A Secure Healthcare System for Privacy-Preserving based on Blockchain Technology

Mohammed Adnan Mohammed
Computer & Embedded Systems. ENIS
University of Sfax
Sfax. Tunisia
Email: mohammed.adnan@enis.tn

Manel Boujelben
Computer & Embedded Systems. ENIS
University of Sfax
Sfax. Tunisia
Email: manel.boujelben@enetcom.usf.tn

Mohamed Abid
Computer & Embedded Systems. ENIS
University of Sfax
Sfax. Tunisia
Email: mohamed.abid_ces@yahoo.fr

Abstract- In recent years, Internet of Things (IoT) technology is recognized as a technological revolution used in different sectors, especially those with the emerged automation concept. It has many applications in various fields, for instance, smart cities, retail, healthcare, etc. However, many issues are yet to be fully addressed, such as scalability, connectivity, privacy and security. Blockchain technology has emerged as a promising solution for privacy and security challenges. It uses a decentralized distributed ledger, which records digital assets' information and keeps these records immutable and then reduces fraud risk. This paper proposes a Blockchain-based medical data protection system that enables users to control over their sensitive data collected from wearable sensors. Patients can upload medical records and healthcare providers can retrieve data while preserving sensitive health information against potential threats. We present a prototype implementation based on Quorum Blockchain and evaluate its memory and CPU time overheads using quorum profiling tool. The empirical results show that the integration of Blockchain technology with existing IoT systems is feasible and provides effective performance and security.

Keywords: Blockchain; Healthcare; IoT; Quorum

I. INTRODUCTION

Nowadays, the Internet of Things (IoT) technologies can provide solutions to sense, actuate with, and communicate over the Internet. The IoT plays a central role in turning current cities into smart cities, electrical grids into smart grids, etc. Furthermore, it visualizes a connected world, where things can communicate measured data and interact, making a digital representation of the real world through many smart applications [1]. Blockchain technology was utilized initially for protecting financial transactions, but when proving its effectiveness, it was used in other fields like transportation, supply chain, healthcare and energy [2]. Blockchain is identified as the key to solve scalability, privacy, and reliability problems related to the IoT paradigm. It can enrich the IoT by providing a trusted sharing service, where information is reliable and can be traceable. Data sources can be identified at any time and data remains immutable over time, increasing its security.

Electronic Health Records (EHRs) have been used as an effective method to store and manage medical data. Currently, EHRs are stored using the client/server architecture by which each hospital retains the stewardship of the patients' data.

Smart healthcare is a part of IoT systems. It facilitates the diagnosis of the diseases and remote monitoring for the patients' vital activities. As a result, these systems deliver faster responses and active treatment to save patients' lives with less effort and cost. As the data of these systems are very sensitive this leads us to many questions such as what are the challenges that face the fonctionning of smart healthcare systems, are these systems safe, how can they protect data from security threats, what are the effects of lack of security and privacy on the work of these systems and what are the most effective ways or technologies to protect data and overcome on these challenges.

Smart healthcare applications have many challenges, such as integration, data overload, accuracy, and cost. Briefly, the most important challenge which is discussed in this paper is data security and privacy. Data of these systems consists of information of patients and hospitals, and other stakeholders that participate in these systems. therefore it is sensitive and vulnerable to various security risks such as eavesdropping, hijacking, denial of service, and tampering. Thereby, these systems cannot be used safely by the health organizations and insurance companies.

Here the need emerged for methods or techniques to solve security challenges and protect data. Recently, there is an increasing trend in deploying Blockchain in the healthcare sector (e.g., public healthcare management, counterfeit drug prevention, and clinical trial). Therefore, this paper proposes to integrate Blockchain technology with EHR systems to protect data and make these systems safer and effective.

