





# An End-to-End Secure Solution for IoMT Data Exchange

Saad El Jaouhari<sup>(✉)</sup>  and Nouredine Tamani 

Institut Supérieur d'Electronique de Paris (Isep), Issy-les-Moulineaux, France  
{saad.el-jaouhari,nouredine.tamani}@isep.fr

**Abstract.** In the field of healthcare, the emerging concept of the Internet of Medical Things (IoMT) plays a crucial role in enhancing the efficiency of medical services and introducing innovative solutions. Traditional healthcare services are no longer adequate to meet the growing medical needs, particularly in countries with an aging population. Remote medical consultations have emerged as a viable solution, especially in rural areas facing the challenge of medical deserts. In such scenarios, instead of physically visiting a hospital, patients can opt for remote medical consultations, particularly for simple cases like medical follow-ups. The patient's health data is collected, monitored, and processed in real-time, subsequently shared with remote doctors or hospitals. IoMT devices, which easily measure vital signs, facilitate the seamless collection of health data. However, ensuring the security and privacy of sensitive IoMT data poses a significant challenge. In this context, one potential solution to ensure the confidentiality and integrity of medical data is the utilization of Blockchain technology. This paper explores the potential of Blockchain in IoMT networks, specifically focusing on guaranteeing privacy, confidentiality, integrity, authentication, and non-repudiation of medical data collected through medical IoT devices. Additionally, a proof of concept is provided to demonstrate how Blockchain can be effectively employed to secure the sharing and storage of IoMT data among connected nodes/devices and authorized users, particularly medical entities.

**Keywords:** IoT · IoMT · Blockchain · Healthcare · Security and Privacy · Confidentiality · Integrity · Authentication

## 1 Introduction

Modern medical systems have progressed from traditional electronic medical records, where patient clinical information resides digitally within a single medical center (typically a hospital), to the era of Electronic Health Records (EHR). In EHR systems, patient medical information is distributed across the healthcare system, enabling access and sharing among various entities. This evolution coincides with the integration of an expanding array of Internet of Medical Things (IoMT) devices that collect patient-related medical and environmental

data. IoMT devices serve the primary purpose of furnishing additional medical information to the medical corps, aiming to enhance the assessment of a patient's health condition and potentially improve medical treatment and services. Notably, IoMT devices have proven efficient in remote monitoring and medical follow-ups, eliminating the necessity for the physical presence of the patient. The IoMT market in the United States reached US\$30.56 billion in 2022 and is projected to exceed US\$327.08 billion by 2032, reflecting a compound annual growth rate (CAGR) of 26.80% from 2023 to 2032, according to a report by [1]. However, this technological advancement has introduced complexities, particularly in the management of data, similar to Electronic Health Records (EHR). Ensuring security and privacy in handling this data is paramount due to the unique nature of the healthcare environment, where security threats can have life-threatening consequences for patients, making it more critical than in any other domain.

For highly sensitive data, ensuring properties such as data integrity, confidentiality, authentication, and non-repudiation becomes imperative. However, in distributed environments, and considering the constraints associated with IoT, maintaining these properties becomes challenging. Specifically, for IoMT data, we must: 1) Ensure that only authorized entities and devices can interact with the medical system, ensuring confidentiality. 2) Guarantee that collected medical data remains unaltered, both accidentally and intentionally, preserving integrity. 3) Ensure the traceability and authentication of data, addressing both authentication and non-repudiation concerns.”

In order to solve some of these issues, the Blockchain emerged as a disruptive solution to add a security and privacy layer to the IoMT environment. Blockchain is proven to be a tamper-proof digital ledger that enables secure peer-to-peer exchange of data. It enables data exchange even between unreliable endpoints without a third party. In this paper, we discuss the potential of Blockchain, and in particular the private ones, in IoMT networks and propose a solution to guarantee the privacy, confidentiality, and integrity of medical data collected through medical IoT devices. The solution uses the Hyperledger Fabric (HLF) developed by IBM [9] as a core in order to build a private blockchain. The latter is used to manage our IoMT data between the different entities involved in the process. In this case, only the authorized and registered peers (hospitals for instance) can check and read the data from the private ledger.

