanted nodes in the blocks and removes them during transaction. Therefore, the data is more secured. Fig. 3 shows the workflow of malicious code detection.

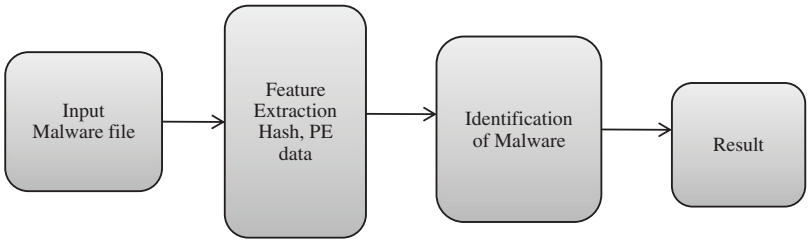

Figure 3: Workflow of malicious code detection

3.2.8 Pre-processing Step

In this step, the input file is processed by first entering the data into the model. Then, the hash values and PE data are extracted.

3.2.9 Hash Extraction

From the input file, the hash value is extracted to determine if the given data is a duplicate or not. The extracted hash value is taken as a primary key, and then the result is added to the database where the duplicate data is modified.

Pseudo code: BSD-PoA malicious code detection

Input: data collected from IoMT devices

Output: Transferring secure data without any loss

Step 1: Receives the data from IoMT device

Step 2: Stores the data in Blockchain

Step 3: Transfers the data through blockchain

Step 4: Malicious code detection

#Result Analysis#

good = con(result[good])

bad = con(result[bad])

Step 5: Final result

If good > bad

Return good

Else

Return bad

Step 6: Secures data transactions

Step 7: Reaches the destination

The above steps show the each and every step of the proposed system.

3.2.10 Basic Transaction Workflow

The basic transaction workflow of sharing healthcare data and accessing the data are shown below. IoMT sensors are used in two categories of aggregation requests. Wearable devices automatically detect the health issues in the body within a daily time period. Fig. 4 shows the basic transaction workflow of medical data.

4 Result Evaluation

The simulation results show the overall performance of the proposed system BSD-PoA malicious code detection algorithm. In this proposed system, several evaluation metrics are analyzed. Accuracy of the task, response time, and trust value of the tasks are verified using the algorithm. By using the consensus algorithm with BSDMF, three parameters are determined, namely, fault tolerance, efficiency, and probability. The proposed model collects the wearable and IoMT applications healthcare data. Tab. 2 shows the simulation parameters of the healthcare management using the proposed system.

The simulation parameters and the metrics used in the proposed systems are also discussed.

