Blockchain: Securing Internet of Medical Things (IoMT)

Nimra Dilawar[1], Muhammad Rizwan[2], Fahad Ahmad[3], Saima Akram[4]
Department of Computer Science, Kinnaird College for Women [1, 2, 3]
Institute of Biochemistry & Biotechnology, University of the Punjab[4]
Lahore, Pakistan

***Abstract*—The internet of medical things (IoMT) is playing a substantial role in improving the health and providing medical facilities to people around the globe. With the exponential growth, IoMT is having a huge influence in our everyday life style. Instead of going to the hospital, patient clinical related data is remotely observed and processed in a real time data system and then is transferred to the third party for future use such as the cloud. IoMT is intensive data domain with a continuous growing rate which means that we must secure a large amount of sensitive data without being tampered. Blockchain is a temper proved digital ledger which provides us peer-to-peer communication. Blockchain enables communication between non-trusting members without any intermediary. In this paper we first discuss the technology behind Blockchain then propose IoMT based security architecture employing Blockchain to ensure the security of data transmission between connected nodes.**

***Keywords*—Blockchain; IoMT; peer-to-peer; security; proof of work (PoW)**

I. INTRODUCTION

The number of connected devices is increasing with every pass day and taking account the continuous increment of connected devices, a new network infrastructure is being planned and introduced. Different production houses have proposed a new perception of the Internet with the Internet of Things (IoT). IoT is expanding rapidly and forming itself as a huge part of the future Internet. The Gartner report [1] predicts that IoT devices will rise to 26 billion in 2020 while Cisco mentions 50 billion [5]. According to forecasts [2], an extensive progression in Machine-to-Machine connections is expected in the upcoming years which may be related to a broader range of applications like home automation [3], transportation [4], wearables [6] or augmented reality [7].

The Internet of Things (IoT) is gaining an exponential growth in the scenario of modern wireless communication. IoT can be defined as "things connected to the Internet" to supply and access all real time information. An IoT device can be smart or any electronic device from wearables to hardware devices with a range of applications comprise of many areas of society [8]. The Internet of Things is the diversification of the existing Internet services. The purpose to connect everything is to accommodate each and every object which exists in the IoT network or likely to exist in the future. The notion to connect everything at any time is captivating.

The internet of medical things (IoMT) is a collection of devices connected to the internet to provide health related services. Basically IoMT is a connected infrastructure of health system such as medical devices, software applications and services as shown in Fig. 1. More explicitly, connection between devices and sensors enables the health care organizations to make their clinical operations and workflow management more efficient and monitoring of patient health even from remote locations. The IoMT integrate the digital and physical world together to speed up the process of diagnosis and treatments with more accuracy to improve the patient health and modifies patient behavior and health status in real-time. Connection of medically related devices will have a profound impact on patients and clinicians.

Healthcare industry is incorporating IoT based solutions swiftly. There is also a 2020 projection made for IoMT. The connected medical devices of the IoMT for diagnosis, monitoring and patients' treatment are expected to rise from $14.9 billion to $52.2 billion by 2022 [9].

To illustrate the IoMT vision, one can imagine that an electronic medical report (EMR) is sent from the medical test center to the patient's smart phone or a patient wears an activity tracker for heart treatment which is monitored by a doctor on a smart phone. These scenarios demonstrate a simple machine-to-machine (M2M) communication which supports IoMT.

Along with the expeditious increase and diverse nature, securing IoMT has become a huge challenge due to advance security problems arise while pervious security problems have become more intense. Hence, security and privacy of IoMT is in our core consideration [10]. The meaning of data security is to store and transfer data without any unauthorized access to assure integrity, authenticity, validity and data privacy. The protected data can only be retrieved by authenticated users [11]. Cybercrime harms devices and networks day by day because anonymous users are communicating with each other. The great amount of IoMT data is collected, transferred and delivered among different parties. The transactions should be done in a secure fashion. Because of this enormous shift, the way for cyber-attacks is more prone and now there is an urgency to make IoMT more secure. The research provides supervision for the use of Blockchain technology with the aim of making a more secure and trustable IoMT model.

