Protecting the Privacy of IoMT-Based Health Records Using Blockchain Technology

T. C. Swetha Priya and R. Sridevi

1 Introduction

Due to tremendous increase in the population of India, it has become a pressure on government to accommodate the healthcare facilities. The government is trying to accommodate the increasing urban population but could not reach the daily increase rate of population. So this has urged the need for latest technology to meet the increasing population health requirements. As the population increases, the need for medical facilities also will be more, and there will be more people with different health problems. So, there will be a need for remote healthcare in recent times. So that there will not be any need for more hospitals. Instead we can have latest technological advancements in terms of embedded devices, smart wearable gadgets, and many such low-cost devices used for healthcare of people. According to modern researchers, it is evident that these less expensive small smart devices have the ability to record health information of a patient and even monitors patient condition 24 × 7.

The IoT technology [1, 2] is one such technology that handles low cost, smart devices, or embedded devices which offers wireless connectivity between smart medical devices, patients, and doctors. IoT technology is based on wireless sensors that continuously records the signals and maps them with various parameters and will be communicated through the IoMT-based network. The received information is processed, stored, and examined with already present data. This data will be used by doctor to suggest appropriate treatment.

T. C. Swetha Priya (✉) · R. Sridevi
Department of Computer Science and Engineering, JNTUH University College of Engineering, Science and Technology, Hyderabad, Telangana, India
e-mail: tcswetha3552@gmail.com

R. Sridevi
e-mail: sridevirangu@jntuh.ac.in

J. K. Mandal et al. (eds.), *Proceedings of International Conference on Network Security and Blockchain Technology*, Lecture Notes in Networks and Systems 738,
https://doi.org/10.1007/978-981-99-4433-0_34

The IoMT [3, 4] comprises medical devices [5], software, and related hardware connected over the Internet for providing connectivity to health-related information. This concept was previously called as IoT for healthcare [6]. IoMT allows remote connectivity of wireless devices for communicating and analyzing the health-related information over the Internet. IoMT has evolved from the concept of IoT. IoT is an interconnection of computing devices that communicate data over the devices without human intervention. IoT supports connectivity between electronic devices providing communication of data between devices in various applications. IoT has made our lives easier when compared to the previous situation.

Figure 1 demonstrates how the communication between devices connected over the network in medical application will happen. Here, all the data will be stored in the central repository in digital format and will be made available to all the stakeholders like the medical lab staff, patients, and doctors involved in the network. So, a patient's complete information can be maintained with the help of this type of IoT-based systems automatically without human intervention. So, such patient's record can be helpful in analyzing the past and predicting the future status of a patient's health condition. So, with the help of such systems, we can automate the old medical devices to meet the present day needs to support real-time data by adding extra devices, sensors, converters, and modems.

IoT systems has complex architecture comprising of various components that interact with each other to support real-time data monitoring, gathering, transferring, and analyzing collected data. IoT includes various technologies that include

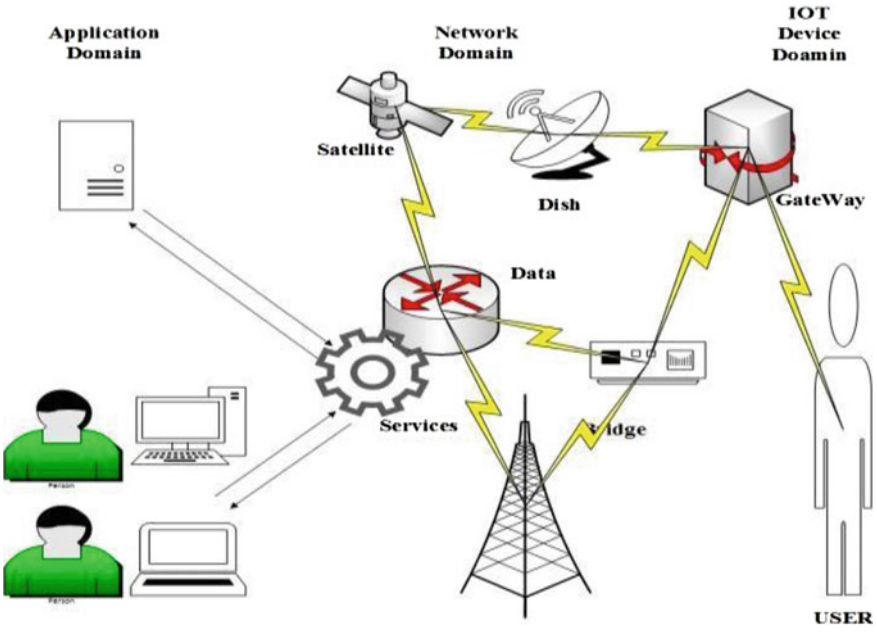

Fig. 1 Communication in IoT

smart homes, augmented reality, smart grids, and so on. IoT integrates the components with these technologies to support real-time data. Now, healthcare has also been transformed through IoT. So the term IoMT has evolved from healthcare application of IoT. IoMT devices can be embedded into various categories like depression monitoring, remote patient monitoring, hygiene monitoring, glucose monitoring, connected inhalers, smart contact lenses, robotic surgery, heart rate monitoring, mood monitoring, and ingestible sensors which has capability to collect data from remote locations. This IoMT can also be helpful in early recognition of various diseases, prevention of dangerous diseases, monitoring monthly status of a patient, and remote diagnosis and cure in critical situations.