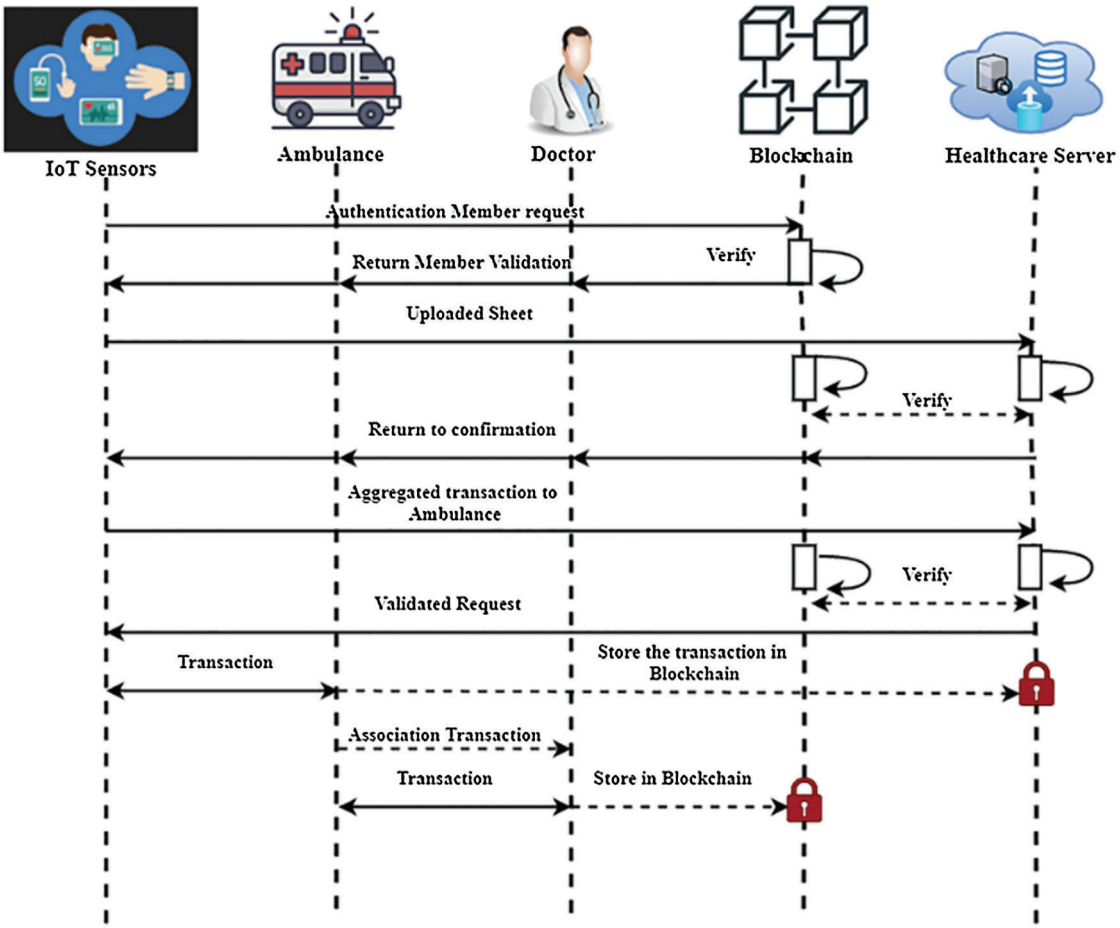

Figure 4: Basic transaction workflow of medical data

Table 2: Simulation parameters

Parameter	Value
No. of cloud service providers	30
No. of patients	150
Transactions of the data	1000 per round
Area of the simulation	500 m × 500 m
No. of IoMT devices	107050550
Response time	2–3 s
Simulation time	100 s

4.1 Accuracy Ratio

IoMT healthcare systems use blockchain techniques to manage data sharing. In the proposed system, the BSD-PoA malicious code detection algorithm helps to predict the threats in many medical devices. The blockchain-based healthcare systems improve the data quality and continuity as well as the service delivery. IoMT-based devices allow for general treatment with great accuracy and increase the outcomes of patient care.

Fig. 5 shows the proposed overall accuracy ratio. Compared with the existing algorithms, BSD-PoA malicious code detection algorithm provides high accuracy ratio.

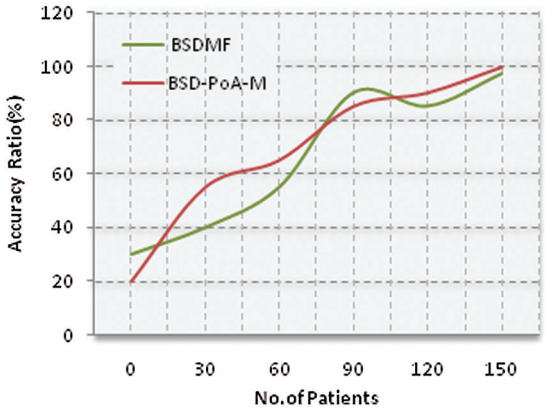

Figure 5: Proposed accuracy ratio

4.2 Response Latency Ratio

For a secure data exchange, the blockchain framework is used between the cloud servers and personal servers. The proposed system minimizes the latency ratio in the processing units, thereby increasing security and privacy between the servers.

Fig. 6 shows that the response latency ratio is lower than that of existing systems. The number of patients with high latency time also decreases.

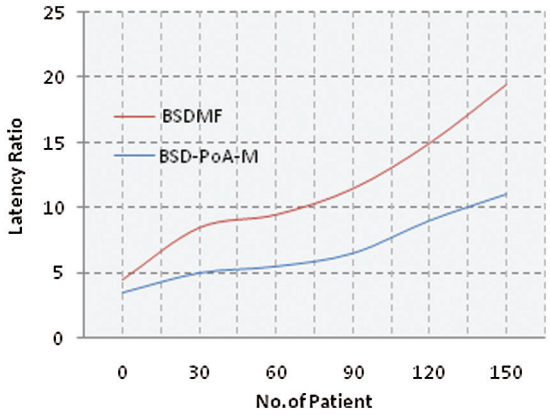

Figure 6: Response latency ratio

4.3 Ratio of Response Time

As stated earlier, the major issue in the IoMT healthcare management is data security. This problem includes the response time, storage, efficiency, and verification of the data.