The rest of the paper is organized as follows: Sect. 2 provides a summary of related works. In Sect. 3, we present our proposed architecture, including a discussion of use cases. Section 4 provides details about the implementation of our proposal as a proof of concept, and the various interactions among the components of our system. The paper concludes in Sect. 5, where we also draw some lines for future work.

## 2 Related Work

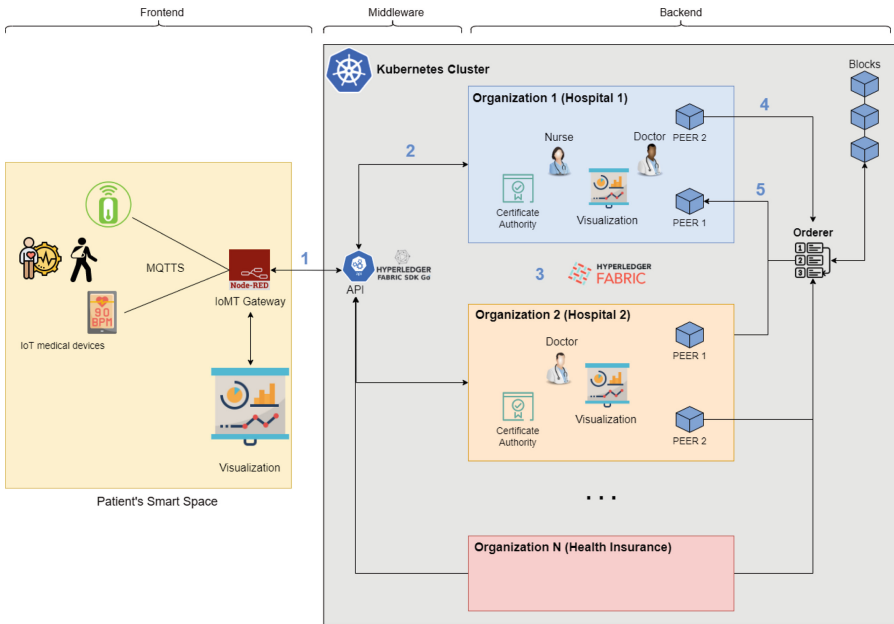
In [13] and in [14], the authors designed a Blockchain architecture, based on the Hyperledger Fabric, to secure IoT-based health monitoring systems. The proposed architecture consists of two Blockchain networks: a) a Local one that is a single-node Blockchain embedded in the Perception Domain (i.e., IoT edge network), and b) a Global one that connects each Perception Domain to a Blockchain. The authors in [12] used the IoT and Blockchain to improve drug traceability in the pharmaceutical supply chain. The solution relies on the distributed ledger (DLT) to keep an immutable record of all transaction data. In [2], and for mesh-based IoT networks, the authors introduced DAGSec, a secure version of directed acyclic graphs (DAG), for IoT environments with high throughput and low latency. They used directed acyclic graphs and local transaction validation instead of global transaction validation to attain a high transaction rate. Also, they developed a Blockchain-based witness system to approximate the chronological order of independent transactions. In [10], the authors developed a novel decentralized Blockchain-based IoMT framework named Electronic Medical Record Infrastructure (EMRI), where all the clinical reports and IoT data are added. EMRI is an immutable and secure platform for the transaction of healthcare data. However, it is still to be implemented in a healthcare organization. In [3], the authors presented a solution for a collaborative healthcare management system, surgical process management, using IoT and Blockchain integration architecture, ERTCA, which relies on Ethereum. They also solve the issues related to constrained IoT resources when adopting the Blockchain mining process by using a rich-thin IoT client categorization approach. In [5], the authors proposed a model based on Blockchain for the remote patient monitoring scenario, where the patient is equipped with wearable IoT devices. Their model consists of five key parts: a Blockchain Network using Proof of Authority (PoA), Cloud Storage, Healthcare Providers, Smart Contracts, and Patients equipped with healthcare wearable IoT devices. Moreover, in [4], the authors developed a platform for combining IoT-based smart healthcare systems and Blockchain. The proposed system is based on HLF and it consists of five components: an IoT gateway devices, HTTP-based API gateway as device-to-Blockchain interface, membership service provider (MSP), peers, and orderers. Finally, the authors in [15] introduced a permissioned Blockchain-based architecture, built in HLF, to manage access control to medical data and to preserve patient data privacy. The data are collected via an IoT Fog Gateway connected to wearable health devices. The ledgers and transactions are stored in the cloud. The proposed architecture is designed for remote patient monitoring.