But to store such huge data of increasing population, we need a technology that can handle large databases. But relational databases do not allow dynamic updates to the patient's data. So a technology that is similar to relational database called blockchain technology is introduced. Blockchain technology is one of the emerging computer protocol generally used for storing electronic records on multiple nodes of the network [7]. Blockchain stores the information in encrypted form or simply in the form of transactions called blocks that are connected in the form of chains. Each block will maintain a header for identification; block ID, the hashed link to corresponding chains. This feature does not allow alteration or deletion of data. Each node in the network has complete blockchain information giving data access publicly to the devices present in the IoMT system. The devices or nodes are patients, lab technicians, and doctors. This is disseminated data storage where data is available to all nodes. So even a small variation in data is immediately identified. So, one advantage of such technology is that we do not require any professional for maintaining security of the data in blockchain.

2 Related Work

Many of the authors have been into research for many years for providing security to the IoMT Network. They have proposed various solutions for protecting the privacy of IoMT [8]. The basic solution that was proposed is encryption of data. The data which is in plain text format is encrypted at the sender side, and it is transformed into cipher text. The cipher text that is communicated over public transmission medium is now sent to receiver which converts cipher text back into plaintext. One such method proposed is end-to-end key management in which keys are exchanged with less utilization of resources. Another solution is proposed by [9] which deal with privacy and protection of healthcare systems. This paper has proposed a lightweight encryption algorithm which is an extension of DES. Hu et al. [10] and Li et al. [11] proposed a scheme that reduces utilization of resources. This method is based on cloud-based IoT sensors [12] to monitor personal information of patient including digital signature and timestamp information. This method uses an improved version of data encryption standard which uses homomorphism algorithm. Gong et al. [9], Li et al. [11], and Sun et al. [13] proposed a key agreement-based secure authentication

method for a IoT cloud system. The method secures medium when the participants register for network. This paper proposes that it addresses challenges in healthcare systems. Li et al. [11], Alasmari and Anwar [14], Esposito et al. [15] proposed cloud-based method for wireless networks in healthcare field. It supports various dynamic security policies that depend on attribute encryption and cipher text policy. Louni et al. [16] introduced an access control method to Patient E Health Records stored in trusted servers. This proposal could provide security at higher level for patient health information by providing attribute-based encryption for encrypting the health records for providing good access control to healthcare information. The servers or cloud [16, 17] environment that is storing the health records are not completely trusted. But the health records should be stored with consistency and integrity. But this data is lacking security, and data is altered or may be removed by unauthorized users. So we need security policies that restrict the unauthorized access. So one way to secure data is encrypting sensitive data before it is transmitted to the other party. Here, the information that has to be secured is patient attributes like disease and type of illness caused. So, these attributes must be protected by providing proper access to patient health records. Yeh et al. [18] have designed an advanced communication technique that is based on networks. They proposed an IoT system for body sensor network that provide effectiveness and security to IoT network. Hu et al. [10] have proposed a multi-communication standard-based IoT system for healthcare devices.

But the previous works have a drawback on data storage system connectivity among various data gathering devices that monitors data constantly at periodic time interval and analyzing data. So, to overcome this drawback of database connectivity and security to the healthcare information, this paper suggests a blockchain-based technology to secure the privacy of IoMT health records.

3 Proposed Work

Due to the widespread use of Internet of things which connects physical things through the means of Internet. Also with the increase of embedded devices technology, IoT technology has widespread demand in all fields including medical and healthcare technology [19]. It helps the future generation to have access to the information at any time and to become smarter and stronger in retrieving up to date information. IoT has capability to integrate real and virtual world. It covers a huge range of advancements technologically that comprise of wearable embedded devices, sensors, cloud computing, ICT, etc., so, IoT has been into one of the fast growing technology in healthcare fields [20]. In the modern wireless communication era, IoT has gained exponential growth. The aim of IoT is to connect every device or object at any instance.