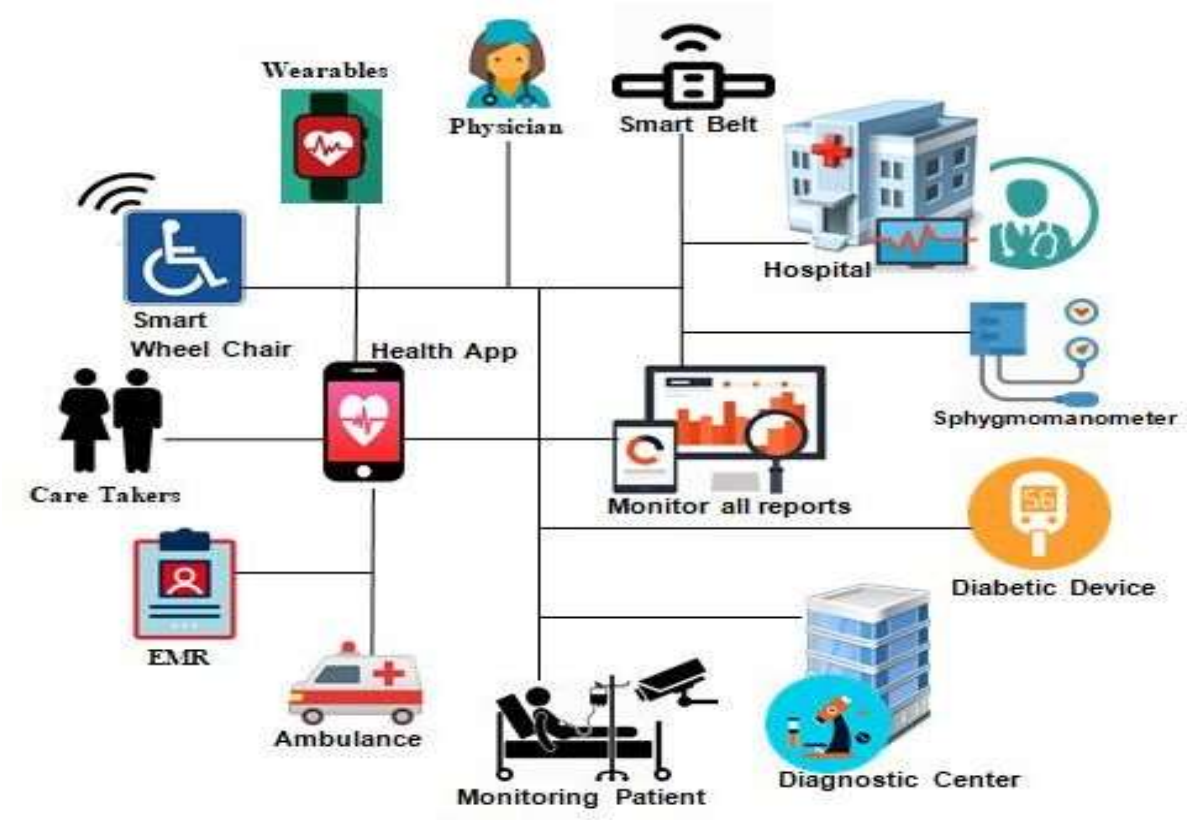

Fig. 1. Internet of Medical Things (IoMT).

II. An Overview of Blockchain Technology

Blockchain is simply a data structure introduced with Bitcoin in 2008 by Satoshi Nakamato [12] which provides unalterable and irremovable transactions by creating a digital ledger. Blockchain is a peer-to-peer technology for distributed data sharing and computing. Blockchain enables the unknown parties to perform different transactions in the network even they don't trust each other. Blockchain is a type of data structure that can track and store information from the enormous number of devices without any centralized cloud.

Blockchain is a tamper-proof digital ledger that maintains the increasing set of data records. There is no centralized approach and no master computer. Public key cryptography is used in this technology to perform transactions among nodes. The transactions are then stored on a shared ledger. The ledger contained the chain of blocks which are cryptographically connected with each other. It is not possible to change or remove blocks of data that are once recorded on the blockchain ledger.

Blockchain users need to solve a puzzle called proof-of-work to add new data to the blockchain. The very first block is called 'Genesis block'. Every N block has hash of the N-1 block Fig. 2. Participants can view the transaction. Viewing the transactions does not mean that everyone can see the actual contact. The actual contact is protected by the private key [13].

The application of blockchain technology goes beyond Bitcoin due to various features [14]. The secure, decentralized and autonomous capabilities of the blockchain make it an ideal solution for IoMT security problems [15]. Blockchain technology has a lot of strengths; few of them are described in Table 1.

A. Proof of work (POW)

The Proof of Work (PoW) [16], a very hard problem computationally and mathematically that makes the blockchain what it is. PoW is a mechanism to determine the chosen peers in the network. It would be not possible to dialog about blockchain without the dialog of PoW. The PoW must be computationally challenging because on the bases of performed work one will get rewards, so it must be difficult. The native objective of the PoW is to evade cyber-attacks. A blockchain network without PoW can be imagined as a user wants to generate DoS attack, he could flood the system with new blocks. This will result in the network congestion and all nodes need to accomplish additional extra work to find a valid block amongst millions of spam blocks. Moreover, the PoW must be an asymmetric task which means easy to verify but hard to resolve. More specifically, a miner must spend much time in solving the hash puzzle, but the other miners in the network can easily and immediately verify the validity of the founded solution.

The hash function is started from consecutive 0 and number of 0's is added according to the difficulty of the puzzle which is then dynamically adjusted by the network. PoW is a type of hash function that can be done by anybody. Any device can solve the hash problem. This characteristic of Pow makes it a standard system [17].