However, compared to our solution, most of these works do not take into account contextual IoT data along with users' immediate environment of in order to enhance medical services such as teleconsultation, remote monitoring, or medical follow-up. Moreover, most of them do not take into account the security inside their perception layer (i.e., between the sensors and the gateway) before even sending the data to the blockchain, which can be exploited by an adversary to meddle with such sensitive data. Finally, we propose to use a permissioned

Blockchain, which allows only selected and verified participants to interact with the Blockchain, which we believe is more suitable in the medical domain to protect data confidentiality and integrity, and hence the privacy of the patients.

### 3 Permissioned Blockchain for IoMT Medical Data

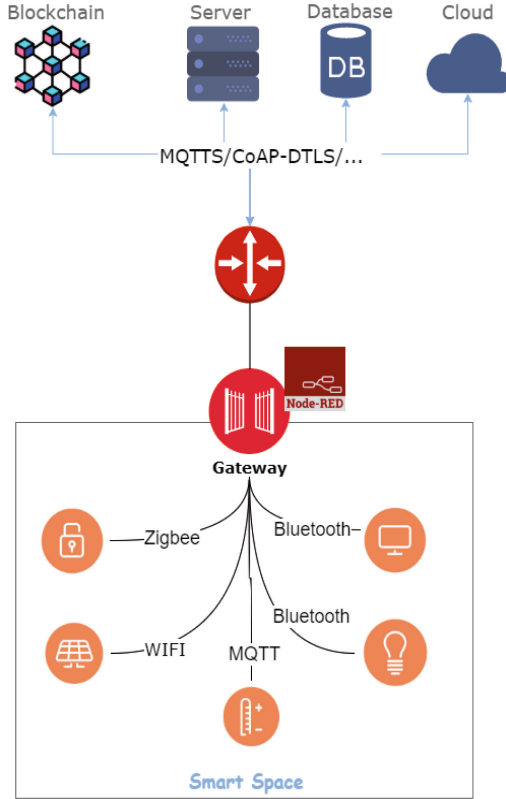
In this paper, a solution based on Hyperledger Fabric (HLF) Blockchain [9], a private and permissioned blockchain, is developed to secure sensitive incoming data from an IoMT sensors network. To do so, Node-RED [7] is used to manage and interact with the different IoMT devices possessed by the patient to collect health data. The data are then sent to the permission Blockchain. Moreover, a User Interface (UI) is also provided to view the history of transactions committed to the ledger. The Blockchain secures the IoMT data with an identity Membership Service Provider (MSP) encapsulated in an X.509 digital certificate and data encryption. The transactions are available and verifiable in the immutable Blockchain ledger ensuring privacy, confidentiality, and integrity to secure the IoMT data. Figure 1 illustrates the functional architecture of the introduced solution along with its main components.



**Fig. 1.** Blockchain-based architecture for securing IoT health data from the patient’s smart space

In what follows, we first present what is a patient’s smart space. Then, we illustrate our solution with some use cases and we explain in detail the interaction

between the main components. Next, we introduce the HLF chaincode lifecycle together with how Node-RED interacts with the ledger. Finally, we focus on the dashboard representing the Visualization part.



**Fig. 2.** Definition of a patient's smart space

### 3.1 Patient's Smart Space

The medical IoT devices are located in the immediate environment of the patient, or in what is called the patient's smart space, as shown in Fig. 2. The goal is to use such medical data, which is considered contextual data, to assist/help the remote medical entity in making decisions.

