Computers, Materials & Continua
DOI:10.32604/cmc.2022.022336
Article

Tech Science Press

Integration of Fog Computing for Health Record Management Using Blockchain Technology

Mesfer AI Duhayyim[1], Fahd N. Al-Wesabi[2], Radwa Marzouk[3], Abdalla Ibrahim Abdalla Musa[4], Noha Negm[5], Anwer Mustafa Hilal[6], Manar Ahmed Hamza[6,*] and Mohammed Rizwanullah[6]

[1]Department of Natural and Applied Sciences, College of Community Aflaj, Prince Sattam Bin Abdulaziz University, Saudi Arabia
[2]Department of Computer Science, College of Science & Art at Mahayil, King Khalid University, Saudi Arabia & Faculty of Computer and IT, Sana'a University, Yemen
[3]Department of Information Systems, College of Computer and Information Sciences, Princess Nourah Bint Abdulrahman University, Saudi Arabia & Department of Mathematics, Faculty of Science, Cairo University, Giza, 12613, Egypt
[4]Department of Computer Science, College of Computer, Qassim University, Buraydah, Saudi Arabia
[5]Department of Computer Science, King Khaled University, KSA & Faculty of Science, Department of Mathematics and Computer Science, Menoufia University, Egypt
[6]Department of Computer and Self Development, Preparatory Year Deanship, Prince Sattam Bin Abdulaziz University, AlKharj, Saudi Arabia
*Corresponding Author: Manar Ahmed Hamza. Email: ma.hamza@psau.edu.sa
Received: 04 August 2021; Accepted: 11 October 2021

Abstract: Internet of Medical Things (IoMT) is a breakthrough technology in the transfer of medical data via a communication system. Wearable sensor devices collect patient data and transfer them through mobile internet, that is, the IoMT. Recently, the shift in paradigm from manual data storage to electronic health recording on fog, edge, and cloud computing has been noted. These advanced computing technologies have facilitated medical services with minimum cost and available conditions. However, the IoMT raises a high concern on network security and patient data privacy in the health care system. The main issue is the transmission of health data with high security in the fog computing model. In today's market, the best solution is blockchain technology. This technology provides high-end security and authentication in storing and transferring data. In this research, a blockchain-based fog computing model is proposed for the IoMT. The proposed technique embeds a block chain with the yet another consensus (YAC) protocol building security infrastructure into fog computing for storing and transferring IoMT data in the network. YAC is a consensus protocol that authenticates the input data in the block chain. In this scenario, the patients and their family members are allowed to access the data. The empirical outcome of the proposed technique indicates high reliability and security against dangerous threats. The major advantages of using the blockchain model are high transparency, good traceability, and high processing speed. The technique also exhibits high reliability and efficiency in accessing data with secure transmission. The proposed technique achieves 95% reliability in transferring a large number of files up to 10,000.

Keywords: Fog computing; IoMT; block chain; YAC; security; IoT; consensus protocol

1 Introduction

Internet of Things (IoT) is collection of sensors and smart devices that connect to the internet for smart applications. Each device has its own IP address for communicating in the network. These devices connect to the internet via an application programming interface. At present, many applications, such as healthcare, smart home, vehicle, and educational applications, are embedded in the IoT. Among these, healthcare provides a wide usage of the IoT in connecting patients online immediately. This application is termed as the Internet of Medical Things (IoMT) through which the health data of users are collected via sensors and stored in smart devices (the IoT). The IoMT transfers, stores, and processes patient data for accurate diagnosis. Secure data transmission is the main expectation of all users of the IoMT. Fog computing is a framework that uses edge devices for computing certain tasks in terms of storage, process, and communication. IoMT data are collected from devices and stored in the cloud. The cloud contains data processing algorithms and applies them on data and then sends the result to the users. The storage of data in a nearby location can improve the efficiency of computation algorithms. Furthermore, the result can be fetched quickly. The state of the art proves that the block chain provides high security for all types of applications. A block chain is a collection of blocks that carry data in a linked list model. Every block has a block header, data, and information on the previous block. Hashing creates the reference key for the previous and next headers. Therefore, it ensures high security in the wide variety of applications because of its strong decentralized approach.

Fog computing is widely used in the IoT for fast data computation. Recently, it has been used in the medical field for processing health care data [1]. Wireless sensor networks in the IoMT [2] are used to obtain data quickly and compute anonymously. Blockchain technology is implemented in a distributed network [3–6] for high security and data authentication. Fog computing is utilized to improve the security and efficiency of transmitting data to the cloud. Then, the transmitted data are analyzed and stored safely. Fog computing is used in the development of the health field, acting as a middle layer between the IoMT and the cloud to improve the data security and confidentiality. In cryptographic implementation, fog computing has deployed a unique way of gathering medical data from various sources. Fog computing is based on the service-oriented architecture, evaluating health care data and validating them for further processing in the health field [7–10].

For high authentication, embedding the IoMT with fog computing (i.e., FOG-IoMT) is proposed for the early diagnosis of diseases. FOG-IoMT uses block chain technology to carry and process data in the fog environment with high authentication. The block chain is composed of various consensus algorithms. Some of these algorithms include proof of work, proof of stake, proof of activity, Byzantine fault tolerance, and the Yet Another Consensus (YAC) protocol. The Byzantine fault tolerance algorithm exhibits delays in providing strong leaders and bad message passing rules. The YAC protocol overcomes the drawback of the Byzantine fault tolerance algorithm. In this research, a YAC-based blockchain is preferred for efficient data computation. The following are the contributions of this research.