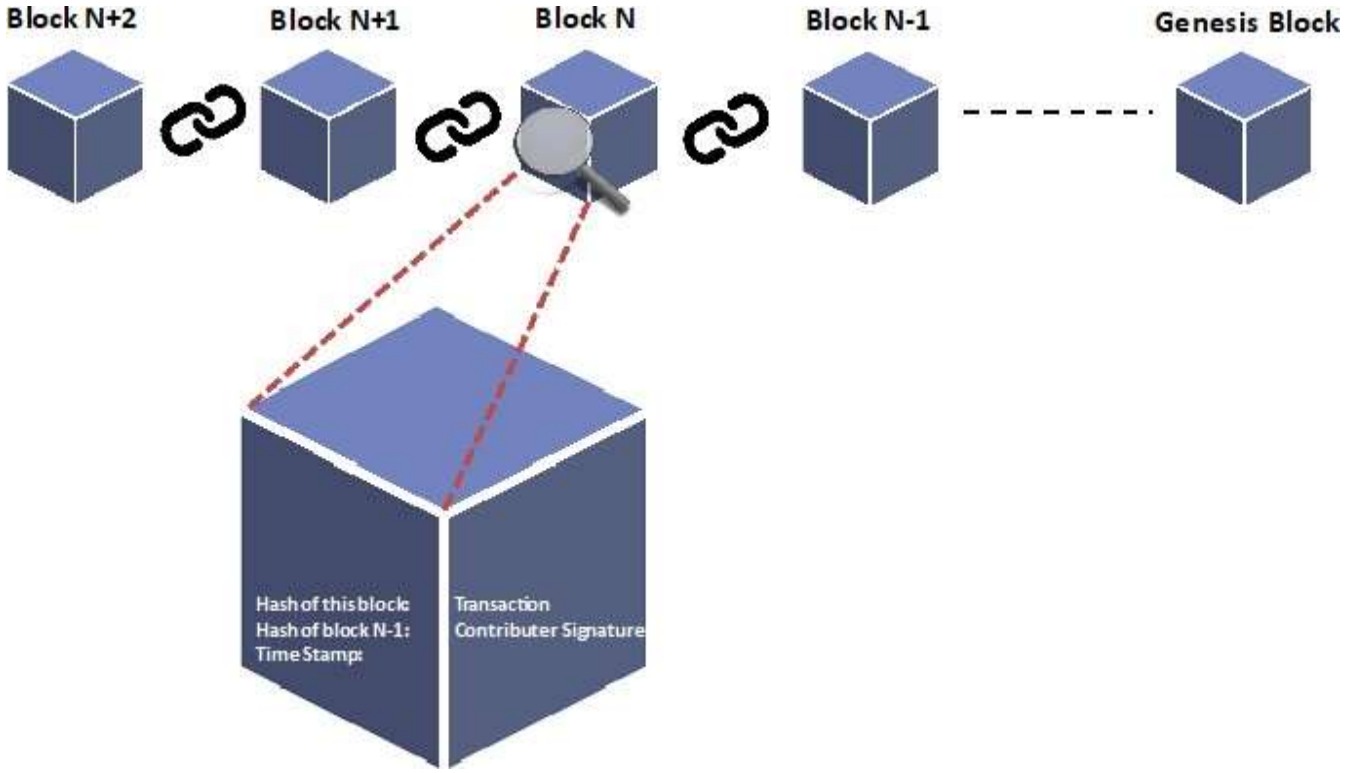

Fig. 2. Blockchain Architecture.

TABLE I. PROPERTIES OF BLOCKCHAIN

Properties	***Description***
Secure and Irrevocable	The blockchain is a tamper-proof digital ledger and no one can alter the records which increases the accuracy of records.
Decentralized Control	A decentralized data structure in which no central data hub and no third party has access.
Auditability and Transparency of Data	A copy of all transactions ever occurred is stored in the blockchain and is visible publicly which increases trust and auditability.
Distributed Information	To avoid having a central authority, every node connected to the network and each node keeps a copy of each record in blockchain.
Peer-to-Peer Transaction	Blockchain allows the parties to have a peer-to-peer connection without any intermediary.
Decentralized Consensus	All nodes of a network confirm the transactions instead of a central node. This breaks the concept of centralized unanimity.

There are other consensus systems such as Proof of Stake (PoS) or Proof of Space (PoSp) in which some nodes are not considered for the mining process because they do not have the basic-needed requirements, whereas in PoW any node can try to solve the problem. Furthermore, PoW makes difficult the addition of new blocks to the chain and the modification of previously added blocks. This means the resilience and safety for the blockchain.

III. RELATED WORK

Many authors have discussed different solutions to secure IoMT. One of the basic solutions to secure IoMT is data encryption. In encryption, they used encryption algorithms to encrypt plain text, the original message into cipher-text. The cipher-text is then transmitted to the receiver on the public channel. The message is then decrypted on the receiver side. There are different mechanisms for data encryption. Due to limited resources and privacy concerns, a light weighted end-to-end key management scheme is introduced by Abdmeziem and Tandjaoui [18] in which keys are exchanged with minimal resource utilization.

From the security point of view, the proposed protocol can provide strong security features as well as the scarcity of resources. Considering the nature of IoT, Gong et al. [19] proposed a solution related to security and privacy protection in current smart healthcare systems. They proposed a prototype system based on lightweight private homomorphism algorithm and an encryption algorithm improved from DES.

Hu et al. [20] introduced a scheme based on cloud computing using IoT sensors which is related to the digital signature, time stamp mechanism and the asymmetric technology to monitor the other personal information. This scheme is very efficient in providing medical services and utilizing less medical resources. Li et al. [21] proposed a secure authentication and the key agreement scheme for a cloud-assisted WBAN system based on Diffie-Hellman key exchange. This scheme can create secure channels or ways for the system participants when they register. Security and performance analysis depicts that the above mention schemes can address the challenges faced in the medical care system.

Another way to secure IoMT is Access Control. In access control data system defines some polices and identity of a user which prevents an unauthorized user to access data. There are various encryption techniques used in access control, including symmetric key encryption (SKE), asymmetric key encryption (AKE) and attribute-based encryption (ABE). The security of cryptography depends on the size and key generation mechanism. Therefore, the life cycle of the security system is directly relying on the keys [22].

Lounis et al. [23] proposed architecture for medical wireless sensor networks based on cloud. They introduced an access control that supports dynamic and complex security policies which depends on cipher text policy attribute-based encryption (CP-ABE). Li et al. [24] introduced a novel patient-centric outline for data access control to personal health records (PHRs) stored in partially trusted servers. To attain fine grained data access control for PHR they used attributed based encryption (ABE) to encrypt PHR files for each patient to provide high degree security for patient records.

Cloud servers are not fully trusted. Medical health records required consistency and integrity, and these could be compromised if data is deleted or corrupted without authorized access. For the security purpose, the rules for data security are typically specified by the user so that the service provider cannot directly access the contact. In addition, the Trusted Third Party (TTP) with a great reputation which provides the unbiased auditing results can be introduced properly to enable the accountability of cloud service providers and to protect the legitimate benefits of cloud users [25]. For data privacy, sensitive data must be encrypted before transmitting which eliminates traditional data utilization based on the plaintext keyword search. Thus, providing an encrypted cloud data search service is of paramount importance [26].