In this context, a Smart Space (SS) [6] is defined as a user-centric set of heterogeneous Smart Objects (SO)s (i.e., medical IoT devices) communicating using different communication protocols, such as BLE, WIFI, Zigbee, MQTT and so on, and which are accessible through a gateway, in our case via Node-RED, which acts as a manager of all these SOs and an aggregator to all of their

data. The latter will be responsible for exchanging and securing the data with the Blockchain, as it will be explained later. For instance, the smart home of a patient can be considered a smart space.

### 3.2 Use Cases

Several use cases can be identified in the field of healthcare where Blockchain can be a great asset to improve efficiency, availability, and trust within an IoMT-based environment [8, 11]. Relevant use cases for our approach can be tele-consultation and remote medical monitoring of the elderly, as shown in Fig. 3.

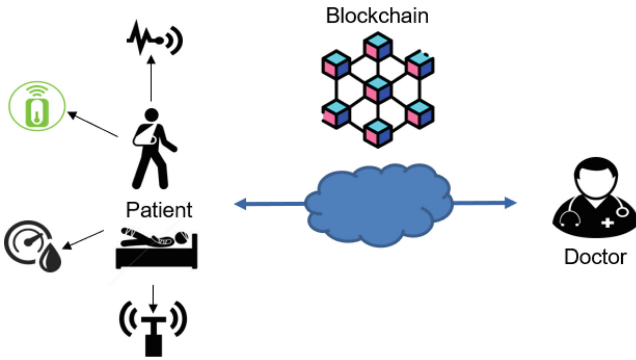


Fig. 3. Tele-consultation and remote monitoring use cases

The use cases can be implemented as distributed autonomous application based on Blockchain. The different identified actors are as follows:

- **Patients** with all their sensors that create and write new data into the Blockchain.
- **Doctors** who consume data and create new data as diagnoses and prescriptions.
- **Pharmacists** who consume data and execute contracts delivering the medication to the patients.
- **Health insurers** who consume data and execute contracts related to health expenses (related to doctors, hospitals, etc.).
- **Hospital emergency** where nurses and doctors can have access to the historical data of a given patient and can also generate data.
- **Nurses** who need to have access to data in case of ambulatory health service.
- **Researchers** who need to have access to the historical data for research purposes

Sensors perform measurements and save the data into the blockchain. The doctor analyses the data, makes a diagnosis, and creates the prescription. The prescription is accessible to the pharmacist and to the health insurers. The pharmacist

serves the patient and validates the prescription and the insurer processes the prescription for the check out. When sensors generate alarming data, a contract can be executed: call the emergency services, call a nurse, schedule an appointment, etc. All these services generate transactions for payments such as a transaction refers to executing a contract. For privacy concerns, the contract can include clauses for the pharmacists who need only to know the prescription content and basic patient information (Social Security Number), and for the insurers who need only to know the client identifier, and the amount of money to pay to a given doctor or hospital.

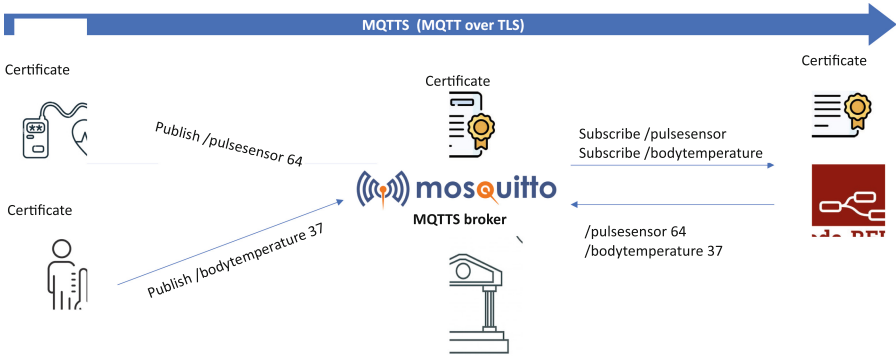


Fig. 4. IoMT devices - gateway communication using MQTTS

## 4 Implementation of a Proof of Concept

The initial step involves establishing an environment conducive to deploy and implement our solution. To do so, we have used an HPC with a CPU 12th generation intel® core(tm) i9-12900k, 32 GB RAM and a GPU Nvidia GP102 Titan XP. As for the software, the Hyperledger Fabric (HLF), an open source enterprise-grade permissioned distributed ledger technology (DLT) platform, Node-RED, Docker, and Kubernetes were deployed.