Fig. 7 shows that the response time of the proposed process is less than that of the existing system.

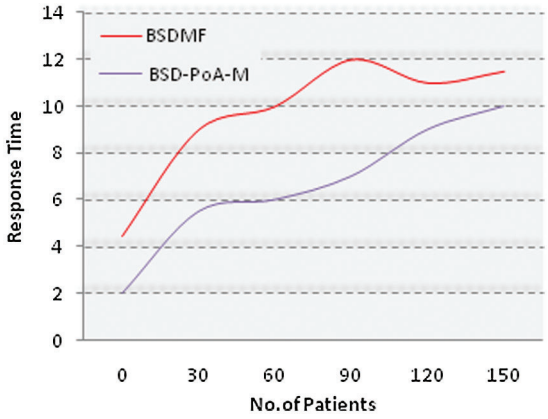

Figure 7: Proposed response time (s)

4.4 Efficiency

In blockchain systems, each block is calculated using time (blockchain seconds). With the help of B_S we can calculate the efficiency

Bs = Overall time taken/overall blocks

The probability of block generation is calculated by using

$$pb_{\Delta t} = (No.\ of\ goodnodes)_{\Delta t} \Big/ (Total\ no.\ of\ nodes)_{\Delta t}.$$

where the *no. of good nodes* denotes the good nodes generated in the blocks and *Total no. of nodes* denotes the total nodes in the blockchain.

4.5 Fault Tolerance

Fault tolerance is used for detecting the interruption nodes in the blockchain-enabled IoMT system.

5 Conclusion

IoMT enabled Blockchain is widely used in the healthcare management system to maintain patient data with high security. The data are collected from wearable devices and healthcare application systems by using sensors, and are then stored in cloud servers. In general, Blockchain provides the security to healthcare management. However, existing systems have no well-defined data security. Comparison of BSDMF and PoA using malicious code detection algorithm provides a high security over data transactions. The results show that the proposed system achieves high accuracy ratio, low response time, latency ratio, fault tolerance, and high efficiency. Malicious threats over the data are easily detected and immediately removed from the transaction. In addition, the algorithm increases the efficiency of the nodes with the help of the probability method.

In the future, IoMT enabled blockchain methods may use various protocols for data security. In addition, healthcare applications can be tested through actual method implementation.

Acknowledgement: We would like to give special thanks to Taif University Research supporting project number (TURSP-2020/98), Taif University, Taif, Saudi Arabia.

Funding Statement: Taif University Researchers Supporting Project Number (TURSP-2020/98), Taif University, Taif, Saudi Arabia.

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

References

[1] F. Al-Turjman, H. Zahmatkesh and L. Mostarda, "Quantifying uncertainty in internet of medical things and big-data services using intelligence and deep learning," *IEEE Access*, vol. 7, no. 3, pp. 115749–115759, 2019.

[2] G. C. Manikis, M. Spanakis and E. G. Spanakis, "Personalized mobile ehealth services for secure user access through a multi feature biometric framework," *International Journal of Reliable and Quality E-Healthcare (IJRQEH)*, vol. 8, no. 1, pp. 40–51, 2019.

[3] A. Abbas, R. Alroobaea, M. Krichen, S. Rubaiee, S. Vimal *et al.,* "Blockchain-assisted secured data management framework for health information analysis based on internet of medical things," *Personal and Ubiquitous Computing*, vol. 4, no. 5, pp. 1–14, 2021.

[4] P. Wei, D. Wang, Y. Zhao, S. K. S. Tyagi and N. Kumar, "Blockchain data-based cloud data integrity protection mechanism," *Future Generation Computer Systems*, vol. 102, no. 6, pp. 902–911, 2020.

[5] I. Makhdoom, I. Zhou, M. Abolhasan, J. Lipman and W. Ni, "PrivySharing: A blockchain based framework for privacy-preserving and secure data sharing in smart cities," *Computers & Security*, vol. 88, no. 3, pp. 101653, 2020.