The remainder of this paper is structured as follows. Section II describes several related work to security challenges in IoT networks and Blockchain Integration into IoT systems. Section III presents the background information about Blockchain technology and its architecture. In Section IV, we further detail the Medical IoT application. Section V focuses on the proposed system steps. In section VI, the performance of our proposal is evaluated with regards to memory and CPU overhead. Section VII represents the challenges related to Blockchain-IoT integration. Finally, in section VIII, conclusions and future works are addressed.

 ISBN: 978-1-61208-862-4

II. RELATED WORK

This section illustrates the related work as below :

A. IoT Networks and their Security Challenges

The IoT is an emerging technology connecting sensors, vehicles, hospitals, industries, and consumers through internet connectivity. However, IoT applications suffer from many challenges. One of these challenges, or maybe the most important one, is security. Many researchers tried to solve the security issues of the IoT systems. The authors in [1] presented a comparative study of various existing architectures in IoT networks for malware detection and prevention. The work highlights different security requirements of IoT communication environment and provides various details of the malware programs. Nevertheless, it has only focused on one layer of IoT architecture and it does not present clear solutions for privacy and security problems.

The authors in [3] analyzed the IoT system's security issues, which helps to understand and improve IoT security architecture. To overcome security problems, the authors propose that smarter security systems should be implemented, including managed threat detection, anomaly detection, and predictive analysis.

The work [4] has conducted a comprehensive security risk assessment using the OCTAVE Allegro method, which stands for the Operationally Critical Threat, Asset, and Vulnerability Evaluation. Then, the authors have identified ten critical cyber and physical assets. As an outcome, approximately fifteen security risks originating from both inside and outside smart homes have been identified. The consequences or impacts of these risks have been described, assuming that the threats are realized. The suitable countermeasures for mitigating the risks to an acceptable level have been produced. This research focuses solely on identifying security threats, impacts or risks, and proper countermeasures for IoT-based smart homes. According to the impacts of attacks on the internet of things, the authors in [5] discussed the procedures to mitigate attacks as DDoS or Mirai attacks on the IoT systems. Their recommendations were that security community must respond more quickly to security needs and establish novel defenses or techniques to avoid disrupting the IoT networks or perhaps the Internet infrastructure itself.

Regarding the security threats of IoT applications and frameworks, the work [6] has explained various security threats at different layers of IoT applications. Also, they discussed the existing and upcoming solutions to IoT security threats, including Blockchain, fog computing, edge computing, and machine learning. They then illustrated the state-of-the-art IoT security with future research directions to enhance upcoming IoT applications security levels.

In the literature, the security of the main IoT frameworks is surveyed in [7]. The authors reviewed the proposed architecture, the essentials of developing third-party smart apps, the compatible hardware, and each framework's security features. The comparison of security architectures revealed that the standards used for securing communications and verifying the various security features and immunity against attacks are one of the most critical contemporary issues facing the IoT. Regarding the layers of the Internet of things systems, it is often necessary to characterize the different threats related to each specific layer of the IoT system model. The authors in [8] analyzed the IoT systems layers or their architectures to detect , which layer is most vulnerable to provide suitable security solutions. The result is that the most vulnerable level of the IoT system model is the perception layer (physical layer). This is due to many reasons, such as technological heterogeneity and constrained resources. Authors demonstrated that it is crucial to work on this level's issues by implementing lightweight security solutions that suit the heterogeneous environments with resource-constrained devices.

B. The integration of Blockchain Technology into IoT Networks

A Blockchain is an immutable distributed database to , which new time-stamped transactions can be appended and grouped into a hash-chain of blocks. The Blockchain protocol structures the information in a chain of blocks , which are linked together by a reference to the previous block. One of the most critical challenges of IoT systems is the lack of confidence. According to the literature, the integration of promising technologies like IoT and Blockchain will become a revolution in IoT systems.