### 4.1 Component Interactions

Before delving into details, we first outline the three types of peers offered by HLF. Each peer is a docker container that is managed by Kubernetes in the Cloud as shown in Fig. 5.

- Endorser peers: with installed chaincode, simulate transaction execution in isolated containers upon receiving a proposal. Using this simulation, they generate a transaction proposal sent to the orderer peer, avoiding the need for sequential transaction execution by all peers.

- Orderer peers: they receive endorsed transactions and organize them into blocks. After grouping transactions, orderers ensure consensus by distributing these blocks to Endorsing peers, where validation occurs before committing the transactions to the shared ledger. Orderer peers maintain records of both valid and invalid transactions, while other peers only store valid transactions.
- Anchor peers: they act as intermediaries between peers within their organization and those belonging to an external one. For instance, an anchor peer is used when a legitimate peer from one organization needs to communicate with a given peer in another organization.

Name	Namespace	Images	Labels	Pods
node-red	default	Show all	Show all	1 / 1
rest-api	default	Show all	Show all	1 / 1
org2peer2	default	Show all	Show all	1 / 1
org3peer1	default	Show all	Show all	1 / 1
org1peer2	default	Show all	Show all	1 / 1
org1peer1	default	Show all	Show all	1 / 1
caorg1	default	Show all	Show all	1 / 1
orderer	default	Show all	Show all	1 / 1

**Fig. 5.** Kubernetes Dashboard (Cloud)

Next, the main interactions between the different components of Fig. 1 are as follows.

1. First, Node-RED is used as a gateway to collect medical data from the patient’s smart space using the lightweight MQTT protocol, as shown in Fig. 4. Moreover, to enhance security, MQTT over TLS (MQTTTS) has been used in order to guarantee end-to-end security from the IoT device to Node-RED. It relies on certificates issued by a Certification Authority (CA) to both encrypt the data and guarantee the identity of the communicating parties, hence, guaranteeing the confidentiality, integrity (by using SHA-256 as a hash function), authentication, and non-repudiation in this part of the architecture. The Node-RED, which represents the front end in this case, interacts directly with the Hyperledger Fabric Client SDK APIs.
2. In order to invoke the chaincode (i.e. read, update, and write data to the blockchain), nodes inside the Node-RED are configured to perform HTTPS requests and return the response to the APIs defined by the Hyperledger Fabric Client SDK. The chaincode invocation/lifecycle is explained below.



3. The APIs in HLF Client SDK can directly interact with the chaincode inside the HLF Network (composed of multiple health organizations contributing to the ledger) and can also update and read from the ledger.
4. Endorser Peer “**PEER 2**” executes the functions that are defined in the chaincode in accordance with the request received from the API and then sends the results to the Ordering Service.
5. The Ordering Service (or **Orderer**) creates the corresponding blocks and sends them to “**PEER 1**”, representing the Anchor Peers, which will then broadcast the blocks to the Endorser Peers. Anchor peers are only configured to broadcast blocks for our application. Such functionalities provide a private environment for different use cases and applications using private Blockchain.
6. Finally, the Endorser Peers broadcast the message to the API defined by the Hyperledger Fabric SDK and the response can be verified by a debugger on Node-RED.

The transaction history of IoMT data can be verified by checking the history of data coming from the Ledger where it is stored securely and immutably in the Blockchain. Moreover, the data received by the blockchain from the IoMT sensor is encrypted (using the AES256 algorithm) and then packaged onto the chaincode. The chaincode is invoked and data is processed through the ledger. Each input data from the sensor is packed into blocks of immutable datasets. This packaging of data into blocks is performed when the HTTPS request initiates the chaincode lifecycle and invokes the chaincode in the blockchain to commit key-value pairs to the ledger.