[6] A. Darwish, A. E. Hassanien, M. Elhoseny, A. K. Sangaiah and K. Muhammad, "The impact of the hybrid platform of internet of things and cloud computing on healthcare systems: Opportunities, challenges, and open problems," *Journal of Ambient Intelligence and Humanized Computing*, vol. 10, no. 10, pp. 4151–4166, 2019.

[7] G. Manogaran, B. S. Rawal, V. Saravanan, P. M. Kumar, O. S. Martínez *et al.,* "Blockchain based integrated security measure for reliable service delegation in 6G communication environment," *Computer Communications*, vol. 161, no. 6, pp. 248–256, 2020.

[8] P. M. Kumar and U. D. Gandhi, "Enhanced DTLS with CoAP-based authentication scheme for the internet of things in health care application," *The Journal of Supercomputing*, vol. 76, no. 6, pp. 3963–3983, 2020.

[9] G. Aceto, V. Persico and A. Pescapé, "Industry 4.0 and health: Internet of things, big data, and cloud computing for healthcare 4.0," *Journal of Industrial Information Integration*, vol. 18, no. 9, pp. 100129, 2020.

[10] B. Muthu, C. Sivaparthipan, G. Manogaran, R. Sundarasekar, S. Kadry *et al.,* "IOT based wearable sensor for diseases prediction and symptom analysis in healthcare sector," *Peer-to-Peer Networking and Applications*, vol. 13, no. 6, pp. 2123–2134, 2020.

[11] H. Kurdi, S. Alsalamah, A. Alatawi, S. Alfaraj, L. Altoaimy *et al.,* "Healthybroker: A trustworthy blockchain-based multi-cloud broker for patient-centered ehealth services," *Electronics*, vol. 8, no. 6, pp. 602, 2019.

[12] D. Połap, G. Srivastava, A. Jolfaei and R. M. Parizi, "Blockchain technology and neural networks for the internet of medical things," in *Proc. INFOCOM WKSHPS*, Toronto, ON, Canada, IEEE, pp. 508–513, 2020.

[13] A. Bhardwaj, S. B. H. Shah, A. Shankar, M. Alazab, M. Kumar *et al.,* "Penetration testing framework for smart contract blockchain," *Peer-to-Peer Networking and Applications*, vol. 14, no. 5, pp. 2635–2650, 2021.

[14] S. Tanwar, K. Parekh and R. Evans, "Blockchain-based electronic healthcare record system for healthcare 4.0 applications," *Journal of Information Security and Applications*, vol. 50, no. 12, pp. 102407, 2020.

[15] G. Manogaran, N. Chilamkurti and C. H. Hsu, "Emerging trends, issues, and challenges in internet of medical things and wireless networks," *Personal and Ubiquitous Computing*, vol. 22, no. 5, pp. 879–882, 2018.

[16] A. K. Luhach, S. V. Kumar and R. C. Poonia, "Speed of things (SoT): Evolution of isolation-to-intermingle (I2I) technology transition towards IoT," *Recent Patents on Computer Science*, vol. 12, no. 4, pp. 354–360, 2019.

[17] M. Shanmugam, S. Nehru and S. Shanmugam, "A wearable embedded device for chronic low back patients to track lumbar spine position," *Biomedical Research (0970–938X)*, vol. 13, no. 2, pp. 1–12, 2018.

[18] R. Belfer, A. Kashtalian, A. Nicheporuk, G. Markowsky and A. Sachenko, "Proof-of-activity consensus protocol based on a network's active nodes," in *Proc. Central Europe (CEUR)*, Yalta, Crimea, 2020.

[19] K. Salah, M. H. U. Rehman, N. Nizamuddin and A. Al-Fuqaha, "Blockchain for AI: Review and open research challenges," *IEEE Access*, vol. 7, no. 5, pp. 10127–10149, 2019.

[20] H. R. Hasan and K. Salah, "Combating deepfake videos using blockchain and smart contracts," *IEEE Access*, vol. 7, no. 7, pp. 41596–41606, 2019.

[21] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Future Generation Computer Systems*, vol. 82, no. 3, pp. 395–411, 2018.