1. Health care record management is implemented through the fog computing of the IoMT to increase the reliability, accuracy, authenticity, and integrity of data management in blockchain technology.
2. Real-time medical data are processed using the fog-based architecture of the IoMT-YAC algorithm, which accesses the data of patients effectively depending on their health conditions.
3. Various challenges in fog-computing-based IoMT with blockchain technology in health care record management were explored.

The rest of this paper is arranged in five sections. Section 2 discusses recent articles. Section 3 describes the methodology of the proposed work and the algorithm used. Section 4 evaluates the outcome of the study, and Section 5 concludes this paper with the future research scope.

2 Related Work

Recently, fog and edge computing have been applied in the examination of medical data in the field of healthcare record management [11]. The IoMT is the network through which people and medical devices exchange the healthcare data via wireless communication as proposed in an article [12]. In exchanging sensitive medical information through network connection, security and privacy are the main factors that must be considered. Thus, the protection of data from anonymous users to maintain data integrity and quality was proposed. Consequently, data collection follows protocols and is implemented in pervasive social network nodes. Data is managed in the blockchain using smart contracts, which is referred to as MedShare in an article. The blockchain structure adopts distributed ledger technology in which data are distributed and managed by various users. A study proposed the consensus between users to add more blocks into the blockchain. Physicians provide medical care for patients in remote areas through the IoMT and deliver solutions to them in critical situations [13]. Fog computing with an open stack platform has been used to improve latency and scalability. In general, the fog computing architecture is a service-oriented structure for telehealth application processing in real time, collecting raw data from wearable sensors and smart devices. To optimize these services, a three-tier architecture was proposed [14,15].

Deployment of fog computing in the IoMT explains in monitoring the health of the patient at a lower cost. It also improves the security and privacy by block chain which was suggested in the paper [16]. Moreover, the Fog-based architecture in the health care management acts as an intermediate layer between cloud and IoMT devices for the enhancement of cryptographic technique. IoMT devices had evaluated and validated the healthcare management via the service-oriented based fog computing which was proposed in the paper [17]. Typically, the medical data management in the fog layer is considered as a challenging task. In addition to that, it is observed that the fog layer has a limited storage space when compared to that of the cloud. Thus, the storage capacity is also considered as another challenge which is listed in the paper. Consensus algorithm provides guarantee in terms of storing the data in the ledger in a secured manner, liveness of the model and maintains consistency. In the model of liveness, errors are recovered from the data wherein the security means accepting only the request of an authorized user and consistency refers to maintain the same ordering and state of data in a globalized manner. In the fully asynchronous network, deterministic solution was given by non-distributed consensus algorithm which was proposed in the paper [18,19].

The decentralized computational problem is difficult to solve the adaptable concept of decentralized consensus algorithm. Similarly, in the decentralized system, sybil attacks are prevented by Proofs-of-Work. Proof-of-Stake and Proof-of-Importance were generated through random numbers for the generation of block hashes and public keys [20–22]. For monitoring the health of patients

while ensuring privacy, the preserved structure of the blockchain-based IoMT has a patient-centric agent in the form of tailored type of blockchain. This patient-centric agent sorts all stored data in the medical record in term of criticalness, as suggested in a study [23]. Data are collected through sensor nodes, and access control is provided, and the medical data are managed using big data application in terms of security, privacy, and integrity, as proposed in previous studies [24–26]. In the article [27], the current status of a patient is described using Petri Nets to enhance the dynamism of real-time applications. In the IoMT, the communication between devices and the interface used in the device may be experience cyberattacks. Further, it may increase the attacks on e-health records. In the modern health care environment, exploiting the growth of products and reducing the vulnerable things are suggested in a paper [28]. The BeeKeeper-based system in the blockchain and the cloud server on the IoMT were proposed to process the data computations of the user. In the BeeKeeper system, the used Ethereum blockchain technology is proposed in [29] to provide authorization for the medical data stored in the blockchain. Tab. 1 shows the summary of related works on blockchain based IoMT technology.

Table 1: Summary of related works

Name of the author	Domain	Advantage	Disadvantage
Pavithran et al. [30]	Ledger based design of Blockchain	The information of the patient is not accessed by a third party	Storage cost is high
Singh et al. [31]	Fog based architecture in Blockchain	Better security	Difficulty in handling e large computation
Mackey et al. [32]	Blockchains for data management and security	Transmitted data is stored	System access control provides unsatisfactory results
Agbo et al. [33]	Blockchain for privacy and security	High potential for hiding the sensitive information of the patient	Maximum degradation in sharing data
Nanayakkara et al. [34]	IoMT based privacy and security	Improved in network security	Communication between IoMT devices is not effective by the model
Neshenko et al. [35]	IoMT based analysis of cost and performance issues	IoMT ensures high communication security	Computation cost is high
Seliem et al. [36]	Data Management on IoMT	Sensitive information of patient is protected by sensors	Partial perfect privacy of medical data
Banerjee et al. [37]	IoMT with Blockchain	Transmission of data between IoMT devices without loss	Delay in the network

(Continued)

Table 1: Continued

Name of the author	Domain	Advantage	Disadvantage
Fernández Caramés et al. [38]	Ledger based design of Blockchain	Ensures security and data privacy	Inefficiency of monitoring data

Tab. 1 lists the disadvantages of the techniques explained in the literature. The existing blockchain technology is mostly focused on ledger-based design. In this article, the draw backs, such as storage, time, and security, are addressed by using a fog-based IoMT with a blockchain protocol for the improvement of security.