The IoMT comprises a set of smart devices that are attached to Internet for providing medical service to any type of users. As time is passing, healthcare industry is slowly adapting IoT-related solutions leading to advancement of IoMT technology. IoMT technology works in this manner: A test report is sent from pathological lab

to patient relatives mobile or the smart watch having tracker collects data and that is examined by doctor's smart phone. This technology involves reliable and an affordable cost handy devices that are embedded in the watch or smart phones that enable interconnection between patients, medical equipment, lab technicians, and doctors. The sensors present will record patient information and compare with existing patient information, and by implementing decision support systems, the doctor can give better treatment and can predict further health risks and warn patient of risks and can suggest better diet.

Because of the widespread and diverse nature of IoMT, several security problems arise. Because of increased utilization of smart devices, integrity of information sent over IoMT should be handled in an efficient manner. So, there is a need for securing the IoMT network from cyber attackers and other third parties through which transferring of patient data is possible. So, one of the possible solutions for securing this patient information is blockchain technology.

3.1 Overview of Blockchain Technology

Blockchain [21, 22] technology because of its unique characteristics such as security, distributed nature, decentralization, and data transparency offers a greater potential to promote various fields. A blockchain works without a centralized server. A blockchain is a network that makes use of databases distributed throughout to share and store information. A blockchain has the capability to maintain a large set of records. Here, there is no central authority to monitor data. It also allows unauthorized parties to do transactions in the network. The transactions that are performed in the network will be notified to each and every peer system present in the network so that all nodes will be aware of the transactions. If any unauthorized user tries to change the data, the other peers will know that some unauthorized activity is being done on the data records because of the variation of hash of the data records present in successive blocks. So, because of these advanced security features and hashing capabilities of blockchain [23, 24], it is an apt solution for securing IoMT health records.

The blockchain includes blocks that are linked to one another that have cryptographic hash of the previous blocks. The chain only stores an associated hash of data records. These blocks include the transactions performed between nodes, base stations, and users. Because of inclusion of hash, all the data records and transactions are immutable. A blockchain is depicted in Fig. 2.

An application programming interface enables communication as well as exchange of data between devices. With the help of API only, interoperability between various sensors and processes is possible. Also it is possible to perform hashing on data and store data directly from sensor nodes, processes, and algorithms.

Due to the advanced characteristics and properties of blockchain technology, it has become one of the mostly used technologies. Some of the relevant characteristics of the blockchain technology are summarized as follows:

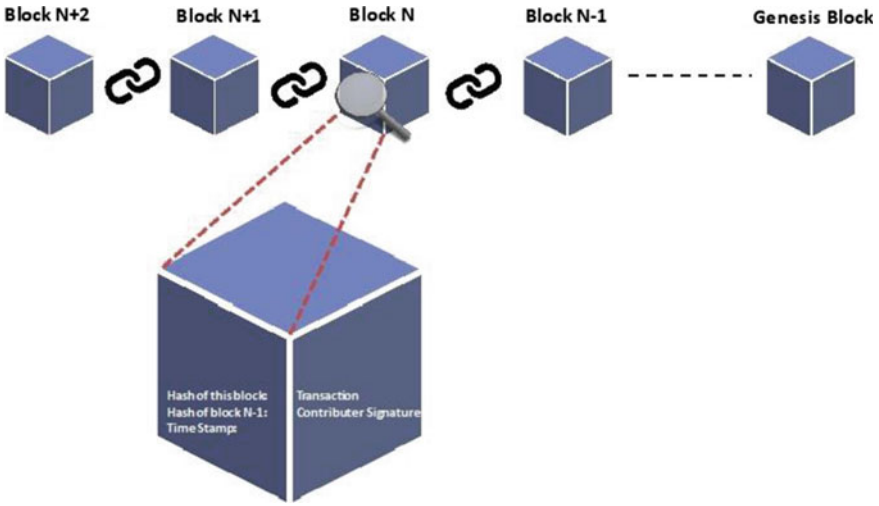

Fig. 2 Structure of blockchain

i. **Stability**

The patient health record once stored in blockchain will not get modified or removed by anybody. This feature enables users to choose this technology.

ii. **Access**

Each blockchain has two types of access: permission less and permission blockchains. Permission less blockchain does not require any permission for data access. It allows any user to access data in blockchain network. A permission blockchain requires access to network to view or alter data. This type of blockchain allows only a certain amount of nodes and gives access rights to only those nodes.

iii. **Cryptographic Hash**

Each block in blockchain is associated with hash of the previous block. This type of implementation of hashing ensures that any kind of changes made to information present in the block affects the subsequent hash values making the entire chain invalid.

iv. **Timestamp**

The records in blockchain will be time stamped. A combination of timestamp with cryptographic hash provides more security. Each record including block creation, transaction, and storage of data in blockchain will also be time stamped.

v. **Decentralized Nature**

This feature helps in eliminating the central authority dependency and removes the single point of failure. Here, a blockchain supports decentralized network where the entire blockchain or only a part of blockchain is distributed over the network. The decentralized versus centralized [25] nature of blockchain is illustrated in Fig. 3.