## 4.2 Hyperledger Fabric Chaincode Lifecycle

The HLF chaincode lifecycle is a sequence of actions performed by organizations to agree on the parameters that define a chaincode (such as name, version, endorsement policy, etc.) and deploy the chaincode to a channel for collaborative use. Channel members come to an agreement via the steps below:

1. Package a chaincode: Every organization (e.g., healthcare organizations such as hospitals in our use case) that wants to call chaincode functions obtains the source code of a chaincode and packages it into an appropriate format.
2. Install the chaincode package: The chaincode should be installed on every organization’s peer that is supposed to execute or endorse chaincode transactions.
3. Approve a chaincode definition: Every organization that is going to use the chaincode composes and submits a chaincode definition—a set of configuration parameters considered to be acceptable by an organization.
4. Commit the chaincode definition to a channel: Once a required number of channel participants have approved the same chaincode definition, this definition can be then committed to a channel. The commit transaction is performed once and can be triggered by any organization.

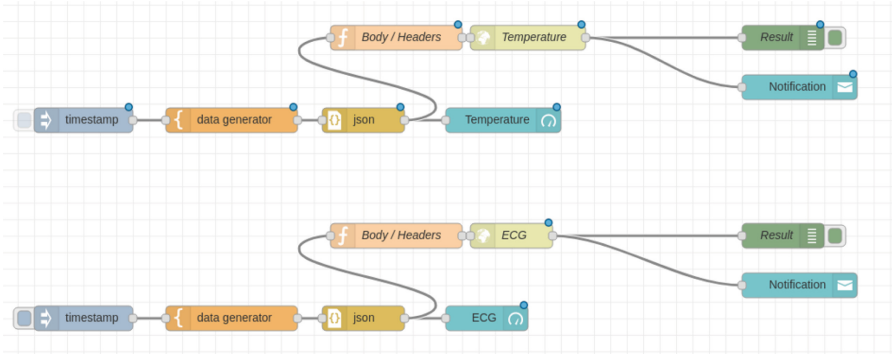


Fig. 6. IoMT sensors network simulated using Node-RED

### 4.3 Node-RED Interactions with the Ledger

Figure 6 provides views from the IoMT nodes simulated using Node-RED. The real sensors were replaced by simulated sensors in Node-RED for simplicity's sake. In our testbed, the medical sensors (blood pressure sensor, pulse sensor, oxygen level sensor, and temperature sensor) were connected to an MQTT broker, and the generated data is then published in the “MQTT subscribe (input)” node, as shown previously in Fig. 4.

### 4.4 Visualization

Following the implementation of previous interactions in HLF with medical data from simulated IoMT sensors using Node-RED, Fig. 7 illustrates the digital representation of the value generated by the IoMT pulse sensor.