Privacy information refers to sensitive attributes of a patient including illness and income. In the process of data publication, while considering the distribution characteristics of these original data, it is essential to confirm that the individual attributes of the new dataset are properly processed and protects the patient's privacy [11].

IV. Problem Statement

Securing information is the major problem in data transmission between networks. The dependency of IoMT applications and platforms on a centralized cloud is compromising security. Our contribution is to propose a secure technique or mechanism to provide confidentiality, authenticity and integrity of data transmission in IoMT with blockchain technology.

V. Blockchain: An Effective Solution

Traditional cloud is compromising security [27] whereas blockchain is secure and irrevocable tamper-proof digital ledger and no one can alter the records which increases the accuracy of records. Cloud provides centralized data structure; however blockchain is a decentralized data structure in which no central data hub and no third party has access. Blockchain provides the auditability and transparency of distributed data which dominates the cloud in terms of security and privacy. Peer to peer transaction is provided by Blockchain without any intermediary and each node conform the transaction instead of central hub.

VI. Proposed Methodology

Patient related medical history contains personal and sensitive information which attracts people from all sectors of society, including attackers or anyone who wants to retaliate. Such data would be protected and temper proved while transmitting. IoMT devices require gigantic storage infrastructure for real-time processing because of the enormous amount of medical records. Currently, most IoMT institutions store the collected medical data and deploy their application servers in the cloud Fig. 3. As mentioned earlier, the biggest concern in implementing IoMT using the cloud is the data privacy and security. Cloud servers are not fully trusted, and we cannot compromise on it as data could be removed or altered. Devices are sharing critical data with each other and we cannot deny the fact of data leakage.

Blockchain have recently attracted attention of everyone (made popular by the successful Bitcoin) due to many diverse features. A blockchain is a remedy for securing cloud based IoMT [29] [30]. There has been recent interest in providing a secure healthcare and data supervision by utilizing blockchain [28]. A temper-prove distributed ledger (Blockchain) can offer a way to secure the IoMT, by recording the transactions of digital communication.

We proposed architecture as a solution for secure transmission of a patient health reports based on blockchain technology to secure medical data. A decentralized blockchain-based methodology would overcome many of the problems associated with the centralized cloud approach. A blockchain based data structure can be explained as a virtually incorruptible cryptographically connected blocks where critical patient related data can be stored. The blockchain based system is created by connecting computers and all the participants with each other. Fig. 4 describes the blockchain based healthcare system.

The doctor is graphically present in some remote location observing the patient activities and advising the patient through the blockchain based system. The doctor is also analyzing the generated reports in the diagnostic center. The medical precisionist from diagnostic center is uploading the electronic medical reports (EMRs) which are eventually added to the patient's history.

Real time statistical reports are generating in some clinic shared on the distributed ledger and analyzed by the health provider. Patient is also monitored by the practitioner through some wearable tracking devices. Wearable devices sense the changes happened in the patient body and this real time data is sending to the doctor. The doctor then advised the patient according to the condition. Care takers of the patient can also view the patient history. The reports and treatment of the patient is shared on the distributed ledger and viewed by every node of the patient network.

The healthcare providers are monitoring the patient condition by wearables [31]. These devices are embedded with sensors which can observe the patient at any time and can send valuable data over IoMT to the medical practitioners.

Electronic medical reports (EMRs) are basically containing the patient related clinical data which is provided by the patient to the medical practitioner or healthcare provider [32]. These EMRs are confidential and essential to provide the optimum treatment to the patient. Electronic medical reports (EMRs) can be generated by the diagnostic labs. Diagnostic lab assistant can add electronic medical reports (EMRs) to the blockchain as he is a part of IoMT network. When the new patient record is created, a new block of data is initiated in the patient network Fig. 5.