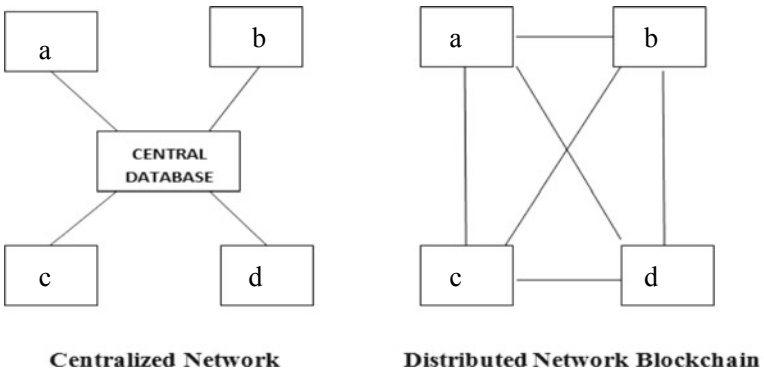

Fig. 3 Distributed versus centralized network

3.2 Types of Blockchains

Basically, three categories of blockchain exist. They are summarized as follows:

i. **Public**

This category of blockchains allows any type of users to access blockchain, and all users are having equal permissions to create, access, or modify the data in the blockchain. This category of blockchains comes under permission less type of blockchain.

ii. **Private**

This category of blockchains allows only a specific group of users who have permission rights to access blockchain. So this blockchain can be considered as permission blockchain. This category of blockchain is controlled by a central authority that has rights to give access to a specific set of authorized users.

iii. **Consortium Blockchain**

The private blockchain is controlled by an authority where as a consortium blockchain is controlled by a group of third party organizations rather than a single one. It also provides high levels of security compared to other type of blockchains.

Because of these advanced features and new opportunities provided by blockchain, blockchain technology has wide scope in healthcare field. It is used to store the patient health record in electronic form. It follows distributed architecture that is the database is stored in hundreds and thousands of computers and users. That means data is redundantly saved in encrypted form in chains. This type of concept helps in reducing the loss of information because this redundant data acts as a backup, i.e., even if data is lost, it can be retrieved from other users. This eliminates the distributed denial of service attacks making it impossible for the hackers to replace or destroy data. In this blockchain technology, new data can be easily added but we cannot modify or remove existing data from chain. Also this technology provides high level

of encryption using private keys which hides the original information from malicious attackers. This has an advantage that if any malicious user tries to change data in record and want to save the data, it requires confirmation from other peer users. If there is any mismatch in any data from other users, that data record will be canceled. This makes the whole blockchain complete. This feature of blockchain makes it a suitable choice for IoMT technology. With this blockchain technology, the patient can be sure that his information is secure and will not be altered by any others. Also a patient can give access to his health-related information to the concerned doctor who is treating the patient. The doctor also can get data from any place in the world.

3.3 Implementation of Blockchain Technology in Healthcare

Blockchain helps in creation of patient record where high security can be provided to data from anywhere. Also the patient data will be synchronized from any place giving the doctor chance to review the history of patient and can suggest recommended treatment based on current and past history of patient only with prior permission of patient. This technology helps in getting the patient information at one place by providing security in a distributed environment.

Previously, creation of patient record, collection of patient information, storing data, and securing the data require more time and waste of space. Even the hardware cost is also more when manual work is more. But now with advancement in IoMT technology, the updating of data will be done on time automatically as that in real time and even the time is also reduced. With IoMT, the doctor can get updated patient information within a few seconds. This helps in identification of patient's health problem and provides diagnosis and medicate in an early stage without going to serious conditions.

Also previously, the data received from multiple sources is not in a common format. When data has to be consolidated and stored in single standardized format it used to take several years for consolidation. This posed a major problem to reliability of information. Also manual patient information monitoring [26] requires confirmation from the patient. But introduction of blockchain technology in healthcare has solved this problem by using standardized protocols and e-records of the patient. It also records each and every transaction between medicine dealer and hospital in the blockchain for providing authentic medicines to patient.

In future, blockchain technology will rule the IoMT. The IoT devices [27] whether may be smart watches, gadgets, etc., will capture patient information using embedded sensors in smart devices and can gather information like heartbeat, temperature, blood pressure, oxygen levels, etc., and send the data to e-record of the patient 24 h and 7 days. This information can be monitored by doctor at any time and can diagnose the disease within few hours and give appropriate treatment. Thus, blockchain technology will create a new revolution in medical field. Blockchain technology in healthcare can be illustrated as shown in Fig. 4.