3 Integration of Fog Computing IoMT in Health Care Using Block Technology

The medical history of a patient usually contains personal information, and sensitive medical information should be protected and transmitted to the other sectors of maintenance in a secured manner, which is a vital task. Thus, IoMT devices require a secured storage infrastructure for processing real-time medical data. To improve the high dimensionality of security, fog-computing-based blockchain technology is needed in the IoMT. This paper proposes the concept of integrating fog computing with the IoMT-YAC algorithm in blockchain technology for health care record management (i.e., FC-IoMT-YAC). The proposed technique includes the following (three) functions.

1. Implementation of the YAC algorithm in blockchain technology.
2. Management of heath care data in FC-IoMT-YAC using blockchain technology.
3. Security of healthcare data in FC-IoMT-YAC using blockchain technology.

Fig. 1 presents the FC-IoMT-YAC architecture. The proposed work is a three-tier architecture.

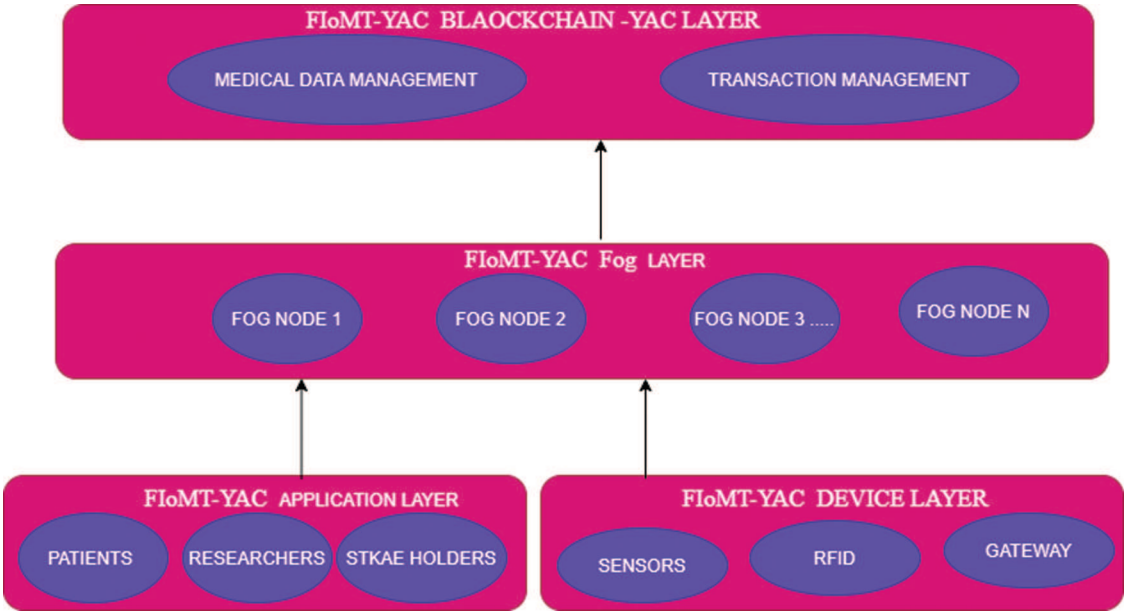

Figure 1: Three-tier architecure of FIoMT-YAC

FC-IoMT-YAC Application Layer

Accessing and manipulating data from patient records are done in this layer. This layer is composed of three modules. In the patient module, patients can view their medical data through the components of the software, allowing them to manage and manipulate their medical data. It acts as a blockchain wallet. Researchers and stake holders can also access medical data through this blockchain wallet when needed. Any of the changes made in this layer are updated in the fog layer.

FC-IoMT-YAC Device Layer

This layer consists of two parts, namely, sensor devices and radio frequency ID (RFID). Patient data are monitored using sensor devices. The IoMT-based RFID is used to tag items and track drug availability problems. Additionally, RFID tags are used for sending signals between two entities. The signals generated by the sensors are received through gateways and sent to the FC-IoMT-YAC fog layer.

FC-IoMT-YAC Fog Layer

This layer is responsible for monitoring medical records, which are near the applications and stored in the subset of data. This layer also receives medical data from the FC-IoMT-YAC application and device layers. A group of modules called fog nodes forms this layer, which is responsible for providing authorization and validation for the FC-IoMT-YAC application layer to manipulate the medical data from a patient.

FC-IoMT-YAC Blockchain-YAC Layer

This layer provides increased security and stores medical records. This layer also provides authorization to a third party to access medical data.

3.1 Proposed FC-IoMT-YAC Consensus Steps Using Blockchain Technology in Health Record Management

The proposed technique aims to efficiently manage the health records of patients in highly secured manner. The benefits of blockchain are as follows:

1. Patients can control their own data, and the members of the family can also view the patients' records.
2. In the blockchain technology, the distribution of data is secured, consistent, and accurate.
3. Any system updated in the blockchain can be easily viewed by all users in the network.
4. Unauthorized users will be prevented from accessing medical data.