Blockchain technology usage in an IoT context has been introduced in [9]. This work explains that Blockchain features, such as immutability, transparency, and data encryption allow tackling IoT challenges. Furthermore, IoT systems have a lack of intrinsic security measures. The authors introduced two usage patterns: Device manipulation and data management. At last, they discussed the main challenges faced by the integration of IoT and Blockchain. A secure Blockchain-based smart home framework has been proposed in [10]. The authors thoroughly analyzed the security concerning the fundamental security goals (confidentiality, integrity, and availability).

The authors [11] discussed implementing e-government in Smart Cities and the available technologies and challenges that face it from a security and privacy perspective. They illustrated how sensitive information goes online and the procedure to protect it while transmitted, stored, and processed. Concerning securing the IoT system layers, this work [12] presents a model of multi-layer secure IoT network model based on Blockchain technology. This model divides the IoT into a multi-level de-centric network and adopts Blockchain technology to ensure high security and credibility. This model provides a solution for the wide-area networking of the IoT. In the smart healthcare field, the authors in [13] proposed a Blockchain leveraged decentralized eHealth architecture , which comprises three layers:

(1) The Sensing layer: Body Area Sensor Networks, (2) The NEAR processing layer: Edge Networks , which consist of devices at one hop from data sensing IoT devices and (3) The FAR processing layer: Core Networks that comprises Cloud or other high computing servers.

A Patient Agent (PA) software executes a lightweight Blockchain consensus mechanism and utilizes a Blockchain leveraged task-offloading algorithm to ensure patient's privacy. The PA processes medical data to ensure reliable, secure, and private communication. Furthermore, concerning the Personal Health Record (PHR) and

Electronic Health Record (EHR), the authors [14] presented the prototype implementation and evaluation of the OmniPHR architecture model that integrates distributed health records using Blockchain technology and the openEHR interoperability standard. The system can maintain distributed data via a Blockchain that could be recovered with low average response time and high availability. Large eHealth systems should have a mechanism to detect unauthorized changes in patients' medical documentation and enable access permissions (transactional transparency).

In the context of transactional transparency, the work in [15] proposed a model of eHealth integrity based on Blockchain to ensure information integrity in the eHealth system. In contrast to existing solutions, the proposed model allows information removal, which is a legal requirement in many countries' eHealth systems. A Blockchain is mainly used to implement a data-integrity service. This service can be implemented using other mechanisms, however, a Blockchain provides a solution that does not require trusted third parties and works in a distributed eHealth environment.

III. BLOCKCHAIN TECHNOLOGY

This section describes the concept of Blockchain technology as next :

A. Blockchain Presentation

A Blockchain is an immutable distributed database to which new time-stamped transactions can be appended and grouped into a hash-chain of blocks. The Blockchain protocol structures information in a chain of blocks where each block links by a reference to a previous block; consequently, forming a chain [16]. Blockchain has many features or benefits. Firstly, it is the best way to secure recording the data on the network. Yet, it is considered as a mechanism for transparent storage; thereby, anyone can verify the information's authenticity on the network. Additionally, the network's data cannot be changed or tampered without incurring huge overheads, making it secure and efficient. Secondly, Blockchain is leading a fundamental shift different from the traditional Internet of information and communications to the Internet of Value, providing trust, achieved through implementing Blockchain technology among strangers. Consequently, data can be exchanged instantly and efficiently without the need for intermediaries or third parties. From the above, we can summarize the features of the Blockchain as follows:

- Trust: adding information (Transaction) to the Blockchain ledger is performed only after the network participants' approval. When satisfaction is received to prove that the information is trustful, an authentication of information is performed in short intervals, and records are updated in the participant's ledgers.
- Immutability and Transparency: The term "immutability" refer to information that can only be appended to previous data, Briefly, it means that each block is related to the previous block. Once the block enters, it cannot be changed or lost. Transparency is ensured while all changes are reflected in the ledger of all participants. It is worth mentioning that any part of the network can audit these changes.
- Substantial Improvements: Blockchain can reduce the cost and greater the speed when transferring money or other assets due to the facts that it works 24/7, it does not need intermediary working during "regular" business hours, nor require a commission to verify the truthfulness of the records [17].
- Disintermediation: One of the Blockchain's important features is the capability of removing the central model. The reason for this feature is it depends on the peer to peer model without the need for any central intermediary to authenticate transactions. Furthermore, Blockchain ledger (database) cannot be maintained by anyone but by all participating network computers distributed worldwide.