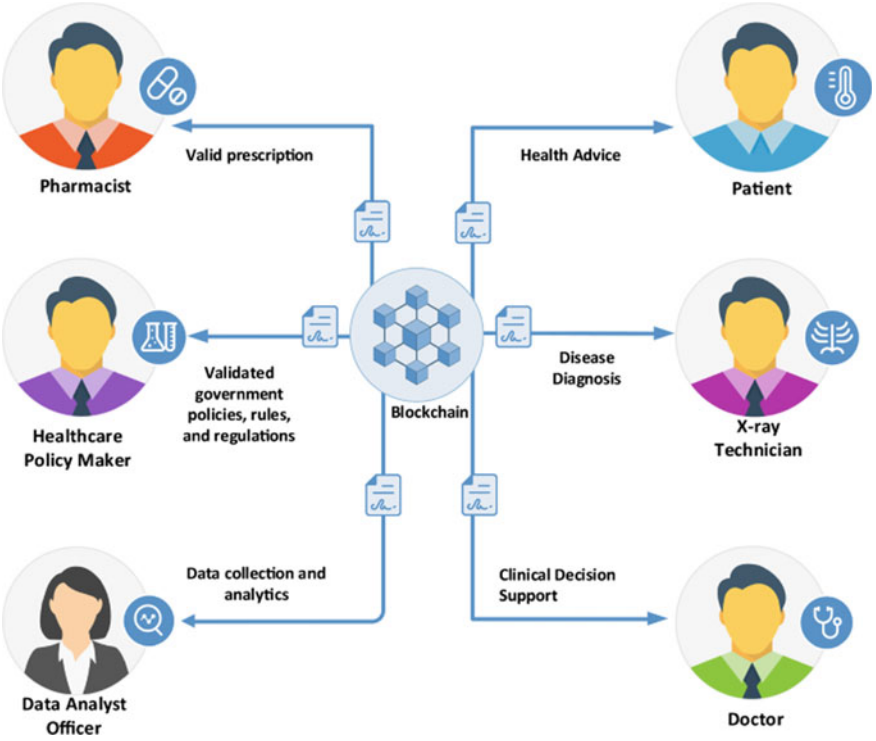

Fig. 4 Blockchain in healthcare

4 Discussion

Blockchain technology is an effective solution for providing solution in healthcare [28]. For secure transmission of patient information, blockchain technology is used in the proposed architecture to provide more security to data. The data structure used is blockchain which stores the important patient health related information in encrypted form. Figure 5 shows the proposed IoMT architecture based on blockchain.

In this type of architecture, the doctor will be in some distant or remote place monitoring the patient [29], and based on condition of patient, the doctor advises proper medication by analyzing the reports generated from laboratory. The reports received from diagnostic center which are in electronic form will be uploaded by practitioner and are updated to the existing patient's history. Along with electronic health records, the patient health information is also captured from the smart wearable devices. These electronic health records are maintained confidentially. By analyzing the tracking information along with the reports, the doctor who is present in distant location can suggest proper treatment at any time. This data will also be recorded in the blockchain in the form of new blocks. The diagnostic laboratory people who are part of IoMT architecture have access to add electronic records to blockchain. When

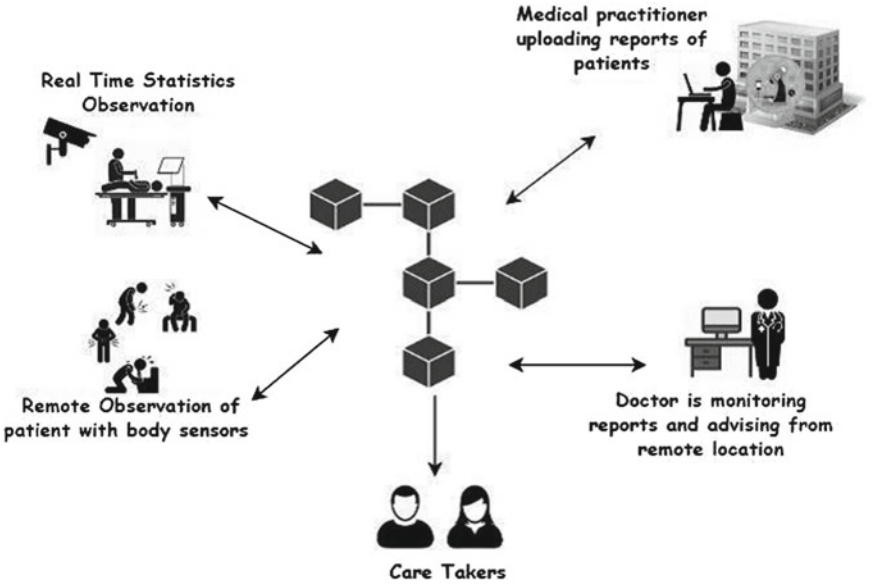

Fig. 5 Blockchain-based IoMT architecture

new patient information is added to IoMT network, a new block of data is appended to end of blockchain as depicted in Fig. 6.