For high security and accuracy, the YAC algorithm of blockchain technology is implemented.

Preliminaries of YAC consensus processing steps

Client: The client generates the user request for medical data and sends them to the ordering service (OS). The user who has a public key can associate with the client.

Peer: The node of the network is responsible for validating and storing medical data into the blocks.

Ordering Service (OS): The OS is responsible for organizing the medical data transactions into a known order.

In the YAC algorithm, the client is considered as the peer and can interact with other known peers. Every client has its own private key and a permission to access medical data in the blockchain. The YAC algorithm of blockchain technology can be described by the following steps.

Procedure for YAC consensus protocol of blockchain technology

Step 1: A client creates a medical data transaction with a private key.

Step 2: The client can send the transaction to other known peers. The receiver peer receives the transaction and verifies the validity of the transaction.

Step 3: The OS creates and shares an unsigned block to peers in the network. The unsigned block is called a proposal.

Step 4: For the verified proposal, the peers calculate the hash and sign it. The <Hash, Signature> tuple is called a vote.

Step 5: From Step 4, the hash value is created for each peer and computes the order of peers. The first peer in the list is called the leader.

Step 6: On the basis of the hash value of the proposed block, the voting peer is created.

Step 7: Votes from other peers are collected through the leader and peer sending the commit message to the block.

Step 8: On the basis of the hash value, the leader collects all votes and identifies the supermajority of the votes. Then, a commit message is sent to the committing block, which is called a commit.

Step 9: The receiver peer, receives the commit and verifies its validity. Then, the block is added into the ledger, completing the consensus.

Applying the above procedure increases the security, accuracy, and consistency of the medical data stored in the blockchain. After executing Steps 1 to 9, the medical data block is added into the chain using Algorithm 1.

Algorithm 1: Adding the YAC-algorithm-based block into the chain

Input: Patient Name
Output: The YAC-algorithm-based clock is added to the block chain
Step 1: ***function*** *add_block*(*patient p*)
Step 2: *connect* → *YAC_blockchain*
Step 3: *id* ← *subscribe*(*id*)
Step 4: *read* ← *Get_file*(*n.db*)
Step 5: *new_YAC_block* ← *create_YAC_block*(*read*, *times tamo*, *id*)
Step 6: *out* ← *broadcast*(: *new_YAC_block*)
Step 7: ***if*** (*out are approved*)
Step 8: ***if*** (*new_YAC_block belongs to the same chain*)
Step 9: add *new_YAC_block _in _ chain* ( )
Step 10: print (*new block is added successfully*)
Step 11: ***else***
Step 12: add *new_YAC_block _in _ Fork* ( )
Step 13: print (*new block is added successfully as a fork in the chain*)
Step 14: ***else***
Step 15: reject *new_YAC_block* ( )
Step 16: print (New Block is Rejected)
Step 17: ***end function***

Every new block contains detailed information about the patient. The details include the creation time of the block, the block generator name, and the hash value of previous block. The new_YAC_block is broadcasted to all peers in the network. The acceptance rate value of new_YAC_block is greater than the number of peers, which is added into the chain. If new_YAC_block does not match the previous block, new_YAC_block gets forked. Once new_YAC_block s added to the chain, it cannot be changed.

3.2 Managing the Heath Care Data in FC-IoMT-YAC Using Blockchain

Medical data are created and stored in blocks in a secure way while maintaining privacy, which is very important. The management of stored data in the block is implemented by the usage of data in the block (authentication details) and the storage of data in the block (data analysis and management).

The procedure in managing health care data in the block chain is as follows:

Step 1. Generate the main source of medical data according to the interaction of patient and doctors.

Step 2. Produce a health record with prescription and treatment details.

Step 3. Assign the ownership of the record with sensitive information to the patient.

Step 4. Assign preliminary rights to the owner.

The preliminary rights are (Steps 6 to 9).

Step 5. Request permission to view the record

Step 6. Forward request to the owner

Step 7. Request received by the owner

Step 8. Decide to permit or deny the request

Step 9. Give authorization to the health care providers

Step 10. Obtain access to end-users, like hospitals and health care providers.

In the management layer, the working of the security and integrity preserved storage is recommended.

3.3 Healthcare Data Security in FC-IoMT-YAC

To perform the security of health care data between IoMT devices, fog nodes, and end-users are used. It consists of patients, doctors, IoMT devices, and fog nodes, which use a fog-computing-based YAC algorithm in the blockchain system for storing and securing medical data. Users can retrieve data from fog nodes. The algorithm performs the IoMT device request through different distributed fog nodes. Tab. 2 defines the symbols used in Algorithm 2.