B. Taxonomy of Blockchain Systems

As listed in Table 1, Blockchain networks have three different types based on network nodes permissions:

- Public Blockchain (permission-less). A public Blockchain network allows anyone to join it, and all the users have equal rights.
- Private Blockchain (permissioned), unlike the previous type, it is a closed network where privacy is important. This network includes the participating nodes that only are pre-selected and vetted. They are permissioned and the users in this type do not have equal rights in the network.
- Consortium Blockchain: This type is considered as a partially private and permissioned Blockchain. It is a set of pre-determined nodes that are responsible for consensus and block validation. Therefore, it is a partially centralized system, owing to some selected validator nodes' control, unlike the private Blockchain (which is entirely centralized) and the public Blockchain (which is entirely decentralized). This type combines the previous two types, as user requirements, whether read or write permissions would be public or limited to the network participants [18].

TABLE 1 : TYPES OF BLOCKCHAIN NETWORKS

		Blockchain systems		
		Public Blockchain	Private Blockchain	Consortium Blockchain
Features	Access	- Anyone	-Single organization	-Multiple selected organizations
	Participants	-Permissionless - Anonymous	-Permissioned -Known identities	- Permissioned -Known identities
	Security	-Consensus mechanism -Proof of Work / Proof of Stake	- Pre-approved Participants - Voting/multi-party consensus	- Pre-approved Participants - Voting/multi-party consensus
	Transaction Speed	- Slow	-Lighter and faster	-Lighter and faster

C. Blockchain system Components:

The Blockchain system consists of many technical components that enable it to provide services, such as security, distributed ledger system, transactions, consensus protocols, cryptographic techniques, and smart contracts.

- Transactions: Blockchain network nodes perform this procedure to exchange information between them based on peer to peer. The source node generates then broadcasts it to the whole network for validation. Lastly, transactions are assembled to form the block.
- The Distributed Ledger: is an append chain of cryptographically-linked blocks of data, maintained and updated by a decentralized network, which means all network nodes share a copy of the information (records). The distributed ledger contains all the transactions on the Blockchain. The network nodes are encouraged by economic incentives to maintain and secure the system so that the data has robust protection from adversarial interference, double-spend, counterfeit, collusion, tampering, or other types of malicious actions. [19].
- The Consensus Mechanism: is how all accounting nodes reach consensus to determine a Blockchain transaction's effectiveness. In the Blockchain network, many different processes need to coordinate their actions and define the total order of the information that is stored on each block to put this into the context of a Blockchain-based system. These processes' challenge lies in reaching a consensus on the block that should be appended to the chain at each particular index. Blocks are time-stamped and thus are ordered chronologically. Therefore, each Blockchain system embeds a consensus protocol that aims to prove that all correct processes agree on the same block, and the chosen block is considered valid and proposed by one process [17]. According to that many consensuses, algorithms are proposed:

a) Proof of Work (PoW): This algorithm relies on the node to carry out mathematical operations to find a random number and obtain the accounting right. Bitcoin, Dogecoin, and Litecoin are among the digital currencies based on the PoW consensus mechanism. However, its resources consumption is high, as the whole network needs to participate in the operation, which has low performance and efficiency.
b) Proof of Stake (PoS): consensus mechanism is that the difficulty of obtaining a node's accounting right is inversely proportional to the stake held by the node. According to the proportion and time of coins taken by each node, the difficulty of mining coins can be reduced in the same proportion to increase the speed of finding random numbers.
c) Proof of Authority (PoA): The transaction and the block are validated by an approved node (called a validator) without a huge computational overhead of a mining process. The validator must authenticate on the Blockchain. The PoA Blockchain becomes safer and cheaper [19].
d) Practical Byzantine Fault Tolerance (PBFT): In this approach, a primary and a secondary replica are utilized in the consensus process. The secondary is continuously evaluating the primary decisions in the Blockchain and make any necessary actions if the primary is compromised.