Every block has the information related to patients, time at which patient record is created and the owner who has created a block. When a novel block is appended to the chain, this information is broadcasted into patient network. Every device in the IoMT system receives the block, and after getting approval from most of the peers, then only the block will be added to the end of chain. If this do not have any comparison with preceding block, then this block do not belong to this chain. But once any new block matches previous block, then it is added to chain. But once a block enters into the chain, it should not be altered or removed from chain. If any such alteration to data happens, then it will be immediately noticeable to every node in the network. That is how complete patients history is publicly visible to all peers in network in an authorized manner.

Appending a block to blockchain is depicted in Fig. 7. In this manner, blockchain provides high security to patient's data. The healthcare provider will take care of addition of new patient information. As and when a new patient enters into the IoMT network, a new block is created with the timestamp, patient data, and identity information. Now, the newly created block has to be broadcasted to all the peers present in the network. Now, the decision will be made by peers whether to approve the new block or not. If the approval is received from all the devices in the IoMT system, then the block is appended to existing blockchain. Otherwise, the block is rejected. The same process will be followed throughout the network upon addition of new patient.

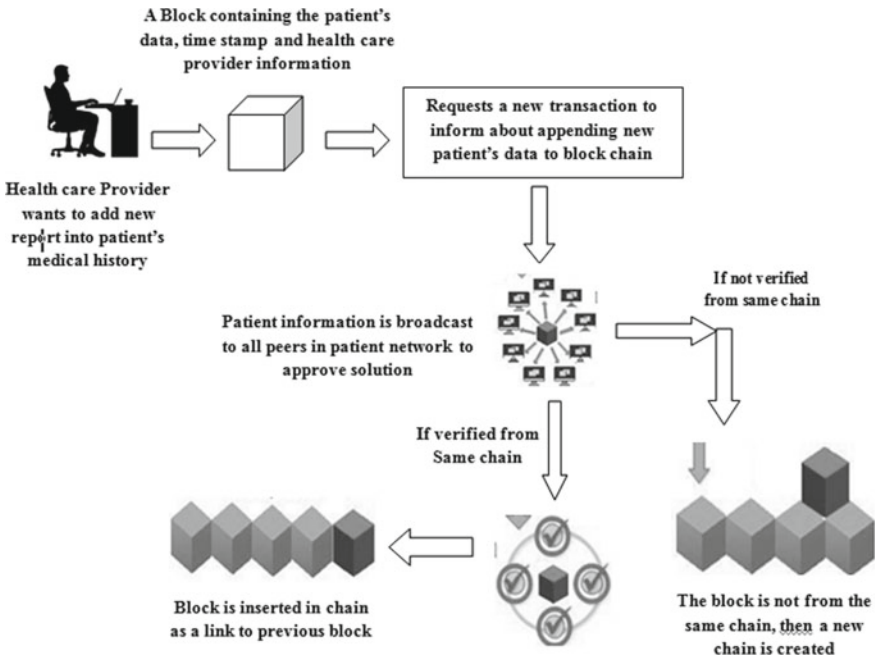

Fig. 6 Adding a block to blockchain

The blockchain technology considers the patient health records that goes to or comes from different devices connected in the IoMT network as transactions [30]. A transaction is illustrated as shown in Table 1.

Information that is exchanged among nodes, patients, lab assistants, and doctors is considered as transactions. The fields present in the table are explained as follows: The previous transaction field is a number that represents the transaction ID. The transaction number represents the transaction count. The node ID represents the number of node. The next field represents the transaction type. This particular field has 5 options or simply they are 5 different types of transactions. They are Start, Save, Retrieve, Examine, and Update. The **Start** transaction represents the first transaction. The **Save** option is used when the patient information has to be stored into the chain. The **Retrieve** option is used when the patient or doctor wants any crucial information for diagnosis. The **Examine** option is used to analyze the patient information that is retrieved from option 3. The **Update** option is used when any patient information has to be modified or any changes have to be updated to chain. The next field is SigReq that represents the node's unique signature. The last field is the actual data that is exchanged over network.