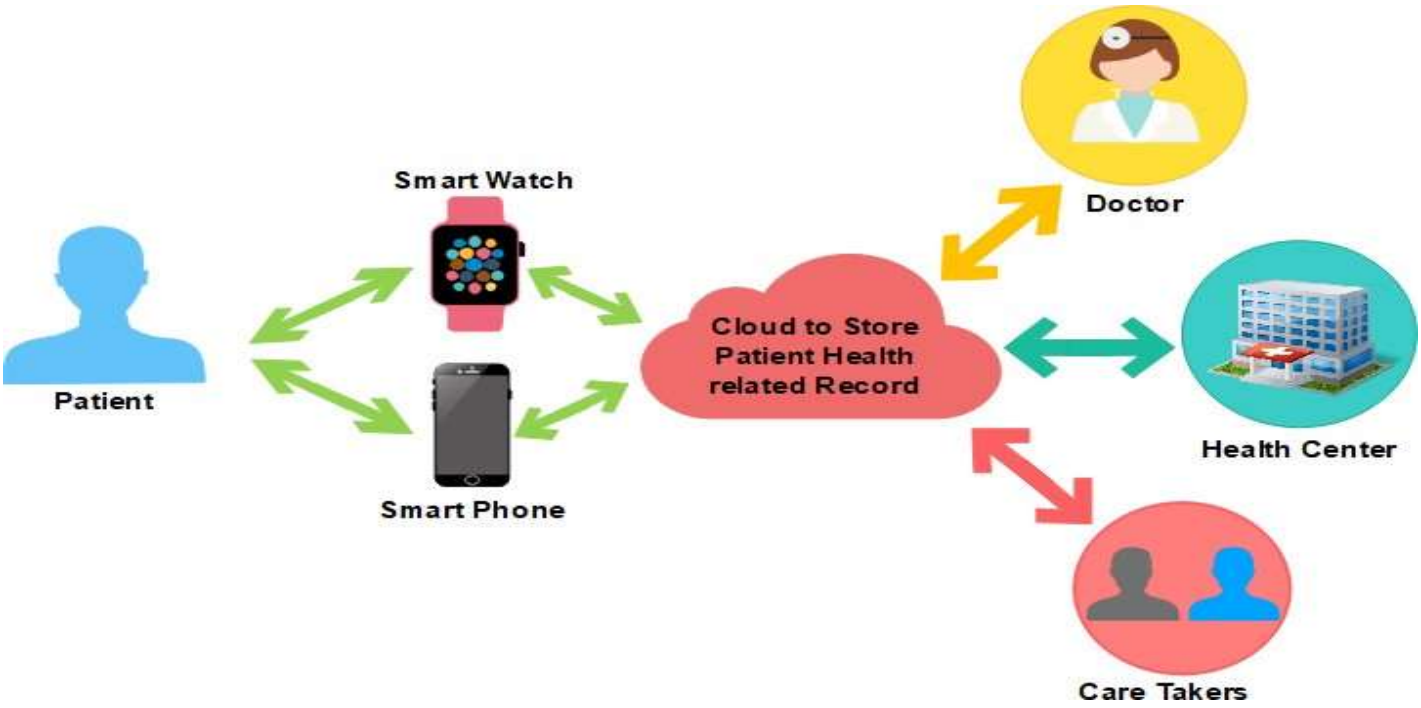

Fig. 3. Cloud based IoMT Architecture.

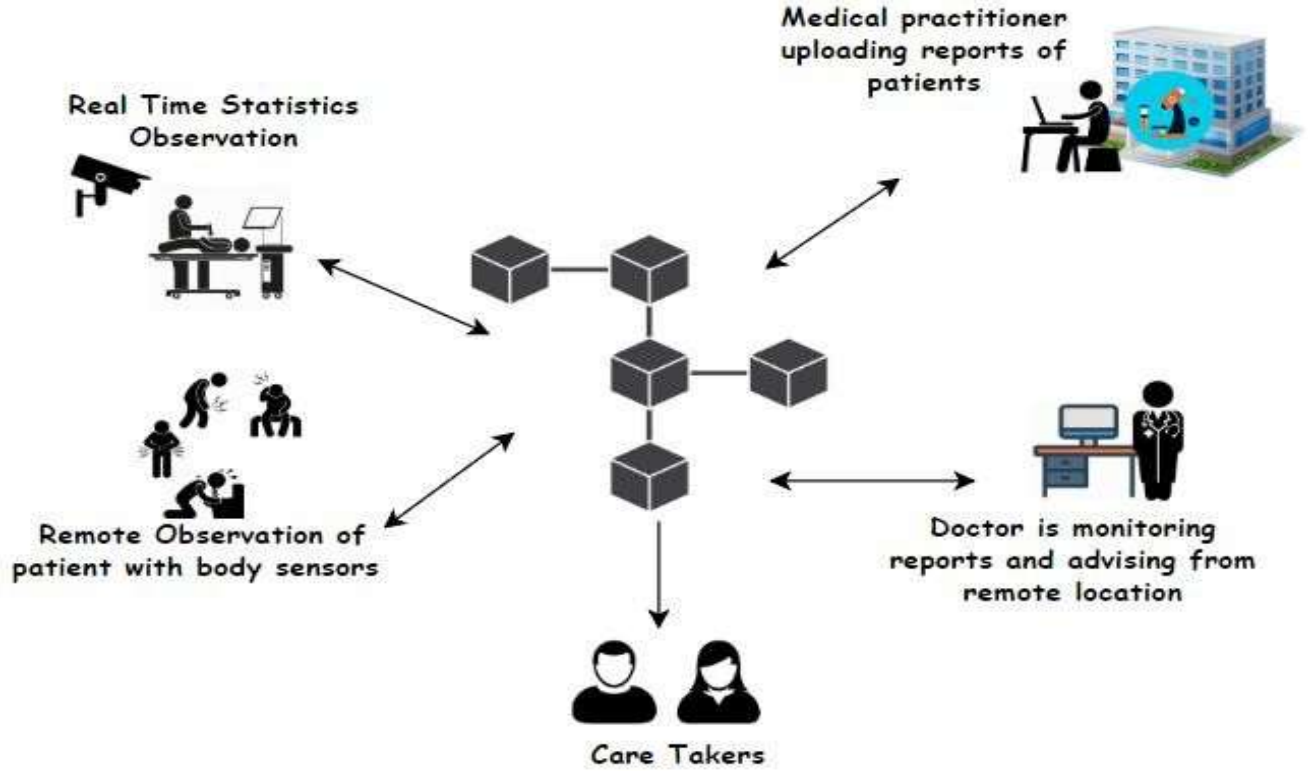

Fig. 4. Blockchain based IoMT Architecture.