Table 2: Symbols and notations

Symbols	Notations
p_i	Patient
d_i	Doctors
PMD	Patient medical data

(Continued)

Table 2: Continued

Symbols	Notations
IoMT	Health care IoMT devices
hrd_i	Health record
FC_YAC	Fog computing in YAC blockchain

Algorithm 2: Security of health care data between IoMT devices to fog nodes and end-users

Step 1: While p_i in patient **do**
Select p_i
For each hrd_i in $IoMT$ do
If d_i select hrd_i then
Retrieve $PMD\ (p_i,\ hrd_i)$
Store in $FC\_YAC(retrieve\_PMD)$
Else
Select $p_i = 1$
End
End
End
Step 2: Function retrieve $PMD\ (p_i,\ hrd_i)$
$p_1 = p_i$ from patient
While hrd_i in $IoMT$ do
If $hrd_i = p_1$ then
Retrieve $PMD[] \leftarrow p_1\ .\ hrd_i\ .\ retrieve\ value$
Return (PMD)
Else
Assign $p_1 \leftarrow IoMT$
Call retrieve $PMD\ (p_i,\ hrd_i)$
End if
End
Step 3: End;

To arrange the medical data exchanged between the fog nodes and the IoMT devices, an application is proposed for performing the operations and the actions through the YAC algorithm in the blockchain. Each IoMT device is uniquely identified by an "ID," which is stored in the medical data of the patient. The mapping of IDs with the IoMT devices is performed by fog nodes for the identification of the device using a configured data stored on the YAC blockchain.

The sequence diagram (Fig. 2) shows the collection of medical data. The fog node composes the requests of the IoMT device user and sends the request to the patients and the doctors.

4 Result Analysis

The performance of the proposed FC-IoMT-YAC consensus algorithm was analyzed using blockchain technology through the latency, running time, efficiency, reliability, and privacy parameters. Data were collected from the interaction of patients with doctors and stored as health records. The

health records include patient, prescription, and treatment details. Fog computing was used to show the high dimensionality of security and the feasibility of the FC-IoMT-YAC algorithm using blockchain technology. The results were compared with those of three other algorithms, namely, the IoMT with cloud computing [6], the IoMT with fog computing [7], and the proposed work fog computing with the YAC algorithm in blockchain technology (i.e., FC-IoMT-YAC).

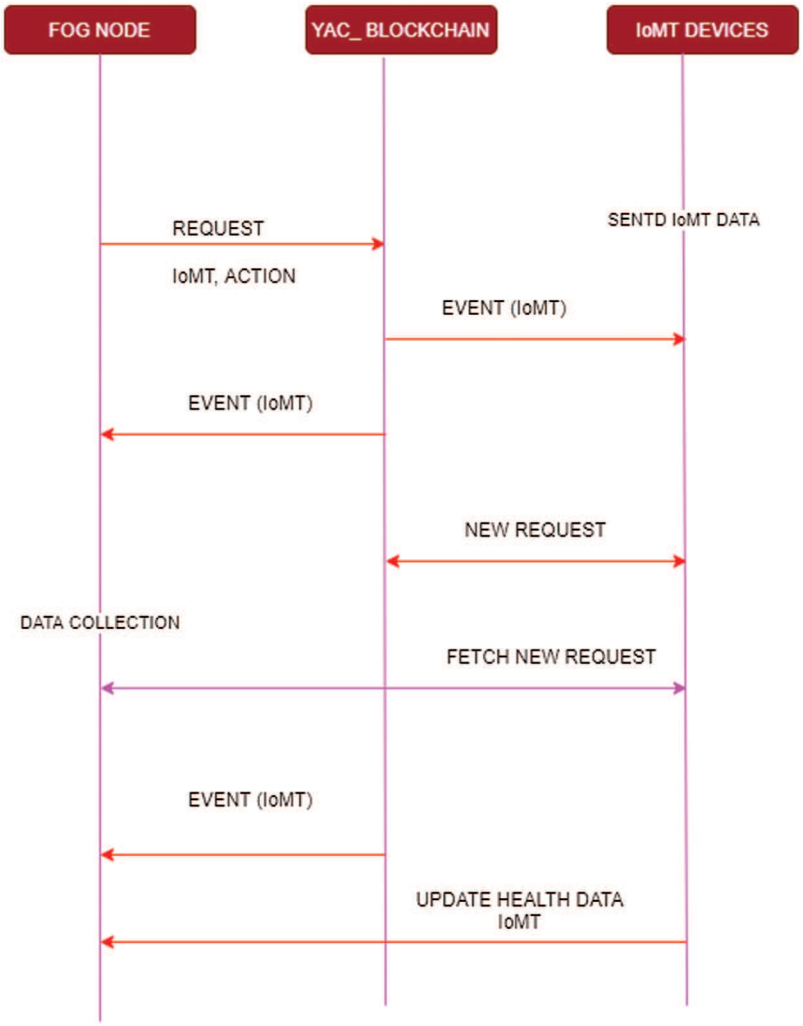

Figure 2: Sequence of steps in the collection of the medical data

FC-IoMT-YAC was implemented using the Java programming language. Furthermore, the fog node executes the YAC consensus algorithm in the blockchain. The aim of the gateway in the FC-IoMT-YAC device layer is to monitor the patient and send the date to the fog node. The fog node is implemented by Raspberry Pi 2 model b. For the blockchain, the YAC algorithm [19] is implemented by the JSON–RPC interface [2]. After installing these software components, the overall test was executed using Apache JMeter. Each test was evaluated on 1000 patient data requests. Finally, the average access time was calculated for each test. Tab. 3 shows the result obtained by using the IoMT with cloud computing.

Table 3: Result obtained by IoMT using cloud computing

Total request	Average access time (ms)	Standard deviation (ms)
1	356.76	148.05
100	1789.45	135.21
200	3457.23	130.67
500	5782.78	125.12
1000	8357.38	120.89

Tab. 3 shows the results of the create and search data requests performed through the communication between the IoMT and the cloud. Tab. 4 shows the results obtained by using the IoMT with fog computing.