A block comprises of collection of **transactions**. The transaction is stored in the available space in block. If the block gets full, then the transaction is stored in the newly created block. A block header is maintained for every block so that the hash is

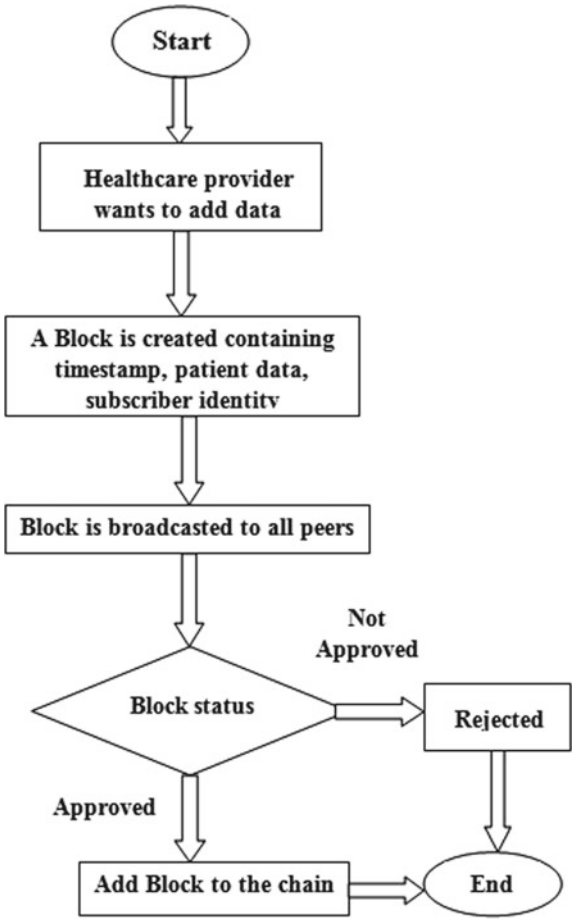

Fig. 7 Process of adding a block to blockchain

Table 1 Transaction

Preceding transaction	Transaction ID	Node number	Type	SigReq	Information
			0 = Start		
			1 = Save		
			2 = Retrieve		
			3 = Examine		
			4 = Update		

Table 2 Representation of policy

Requester	Request for	Node ID	Action
	…	……	
U_h	Retrieve	< Node IDs >	Allow
…	.	…	
$N_{1.....}N_h$	Update	< BS IDs >	Allow

computed for preceding and subsequent blocks. So the computation of hash in this chain ensures consistency of information.

The access given to the patients, lab assistants, and doctors is named as policies [30]. These are stored in representation of block. The modifications made to the IoMT network result in the formation of novel policies. The structure of policy is presented in Table 2.

The patient health information update to all the nodes is done as follows: First, the patient nodes send the information to be updated to all peer nodes or to all the base station [31, 32] in the form of cipher text. Now, the policy lookup is done, and verification is done on whether the patient has access to update the requested information or not. Once the status in the policy lookup table is "allow", then the requested information is encrypted and updated to all the nodes. This updation has to be recorded as transaction. This updated record must be signed with timestamp and is encrypted and exchanged to patients in the IoMT system. So, this facilitates to have updated information with all the peer nodes. So if any person tries to change the data, then all the nodes will be notified about the changes made, and these updations will be canceled because there will be mismatch in the computed hash if the data is modified in only in single block. This helps in protecting the privacy of the patient's health records.

If the users of IoMT network, i.e., the lab assistants, doctors, patients, etc., requests access to the patient's updated information, then the policy check has to be done for that particular user. If the policy lookup has "retrieve" permission, then the user is allowed to access the requested information. Then, the patient health record is obtained and is signed with the key [33] of the base station that provides data. Then, the transaction has to be updated to all the users of IoMT network. This transaction data is encrypted and signed with random keys. Now, this information is communicated to all the nodes in the network. This is how patient health information is accessed from the blockchain providing secure access to the data.

5 Conclusion

Because of the revolutionary rise in IoT technology in various fields, many industries could utilize this opportunities very fastly. One such industry is the healthcare industry which could make use of these Internet of medical things-related things [34]. Because of this varied nature, security will be one of the important issues. So,

blockchain technology promises privacy and security of health records in IoMT. It provides security to electronic health records of patient and provides access publicly to the users in IoMT network. Thus, blockchain provides privacy and security to the patient information. Blockchain technology will not replace advanced or ancient technologies. But blockchain can be a complementary application to other similar technologies. In future, this even may lead to development of new technologies that provide privacy to health records.

6 Future Work

As we keep on storing the new patient's health record information in the form of transactions, the size of blockchain will also increase. This leads to need of extra space. But the traditional method of using database systems may not be efficient method for storing the blockchain. So, to overcome this extra memory requirement issue, in future, we can extend the blockchain to be saved in an external cloud environment.