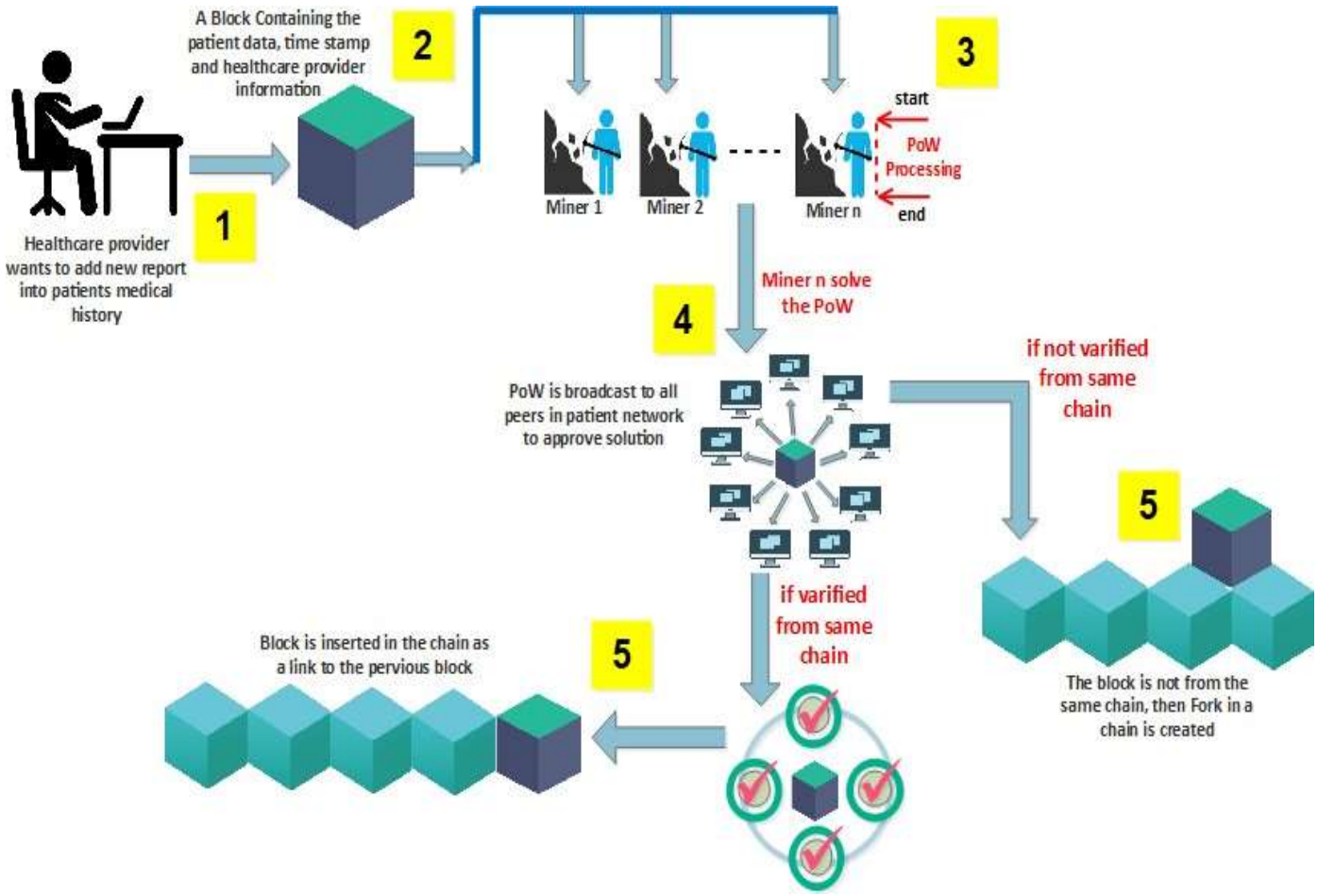

Fig. 5. Adding a Block.

The block contains the patient data, time of creation and the information of the initiator of the block. There are some special nodes called miners. These nodes have to perform some working called mining to add a transaction into the network. The approval of the block is based on the proportion of the mining data.

The first miner who solves the mathematical puzzle will get reward. In case a miner reaches the exact solution, it broadcasts the created block into the network. The block is distributed to all peers in the patient network. When the new block is approved by the majority of the peers, it will be inserted into the chain. If this block will not match with the previous block then a fork is generated in the chain and the block is defined as an orphan in the chain. This means that the new block is not match with the previous one and does not belong to the same chain. Once a data block is added to the chain, it cannot be removed or modified without altering the subsequent block. Simply we can say that the modification can be easily detected if anyone try to change the data. Patients' history can be viewed publically in a very authenticated manner with no fear of any alteration.

We can state that reasonably, blockchain design is secure offering the capacity to accomplish decentralized agreement, consistency and flexibility to expected or unexpected attacks. Key benefits of deploying blockchain are given below:

- Purpose of securing medical records cannot be completed without the involvement of a trusted intermediary avoiding a performance bottleneck and a single point of failure.
- Patients can access, and have control over their data and family members can also view the details of their patient condition.
- Distribution of data is accurate, consistent and timely in blockchain.
- Any change happens in the blockchain can easily be visible by all the members of the patient network.
- Any unauthorized alteration can be detected trivially.

Before adding a block into the chain, we must fetch the patient EMR form data base. The following function is taking file name as an input and returns the required file.

```
1: function Load_File (file )
2:     read fetch(file)
3:     return read
4: end function
```

To attach a block containing patient data or EMR into the blockchain, medical practitioners must connect to blockchain.

The following algorithm is describing that how a block is added into blockchain. The input of the function is the patient name.

```
1: function Attach_block(patient n)
2:    connect  ⟶  blockchain
3:    Identity ⟵  subscribe(identity)
4:    read     ⟵  Load_File(n.EMR)
5:    block    ⟵  create_block(read, timestamp, identity)
6:    result   ⟵  broadcast(block)
7:    if (result are approved)
8:       if (block belongs to the same chain)
9:          add_block_in_Chain()
10:         display (Block is added successfully into the same chain)
11:      else
12:         add_block_in_Fork()
13:         display(Block is added successfully as a fork into the chain)
14:   else
15:      reject_block()
16:      display (Block is rejected)
17: end function
```

A medical practitioner will use the above algorithm to add a block into the blockchain.

The following flowchart illustrates the flow of adding a block into blockchain (Fig. 6).

VII. Limitation and Solution

Blockchain holds the property for storing data without unauthorized modification. However, there are still many obstacles in engaging blockchain in industries. The size of personal healthcare data is a way extensive than the size of the most of public blockchain. One of the major challenges is storing personal healthcare records (PHRs) in the blockchain. The size of the entire blockchain will be tremendous and it is very difficult to manage the huge data which needs to be studied further. Blockchain was originally design to store small data in blocks (Bitcoin). In order to deal with the storage challenges, data would be store in a separate off-chain storage system. Instead of storing the whole data, blockchain only contain hash references for stored data where clinical related data need to be stored off-chain in the traditional database system while immutable hash of the healthcare data are stored on-chain for checking the authenticated access to the off-chain clinical patient records.