Table 4: Result obtained by IoMT with fog computing

Total request	Average access time (ms)	Standard deviation (ms)
1	31.06	3.12
100	335.02	4.82
200	375.61	8.35
500	467.08	14.78
1000	1745.12	23.68

Tab. 4 shows the results of the create and search data requests performed through the communication between the IoMT and the fog. Tab. 5 shows the results obtained by using the proposed approach (i.e., FC-IoMT-YAC)

Table 5: Result obtained by proposed method (FC-IoMT-YAC)

Total request	Average access time (ms)	Standard deviation (ms)
1	15.87	0.72
100	275.67	4.22
200	325.13	6.67
500	413.56	7.97

Tabs. 3 and 4 indicate that the access time (of medical records) of the IoMT with fog computing is optimal. Therefore, the IoMT with fog computing exhibits high performance in terms of several parameters. The average response time increases with the number of requests. The tables also show that the proposed technique produces a good result in terms of the time consumed in accessing medical

records. Fig. 3 shows the reliability of three different methods with the number of files in the data storage. The reliability of FC-IoMT-YAC increases with the number of files.

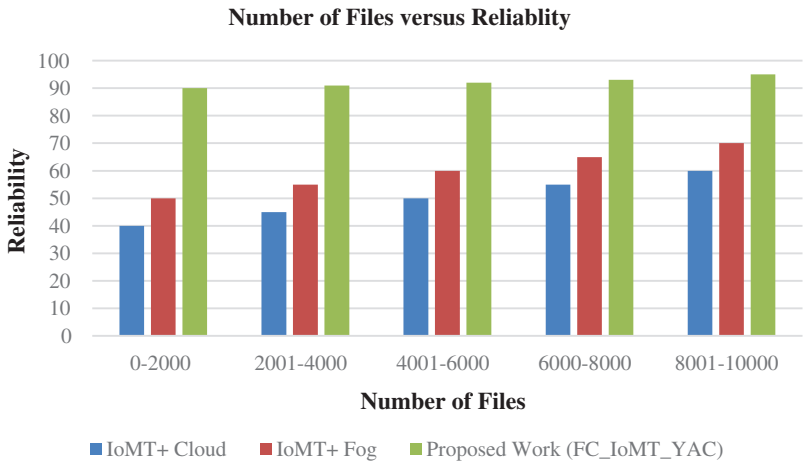

Figure 3: Data volume (number of files) *vs.* reliability

Fig. 4 shows the efficiency of three different methods with the number of files in the data storage. The efficiency of FC-IoMT-YAC increases with the number of files.

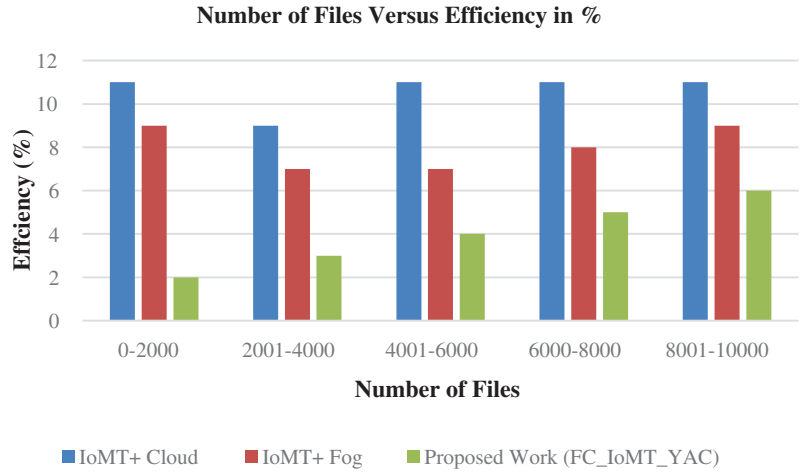

Figure 4: Data volume (number of files) *vs.* efficiency%

Fig. 5 shows the running time using three different methods with the number of files in the data storage. The execution of FC-IoMT-YAC is fast. The running time increases with the number of files.

The proposed work is evaluated based on the latency parameter as shown in Eq. (1).

$$Latency\ of\ service\ delivery = Completion\ time\ of\ task + Network\ propagation \tag{1}$$

Fig. 6 shows the latency of three different algorithms, namely, IoMT + Cloud, IoMT + Fog, and FC-IoMT-YAC. Fog computing brings the computation near the database, reducing the network delay.

If the database is small, the fog computing process will take a short time. The proposed work decreases the latency by using the YAC algorithm of blockchain technology in the fog computing architecture.