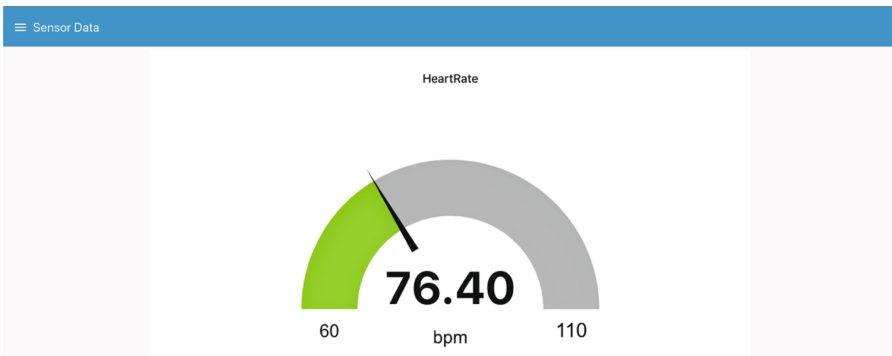


Fig. 7. IoMT data fetching and visualization

Transaction ID	Sensor ID	Timestamp	Value
44a6629503bc824d296b48461777287196932a92ab0f83e707644a2a571	sensor1	09/23/2021, 1:37:36 AM	
9930c0381c4b2f758f3f62d9fbee9752a840118b71ba089c20507b187dc212	sensor1	09/23/2021, 1:37:44 AM	
4efcc2e72424c48a83b6915b0e7471dd51f5330353a189092e46805ad6bc7063	sensor1	09/23/2021, 1:41:26 AM	24.33
0dce216cc15c51f7a43a2acea35221c86396d9c69fba54efbe58493a894646	sensor1	09/23/2021, 2:19:47 AM	-3.80
6811b721766d321c787b438739c92bc750c0194ef06317a486d7cd715aaafe	sensor1	09/23/2021, 6:06:02 PM	18.50
cb767dfcb3b324ec38c78b2ae9ee64c20fb88ec746641fe3c8238b75c7c95e95	sensor1	09/23/2021, 6:06:56 PM	27.53
fec2e17704da619f7aae337bd391d893a8e22de2daae47156ec290ac0d09d4f	sensor1	09/24/2021, 3:01:50 PM	24.79
c474233096eeef746f2ed31042ebb3d39ea0fca3bcea56f0a5ad06031f155ef	sensor1	09/24/2021, 3:06:07 PM	-3.85
4742f0b174e9a37e85668a8791d2a4ea6c304ed9d35e20e442216a9ccca956	sensor1	10/06/2021, 10:58:23 PM	34.19
b73475643f0403f902020f1d5303448df75795794ae56e71b4ad89d2da2	sensor1	10/06/2021, 10:59:53 PM	13.05
54298e1e14b59e6638c2d936ec0a157b62fe55bf114e66252ce8f09cd62e	sensor1	10/06/2021, 11:00:47 PM	61.19
9be785f5d191ef6cd39c7fd1bc71f0e3cb89256469dacaebb1dae48699c6db	sensor1	10/06/2021, 11:01:24 PM	77.10
dc50f29e0b0b5b39934b73043886b19bb9af12b6ad999aba182592cc091063	sensor1	10/06/2021, 11:01:57 PM	87.95
e865fabf283b361b99f0fb6d2dca18703359a8d59e01e87ebaba16acd3b6e3	sensor1	10/06/2021, 11:04:38 PM	62.15
38c461d769491a332e93938771aa556d11c7b1c231f4f691c1347bc040570f	sensor1	10/06/2021, 11:05:18 PM	95.93
44655c8f63b7d09b95e6ea7ec3779fe28be3281e132aaeb4b0b024b39412b5a	sensor1	10/06/2021, 11:07:02 PM	86.01
d29d9152658d83c04457a3ef93254f6d5eed9f3e3587117aa66d5396fe194e	sensor1	10/07/2021, 12:00:30 AM	70.97
2502d5e44ce37c8d8d2253a888ef9a529f31d840e30ab7c42de88c3d074a23	sensor1	10/07/2021, 12:00:48 AM	67.23
0c16711cd1219a668d342c85c50134b3b271b30acc66d8b243af4ba80dc2b3d	sensor1	10/07/2021, 12:01:19 AM	76.40

Fig. 8. Sensors data transaction history table

Moreover, Fig. 8 shows the history of the ledger, which contains transaction Identities (T×Id), Sensor number, timestamp data, and the value of the data generated by the sensor and fetched from the Hyperledger Fabric API. For instance, in the last transaction details, we can confirm that it is identical to the sensor data generated in Fig. 7. The history is fetched from the Ledger where the data is stored immutably in the Blockchain.

## 5 Conclusion

In this paper, a permissioned Blockchain solution based on HLF is used to enhance the security and privacy of the IoMT environment. In this environment, the involved parties are well-known and trusted since X.509 certificates are used to identify each stakeholder. The solution encrypts IoMT data to ensure its privacy and integrity. Moreover, the IoMT data stored in the Blockchain is tamper-proof and cannot be modified. Furthermore, transaction hashes and the history of the ledger are verifiable, ensuring, hence, accountability and traceability of the IoMT data. A proof-of-concept using Node-RED, HLF, and IoMT sensors, has also been developed and showed the successful configuration and the real-time deployment of our solution. In future work, we plan to extend our approach to execute smart contracts among the stakeholders involved in health-care ecosystems, including insurers, practitioners, nurses, pharmacists, etc. to implement a secure end-to-end distributed application. Furthermore, we plan to conduct extensive experiments to validate and assess the performance of our approach.