References

1. Atzori L et al (2010) The Internet of Things: a survey. Comput Netw 54:2787–2805
2. Cisco (2017) Enterprises are leading the internet of things innovation. Huffington Pos, Huffpost News
3. Rodrigues JJPC et al (2018) Enabling technologies for the Internet of Health thing. IEEE Access 6:13129–13141
4. Robert S et al (2012) Internet of M-health things. In: 2011, IET Seminar
5. Mohan A (2014) Cyber security for personal medical devices Internet of Things. In: IEEE international conference on distributed computing in sensor systems, Marina Del Rey, CA, pp 372–374
6. Porambage P et al (2015) Secure end-to-end communication for constrained devices in IoT-enabled ambient assisted living systems. In: IEEE 2nd World Forum on Internet of Things, Milan, pp 711–714
7. Qiao R et al (2018) Blockchain based secure storage scheme of dynamic data. Comput Sci 45:57–62
8. Halpin H, Piekarska M (2017) Introduction to security and privacy on the blockchain. In: European symposium on security and privacy workshops (EuroS & PW), IEEE Computer Society.
9. Gong T et al (2015) A medical healthcare system for privacy protection based on IoT. In: Proceedings of the 7th international symposium on parallel architectures, algorithms, and programming (PAAP), pp 217–222
10. Hu J-X et al (2017) An intelligent and secure health monitoring scheme using IoT sensor based on cloud computing. Journal of Sensors 2017:3734764
11. Li M et al (2013) Scalable and secure sharing of personal health records in cloud computing using attribute based encryption. IEEE Trans Parallel Distrib Syst 24(1):131–143
12. Hassan Alieragh M et al (2015) Health monitoring and management using internet-of-things (IoT) sensing with cloud-based processing: opportunities and challenges.

13. Sun W et al (2018) Security and Privacy in the medical internet of things: a review. Hindaw Secur Commun Netw 2018:1–9
14. Alasmari S, Anwar M (2016) Security and privacy challenges in IoT-based health cloud. In: International conference on computational science and computational intelligence. doi: https://doi.org/10.1109/CSCI.2016.43
15. Esposito C et al (2018) Blockchain: A panacea for healthcare cloud-based data security and privacy? IEEE Cloud Comput 5(1):31–37
16. Louni A et al (2016) Healing on the cloud: secure cloud architecture for medical wireless sensor networks. Futur Gener Comput Syst 55:266–277
17. Cubo J, Nieto A, Pimentel E (2014) A cloud-based internet of things platform for ambient assisted living. Sensors 14(8):14070–14105
18. Yeh K-H (2016) A secure IoT-based healthcare system with body sensor networks. IEEE Access 4:10288–10299
19. Páez DG et al (2014) Big data and IoT for chronic patients monitoring. Springer, pp 416–423
20. Yin Y et al (2016) The Internet of Things in healthcare: an overview. J Ind Inf Integr 1:3–13
21. Zyskind G, Nathan O, Pentland AS (2015) Decentralizing privacy: using block chain to protect personal data. In: Proceedings—2015 IEEE Security and Privacy Workshops, SPW 2015, pp 180–184
22. Yuan Y, Wang F (2016) Blockchain: the state of the art and future trends. Acta Autom Sinica 42(4):481–494
23. Hölbl M et al (2018) A systematic review of the use of blockchain in healthcare. Faculty of Electrical Engineering and Computer Science, University of Maribor, Slovenia
24. Darshan KR, Ananda Kumar KR (2015) A comprehensive review on usage of internet of things (IoT) in healthcare system. In: International conference on emerging research in electronics, computer science and technology
25. Krishnan B, Sai SS, Mohanthy SB (2015) Real time internet application with distributed flow environment for medical IoT. In: International conference on green computing and internet of things, Noida, pp 832–837
26. Khan SF (2017) Health care monitoring system in Internet of Things (loT) by using RFID. In: IEEE international conference on industrial technology and management, pp 198–204
27. Barro-Torres SJ et al (2012) Real-time personal protective equipment monitoring system. Comput Commun 36(1):42–50
28. Kumar DD, Venkateswarlu P (2016) Secured smart healthcare monitoring system based on IoT. Imperial J Interdiscip Res 2(10)
29. Saha HN, Auddy S, Pal S et al (2017) Health monitoring using Internet of Things (IoT). IEEE J 2017:69–73
30. Swetha Priya TC, Kanaka Durga A (2020) Clustering-based blockchain technique for securing wireless sensor networks. Data Engineering and Communication Technology. Springer, Singapore, pp 461–471
31. Deng R, He S, Chen J (2018) An online algorithm for data collection by multiple sinks in wireless sensor networks. IEEE Trans Control Netw Syst 5(1):93–104
32. Reddy NG, Chitare N, Sampalli S (2013) Deployment of multiple base-stations in clustering protocols of wireless sensor networks. In: 2013 international conference on advances in computing, communications and informatics (ICACCI), pp 1003–1006
33. Rahman M, Sampalli S (2015) An efficient pair wise and group key management protocol for wireless sensor network. Wireless Pers Commun 84(3):2035–2053
34. Yeole AS, Kalbande DR (2016) Use of Internet of Things (IoT) in healthcare: a survey. In: Proceedings of the ACM symposium on women in research 2016 (WIR '16). Association for computing machinery, New York, NY, USA, pp 71–76. https://doi.org/10.1145/2909067.2909079