Figure 5: Data volume (number of files) *vs.* running time

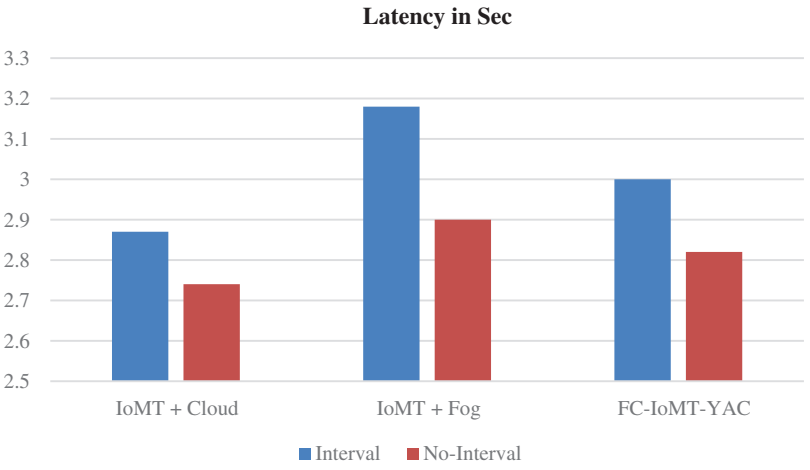

Figure 6: Comparison of latency (proposed work) with YAC blockchain technology

5 Conclusion

This paper describes the health care data management using fog computing based IoMT in blockchain technology. The proposed technique is based on the performance, privacy, and security parameters through the YAC algorithm in the blockchain. The major issue is the security threat during the access and sharing of data over the network. To address this issue, the YAC blockchain provides high-dimensional security and privacy in the IoMT. The embedding of the YAC blockchain in the IoMT provides a decentralized structure in the management of health records. The proposed FC_IoMT_YAC blockchain architecture mitigates the privacy and security threats. The proposed approach, that is, FC_IoMT_YAC, is efficient in the aspects of latency, running time, efficiency, reliability, and privacy. The computation takes only 1563 ms because fog computing and blockchain

technology effectively collect data and implement the patient's request. In future work, soft computing techniques can be utilized to reduce the network problem and increase the efficiency of health record management. The blockchain concept can be further implemented for resolving data storage problems.

Funding Statement: The authors extend their appreciation to the Deanship of Scientific Research at King Khalid University for funding this work under Grant Number (RGP 1/147/42). This research was funded by the Deanship of Scientific Research at Princess Nourah bint Abdulrahman University through the Fast-Track Research Funding Program.

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

References

[1] I. V. Pustokhina, D. A. Pustokhin, D. Gupta, A. Khanna, K. Shankar *et al.,* "An effective training scheme for deep neural network in edge computing enabled internet of medical things (IoMT) systems," *IEEE Access*, vol. 8, pp. 107112–107123, 2020.

[2] G. Bigini, V. Freschi and E. Lattanzi, "A review on blockchain for the internet of medical things: Definitions, challenges, applications, and vision," *Future Internet*, vol. 12, no. 12, pp. 1–16, 2020.

[3] M. Mostert, A. L. Bredenoord, M. C. Biesaart and J. J. Van Delden, "Big data in medical research and EU data protection law: Challenges to the consent or anonymise approach," *European Journal of Human Genetics*, vol. 24, no. 7, pp. 956–960, 2016.

[4] J. Zhang, N. Xue and X. Huang, "A secure system for pervasive social network-based healthcare," *IEEE Access*, vol. 4, pp. 9239–9250, 2016.

[5] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. E. Christidis *et al.,* "Hyperledger fabric: A distributed operating system for permissioned blockchains," in *Proc. EuroSys '18*, Porto, Portugal, pp. 1–15, 2018.

[6] 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.

[7] B. Farahani, F. Firouzi, V. Chang, M. Badaroglu, N. Constant *et al.,* "Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare," *Future Generation Computer Systems*, vol. 78, pp. 659–676, 2018.

[8] I. Azimi, A. Anzanpour, A. M. Rahmani, P. Liljeberg and T. Salakoski, "Medical warning system based on internet of things using fog computing," in *Proc. IWBIS*, IEEE, Jakarta, Indonesia, pp. 19–24, 2016.

[9] S. Sathesh, V. A. Pradheep, S. Maheswaran, P. Premkumar, N. S. Gokul *et al.,* "Computer vision based real time tracking system to identify overtaking vehicles for safety precaution using single board computer," *Journal of Advanced Research in Dynamical and Control Systems*, vol. 12, no. 7, pp. 1551–1561, 2020.

[10] K. Kavin Kumar, M. Devi and S. Maheswaran, "An efficient method for brain tumor detection using texture features and SVM classifier in MR images," *Asian Pacific Journal of Cancer Prevention*, vol. 19, no. 10, pp. 2789–2794, 2018.

[11] M. Kollmitz, A. Eitel, A. Vasquez and W. Burgard, "Deep 3D perception of people and their mobility aids," *Robotics and Autonomous Systems*, vol. 114, pp. 29–40, 2019.

[12] F. Al. Turjman, M. H. Nawaz and U. D. Ulusar, "Intelligence in the internet of medical things era: A systematic review of current and future trends," *Computer Communications*, vol. 150, pp. 644–660, 2020.

[13] M. A. Jan, M. Usman, X. He and A. U. Rehman, "SAMS: A seamless and authorized multimedia streaming framework for WMSN-based IoMT," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1576–1583, 2018.

[14] D. Bruneo, S. Distefano, F. Longo, G. Merlino, A. Puliafito *et al.*, "Stack things as a fog computing platform for smart city applications," in *Proc. INFOCOM WKSHPS*, San Francisco, USA, pp. 848–853, 2016.

[15] H. Dubey, J. Yang, N. Constant, A. M. Amiri, Q. Yang *et al.,* "Fog data: Enhancing telehealth big data through fog computing," in *Proc. ASE BD&SI '15*, Kaohsiung, Taiwan, pp. 1–6, 2015.