## References

1. Internet of medical things market (2023). <https://www.precedenceresearch.com/internet-of-medical-things-market>
2. Alvarenga, I.D., Camilo, G.F., De Souza, L.A.C., Duarte, O.C.M.B.: Dagsec: a hybrid distributed ledger architecture for the secure management of the internet of things. In: 2021 IEEE International Conference on Blockchain (Blockchain), pp. 266–271 (2021). <https://doi.org/10.1109/Blockchain53845.2021.00043>
3. Bataineh, M.R., Mardini, W., Khamayseh, Y.M., Yassein, M.M.B.: Novel and secure blockchain framework for health applications in IoT. *IEEE Access* **10**, 14914–14926 (2022). <https://doi.org/10.1109/ACCESS.2022.3147795>
4. Bhawiyuga, A., Wardhana, A., Amron, K., Kirana, A.P.: Platform for integrating internet of things based smart healthcare system and blockchain network. In: 2019 6th NAFOSTED Conference on Information and Computer Science (NICS), pp. 55–60 (2019). <https://doi.org/10.1109/NICS48868.2019.9023797>
5. Dwivedi, A.D., Malina, L., Dzurenda, P., Srivastava, G.: Optimized blockchain model for internet of things based healthcare applications. In: 2019 42nd International Conference on Telecommunications and Signal Processing (TSP), pp. 135–139 (2019). <https://doi.org/10.1109/TSP.2019.8769060>
6. El Jaouhari, S., Bouabdallah, A., Corici, A.A.: SDN-based security management of multiple wot smart spaces. *J. Ambient. Intell. Humaniz. Comput.* **12**, 9081–9096 (2021)
7. Foundation, O.: Node-red - low-code programming for event-driven applications. <https://nodered.org/>. Accessed 13 Sept 2022
8. Haleem, A., Javaid, M., Singh, R.P., Suman, R., Rab, S.: Blockchain technology applications in healthcare: an overview. *Int. J. Intell. Netw.* **2**, 130–139 (2021). <https://doi.org/10.1016/j.ijin.2021.09.005>. <https://www.sciencedirect.com/science/article/pii/S266660302100021X>
9. IBM: Getting started with iot blockchain service (2021). <https://www.ibm.com/docs/en/wip-bs?topic=SSCG66/iot-blockchain/developing/generic.connect.html>. Accessed 13 Sept 2022
10. Mallick, S.R., Sharma, S.: EMRI: a scalable and secure blockchain-based iomt framework for healthcare data transaction. In: 2021 19th OITS International Conference on Information Technology (OCIT), pp. 261–266 (2021). <https://doi.org/10.1109/OCIT53463.2021.00060>
11. Mamun, Q.: Blockchain technology in the future of healthcare. *Smart Health* **23**, 100223 (2022). <https://doi.org/10.1016/j.smhl.2021.100223>. <https://www.sciencedirect.com/science/article/pii/S2352648321000453>
12. Nawale, S.D., Konapure, R.R.: Blockchain & iot based drugs traceability for pharma industry. In: 2021 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC), pp. 1–4 (2021). <https://doi.org/10.1109/ICE/ITMC52061.2021.9570251>
13. Oikonomou, F.P., Mantas, G., Cox, P., Bashashi, F., Gil-Castiñeira, F., Gonzalez, J.: A blockchain-based architecture for secure iot-based health monitoring systems. In: 2021 IEEE 26th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), pp. 1–6 (2021). <https://doi.org/10.1109/CAMAD52502.2021.9617803>
14. Oikonomou, F.P., Ribeiro, J., Mantas, G., Bastos, J.M.C., Rodriguez, J.: A hyperledger fabric-based blockchain architecture to secure iot-based health monitoring

- systems. In: 2021 IEEE International Mediterranean Conference on Communications and Networking (MeditCom), pp. 186–190 (2021).<https://doi.org/10.1109/MeditCom49071.2021.9647521>
15. Zaabar, B., Cheikhrouhou, O., Ammi, M., Awad, A.I., Abid, M.: Secure and privacy-aware blockchain-based remote patient monitoring system for internet of healthcare things. In: 2021 17th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), pp. 200–205 (2021).<https://doi.org/10.1109/WiMob52687.2021.9606362>