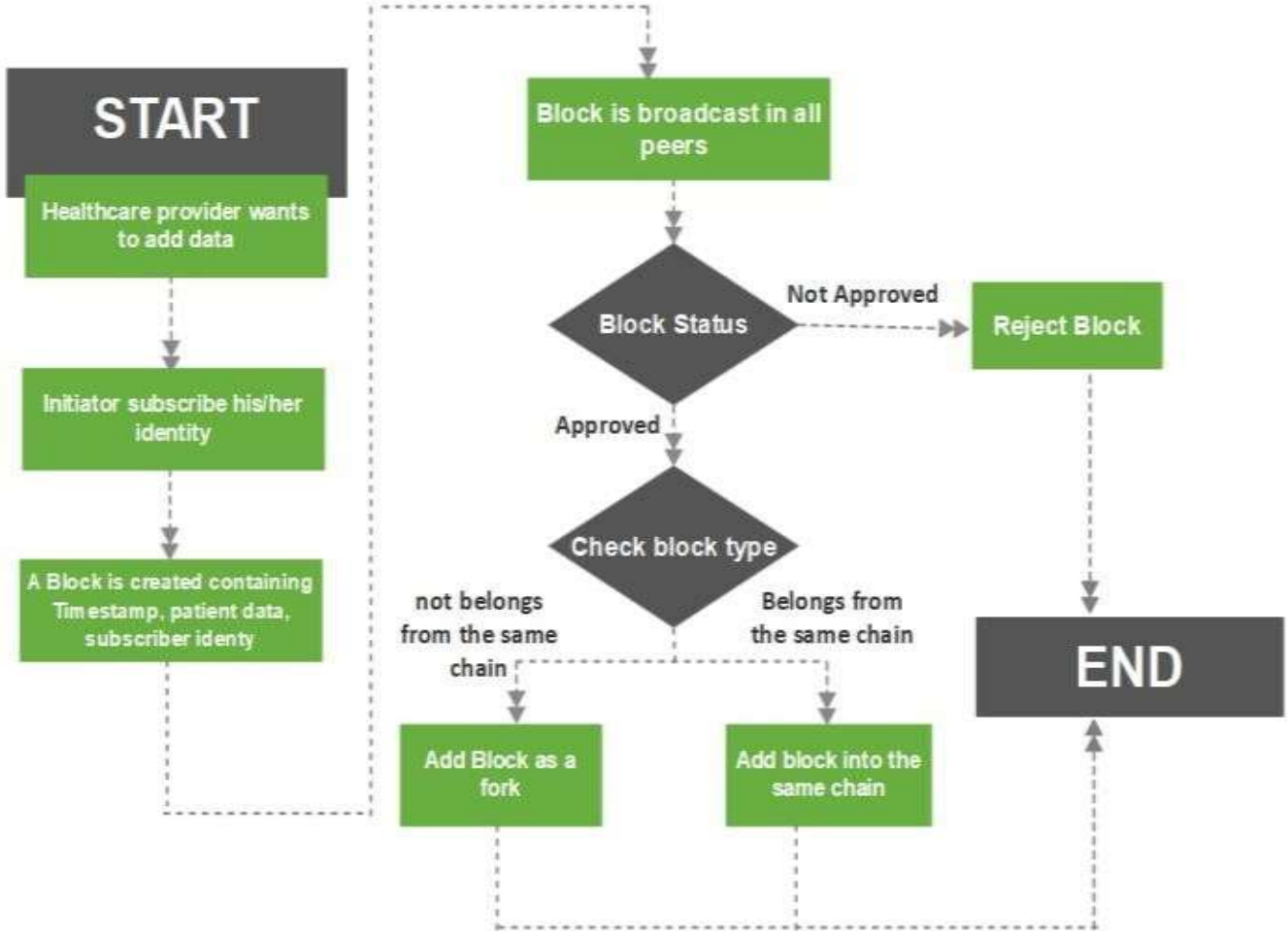

Fig. 6. Flowchart for Adding a Block.

VIII. Conclusion

Internet of Things has revolutionized many segments of the industry. The healthcare industry is one of the fastest to embrace this opportunity by making the internet of medical related things. Due to the expeditious increase and diverse nature, security has become the major issue. Blockchain holds promise for privacy and security in IoMT. Merging blockchain with the Internet of Medical Things has been provided a decentralized way to manage the rapidly increasing number of IoMT devices. Our proposed blockchain based IoMT architecture handles most of the security and privacy threats. The data stored in blockchain cannot modifiable; therefore a verified consensus based digital ledger of data can be generated. Hence, blockchain assures the security of patient clinical history in real time and grants tempered proof open access to every node in the IoMT network. In future work, we will further explore blockchain to resolve the storage problems.

References

[1] Forecast: The Internet of Things, Worldwide, 2013, Gartner, Stamford, CA, USA, Nov. 2013.

[2] WhitePaper: Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2016–2021. San Jose, CA, USA, Mar. 2017.

[3] M. Suárez-Albela, P. Fraga-Lamas, T. M. Fernández-Caramés, A. Dapena, and M. González-López, ''Home automation system based on intelligent transducer enablers'', Sensors, vol. 16, no. 10, no. 1595, pp. 1–26, Sep. 2016.

[4] P.Fraga-Lamas,T.M.Fernández-Caramés,andL.Castedo,''Towardsthe Internet of smart trains: A review on industrial IoT-connected railways'', Sensors, vol. 17, no. 6, no. 1457, pp. 1–44, Jun. 2017.