[16] T. N. Gia, M. Jiang, V. K. Sarker, A. M. Rahmani, T. Westerlund *et al.*, "Low-cost fog-assisted health-care IoT system with energy-efficient sensor nodes," in *Proc. IWCMC*, Valencia, Spain, pp. 1765–1770, 2017.
[17] M. Ahmad, M. B. Amin, S. Hussain, B. H. Kang, T. Cheong *et al.,* "Health fog: A novel framework for health and wellness applications," *The Journal of Supercomputing*, vol. 72, no. 10, pp. 3677–3695, 2016.
[18] L. Lamport, "Generalized consensus and paxos," *Computer Science*, 2005. https://www.semanticscholar.org/paper/Generalized-Consensusand-Paxos-Lamport/fc3fbb4c76448e8968f8a19f076d133b2e7a2849.
[19] F. Muratov, A. Lebedev, N. Iushkevich, B. Nasrulin and M. Takemiya, "YAC: BFT consensus algorithm for blockchain," arXiv preprint arXiv:1809.00554, 2018.
[20] S. Nankamoto, "Bitcoin: A peer-to-peer electronic cash system," 2021. [Online]. Available: https://bitcoin.org/bitcoin.pdf.
[21] I. Bentov, R. Pass and E. Shi, "Snow white: Provably secure proofs of stake," *IACR Cryptol. EPrint Arch*, vol. 2016, no. 919, pp. 918–919, 2016.
[22] P. Daian, R. Pass and E. Shi, "Snow white: Robustly reconfigurable consensus and applications to provably secure proof of stake," 2021. [Online]. Available: https://eprint.iacr.org/2016/919.
[23] M. A. Uddin, A. Stranieri, I. Gondal and V. Balasubramanian, "A patient agent to manage blockchains for remote patient monitoring," *Studies in Health Technology and Informatics*, vol. 254, pp. 105–115, 2018.
[24] M. Simić, G. Sladić and B. Milosavljević, "A case study IoT and blockchain powered healthcare," in *Proc. ICET*, Antalya, Turkey, pp. 10–25, 2017.
[25] J. Xie, H. Tang, T. Huang, F. R. Yu, R. Xie *et al.*, "A survey of blockchain technology applied to smart cities: Research issues and challenges," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2794–2830, 2019.
[26] J. Indumathi, A. Shankar, M. R. Ghalib, J. Gitanjali, Q. Hua *et al.*, "Block chain based internet of medical things for uninterrupted, ubiquitous, user friendly, unflappable, unblemished, unlimited health care services, " *IEEE Access*, vol. 8, pp. 216856–216872, 2020.
[27] M. Dotoli, M. Fanti, G. Iacobellis, L. Martino, A. Moretti *et al.,* "Modeling and management of a hospital department via petri nets," in *Proc. WHCM*, IEEE, Venice, Italy, pp. 1–6, 2010.
[28] J. D. Rockoff, "Warned insulin pump vulnerable to cyber hacking," *Wall Street Journal Internet*, vol. 3, pp. 31–71, 2016.
[29] L. Zhou, L. Wang, Y. Sun and P. LV, "Beekeeper: A blockchain-based IOT system with secure storage and homomorphic computation," *IEEE Access*, vol. 6, pp. 43472–43488, 2018.
[30] D. Pavithran, K. Shaalan, J. N. A. Karaki and A. Gawanmeh, "Towards building a blockchain framework for IoT," *Cluster Computing*, vol. 23, no. 3, pp. 2089–2103, 2020.
[31] P. Singh, A. Nayyar, A. Kaur and U. Ghosh, "Blockchain and fog based architecture for internet of everything in smart cities," *Future Internet*, vol. 12, no. 4, pp. 1–12, 2020.
[32] T. K. Mackey, T. T. Kuo, B. Gummadi, K. A. Clauson, G. Church *et al.*, "Fit for purpose challenges and opportunities for applications of blockchain technology in the future of healthcare," *BMC Medicine*, vol. 17, no. 1, pp. 1–17, 2019.
[33] C. C. Agbo, Q. H. Mahmoud and J. M. Eklund, "Blockchain technology in healthcare: A systematic review," Healthcare, Multidisciplinary Digital Publishing Institute, vol. 7, no. 2, pp. 1–30, 2019.
[34] M. Nanayakkara, M. Halgamuge and A. Syed, "Security and privacy of internet of medical things (IoMT) based healthcare applications: A review," in *Proc. ICABMIT*, Putrajaya, Malaysia, pp. 1–18, 2019.
[35] N. Neshenko, E. Bou Harb, J. Crichigno, G. Kaddoum and N. Ghani, "Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on internet-scale IoT exploitations," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2702–2733, 2019.
[36] M. Seliem and K. Elgazzar, "BIoMT: Blockchain for the internet of medical things," in *Proc. BlackSeaCom*, Sochi, Russia, pp. 1–4, 2019.
[37] M. Banerjee, J. Lee and R. Choo, "A blockchain future for internet of things security: A position paper," *Digital Communications and Networks*, vol. 4, no. 3, pp. 149–160, 2018.
[38] T. M. Fernández Caramés and P. Fraga Lamas, "A review on the use of blockchain for the internet of things," *IEEE Access*, vol. 6, pp. 32979–33001, 2018.