[22] R. Almadhoun, M. Kadadha, M. Alhemeiri, M. Alshehhi and K. Salah, "A user authentication scheme of IoT devices using blockchain-enabled fog nodes," in *Proc. IEEE/ACS 15th Int. Conf. on Computer Systems and Applications (AICCSA)*, Aqaba, Jordan, pp. 1–8, 2018.

[23] A. Suliman, Z. Husain, M. Abououf, M. Alblooshi and K. Salah, "Monetization of IoT data using smart contracts," *Institution of Engineering and Technology (IET) Networks*, vol. 8, no. 1, pp. 32–37, 2019.

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

[25] A. Barhanpure, P. Belandor and B. Das, "Proof of stack consensus for blockchain networks," in *Proc. Int. Symp. on Security in Computing and Communication*, Bangalore, India, Springer, pp. 104–116, 2018.

[26] M. Abdel-Basset, N. Moustafa, R. Mohamed, O. Elkomy and M. Abouhawwash, "Multi-objective task scheduling approach for fog computing," *IEEE Access*, vol. 9, no. 3, pp. 126988–127009, 2021.

[27] 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.

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

[29] 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. 4, pp. 114699, 2021.

[30] M. Masud, G. Gaba, K. Choudhary, M. Hossain, M. Alhamid *et al.,* "Lightweight and anonymity-preserving user authentication scheme for IoT-based healthcare," *IEEE Internet of Things Journal*, vol. 24, no. 2, pp. 1–12, 2021.

[31] A. Ali, H. A. Rahim, J. Ali, M. F. Pasha, M. Masud *et al.,* "A novel secure blockchain framework for accessing electronic health records using multiple certificate authority," *Applied Sciences*, vol. 11, no. 21, pp. 1–14, 2021.

[32] M. Masud, G. S. Gaba, K. Choudhary, R. Alroobaea and M. S. Hossain, "A robust and lightweight secure access scheme for cloud based E-healthcare services," *Peer-to-Peer Networking and Applications*, vol. 14, no. 3, pp. 3043–3057, 2021.

[33] M. Masud, G. Gaba, S. Alqahtani, G. Muhammad, B. Gupta *et al.,* "A lightweight and robust secure key establishment protocol for internet of medical things in COVID-19 patients care," *IEEE Internet of Things Journal*, vol. 8, no. 21, pp. 15694–15703, 2021.

[34] S. Ibrahim, H. Alhumyani, M. Masud, S. S. Alshamrani, O. Cheikhrouhou *et al.,* "Framework for efficient medical image encryption using dynamic S-boxes and chaotic maps," *IEEE Access*, vol. 8, no. 13, pp. 160433–160449, 2020.

[35] M. Rawashdeh, M. Zamil, S. M. Samarah, M. Obaidat and M. Masud, "IOT-based service migration for connected communities," *Computers & Electrical Engineering*, vol. 96, no. 3, pp. 1–10, 2021.

[36] Y. Wang, J. Ma, A. Sharma, P. K. Singh, G. Singh *et al.,* "An exhaustive research on the application of intrusion detection technology in computer network security in sensor networks," *Journal of Sensors*, vol. 2021, no. 3, pp. 1–11, 2021.

[37] M. Masud, M. Alazab, K. Choudhary and G. S. Gaba, "3P-SAKE: Privacy-preserving and physically secured authenticated key establishment protocol for wireless industrial networks," *Computer Communications*, vol. 175, no. 4, pp. 82–90, 2021.

[38] P. Singh, M. Masud, M. S. Hossain and A. Kaur, "Cross-domain secure data sharing using blockchain for industrial IoT," *Journal of Parallel and Distributed Computing*, vol. 156, no. 3, pp. 176–184, 2021.

[39] S. M. M. Rahman, M. Masud, M. A. Hossain, A. Alelaiwi, M. M. Hassan *et al.,* "Privacy preserving secure data exchange in mobile P2P cloud healthcare environment," *Peer-to-Peer Networking and Applications*, vol. 9, no. 5, pp. 894–909, 2016.

[40] M. Masud and M. S. Hossain, "Secure data-exchange protocol in a cloud-based collaborative health care environment," *Multimedia Tools and Applications*, vol. 77, no. 9, pp. 11121–11135, 2018.