[5] Cisco: Enterprises Are Leading The Internet of Things Innovation, Aug,2017.

[6] S. J. Barro-Torres, T. M. Fernández-Caramés, H. J. Pérez-Iglesias, and C. J. Escudero, ''Real-time personal protective equipment monitoring system'', Comput. Commun., vol. 36, no. 1, pp. 42–50, 2012.

[7] P. Fraga-Lamas, T. M. Fernández-Caramés, Ó. Blanco-Novoa, and M. A. Vilar-Montesinos, ''A review on industrial augmented reality systems for the industry 4.0 shipyard'', IEEE Access, vol. 6, pp. 13358–13375, 2018.

[8] L. Atzori et al., The Internet of Things: A survey, Comput. Netw. (2010)

[9] F orcast: "Medtech and the Internet of Medical Things", July 2018, Deloitte Centre for Health Solutions

[10] J. J. P. C. Rodrigues, D. B. D. R. Segundo, H. A. Junqueira, M. H. Sabino, R. M. Prince, J. Al-Muhtadi, V. H. C. D. Albuquerque, "Enabling Technologies for the Internet of Health Thing", IEEE Access, Volume 6, 2018.

[11] W. Sun, Z. Cai, Y. Li, F. Lui, S. Fang, G.Wang, "Security and Privacy in the Medical Internet of Things: A Review", Hindaw, Security and Communication Networks, Volume 2018, Article ID 5978636, 9 pages.

[12] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. N.Kshetri. (2017). "Can Blockchain Strengthen the Internet of Thngs". IEEE Computer Society.

[13] M. H. Miraz, M. Ali "Applications of Blockchain Technology beyond Cryptocurrency", Annals of Emerging Technologies in Computing (AETiC) Vol. 2, No. 1, 2018.

[14] H. Halpin, M. Piekarska, "Introduction to Security and Privacy on the Blockchain", European Symposium on Security and Privacy Workshops (EuroS&PW), (2017), IEEE Computer Society.

[15] B. Laurie and R. Clayton, ""Proof-of-Work" Proves Not to Work", May 2004.

[16] M. Hölbl, M. Kompara, A. Kamišali´c, L. N. Zlatolas, "A Systematic Review of the Use of Blockchain in Healthcare", Faculty of Electrical Engineering and Computer Science, University of Maribor, Slovenia, October, 2018.

[17] M. R. Abdmeziem and D. Tandjaoui, "A cooperative end to end key management scheme for e-health applications in the contextofinternetofthings," in Ad-hoc Networks and Wireless, pp.35–46,Springer,BerlinHeidelberg,2014.

[18] T. Gong, H. Huang, P. Li, K. Zhang, and H. Jiang, "A Medical Healthcare System for Privacy Protection Based on IoT," in Proceedings of the 7th International Symposium on Parallel Architectures, Algorithms, and Programming, PAAP'15, pp.217– 222, December 2015.

[19] J.-X.Hu,C.-L.Chen,C.-L.Fan,andK.-H.Wang,"Anintelligent and secure health monitoring scheme using IoT sensor based on cloud computing," Journal of Sensors, vol. 2017, Article ID 3734764,11 pages, 2017.

[20] C.-T. Li, C.-C. Lee, and C.-Y. Weng, "A secure cloud-assisted wireless bodyarea network in mobile emergency medical care system," Journal of Medical Systems, vol.40, no.5, pp.1–15, 2016.

[21] X.Yan, T.Geng, H.Ding, "Efficient Cryptographic Access Control Protocol for Sensitive Data Management", Journal of Computers, vol. 9, no. 1, January 2014.

[22] A. Lounis, A. Hadjidj, A. Bouabdallah, Y. Challal, "Healing on the cloud: secure cloud architecture for medical wireless sensornetworks," Future Generation Computer Systems, vol.55, pp.266–277, 2016.

[23] M. Li, S. Yu, and Y. Zheng, "Scalable and secure sharing of personal health records in cloud computing using attributebased encryption,"

[24] IEEE Transactions on Parallel and Distributed Systems, vol.24, no.1, pp.131–143, 2012.

[25] V.Venkatesh and P.Parthasarathi, "Trusted third party auditing to improve the cloud storage security" Wireless Communication, 2013.

[26] N. Cao, C. Wang, M. Li, K. Ren and W. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," 2011 Proceedings IEEE INFOCOM, Shanghai, 2011, pp. 829-837. doi: 10.1109/INFCOM.2011.5935306.

[27] S. Mathew, S. Gulia, V. Singh, V. Dev, "A Review Paper on Cloud Computing and its Security Concerns", (2017), Intelligent and Computing in Engineering pp. 245–250 ACSIS, Vol. 10 ISSN 2300-5963.

[28] T. Ahram, A. Sargolzaei, S. Sargolzaei, J. Daniels, B. Amaba, "Blockchain Technology Innovations", 2017 IEEE Technology & Engineering Management Conference (TEMSCON).

[29] J. Zhang, N. Xue, and X. Huang, "A Secure System for Pervasive Social Network Based Healthcare," IEEE Access, vol. 4, 2016, pp. 9239–9250.

[30] C, Esposito, A. D. Santis, G. Tortora, H. Chang, K. Kwang, R.Choo, "Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy?" ,2018 IEEE Cloud Computing.

[31] Rasheed, Mohd. Anas. (2017). ,"White Paper: Blockchain for Wearable Devices." 10.13140/RG.2.2.31271.44969.

[32] E. C. Murphy, F. L. Ferris, W. R. O'Donnell, (2007). "An electronic medical records system for clinical research and the EMR EDC interface," Investigative ophthalmology & visual science, 48(10), 4383-9.