- The Smart Contract: It is a predefined code that is automatically executed by a Blockchain miner. As a result, it updates the ledger status on the Blockchain network. These changes cannot be falsified or tampered with once a specific consensus mechanism confirm them. The smart contract refers to the code that realizes the functions of receiving, storing, and transferring information. The smart contract will be triggered automatically without the outside parties' participation once the conditions are met. Due to the decentralized nature and the cryptographic algorithms of the Blockchain, the participating parties do not have the authority to change the clauses individually, which makes them trustful [20].
- The Asymmetric Encryption and Authorization Technology: The account identification information is highly encrypted and can only be accessed under the data owner's authorization. To use the Blockchain, every node will get a pair of keys. The first key is called the public key , which is used as a unique address and shared with all nodes in the network. It encrypts the message (Transaction) and verifies the received signatures. The Second key is called the private key, which must be kept secret. It is used for signing Blockchain transactions and decrypting the received messages.

D. How the Blockchain Technology Works

The first block is created and called the "Genesis Block"; then, the second one is formed and connected to the first block in chronological order. Similarly, the following blocks are performed. The Blockchain users search the numerical solution that corresponds to the specific hash value, which is called "digging mine". Any user (node) who finds the solution broadcasts it to the whole network and it will get the reward. The rest of network users will stop looking for the solution and start verifying the numerical solution. When the numerical solution is verified, the newly built blocks are added to the existing Blockchain. After that, the complete Blockchain is generated [21].

To clarifies the work of Blockchain, we use a Bitcoin Blockchain as an example. If the source node wants to send bitcoins to another node (destination node) it will create the transaction and broadcasts it to the entire network. Then, all transactions are queued in the transaction pool. Miners create blocks (sets of transactions) to be added to the chain. Miners are required to check each transaction's validity, and the current block connects and refers to the correct hash of the previous block. By this way, it is easy to detect whether data from a block is tampered with or not. In this case, the proposed block is added to the chain, and all nodes update the distributed ledger. Finally, the send bitcoin

 ISBN: 978-1-61208-862-4

process (Transaction) from the source node to the destination node is complete.

IV. MEDICAL IoT APPLICATION

This section describes the concept of medical IoT applications as next :

A. EHR Systems

A key feature of an EHR is that health information can be created and managed by authorized users in a digital format that can be shared across the entire healthcare ecosystem. This includes patient information from wearable devices owned and controlled by patients to be sent to healthcare providers, physicians, specialists, pharmacies, laboratories, and emergency facilities. Electronic healthcare records will consist of health information from all providers involved in a patient's care [22]. EHR systems can improve many major areas in the healthcare industry as follows:

a) Physician productivity can speed up physician diagnoses and digitize administrative tasks.

b) Patient satisfaction: provide them the ability to quickly obtain their data and see , which areas of their health history require improvement.

c) Ensuring the confidentiality, integrity, and availability of the stored data because data sharing will be only among authorized users.

The EHR system uses encryption techniques and cryptographic signatures to achieve confidentiality and ensure electronic health data integrity and authenticity. EHR system also uses access authorization to health data records to avoid data breach risks. Nevertheless, when integrated with Blockchain technology, EHR can use Blockchain mechanisms to manage the health data. In EHR systems, the patient uploads encrypted data to the system. The authorized Healthcare Provider retrieves these data and decrypts them to provide diagnosis and encrypt them again to be sent to another unit, such as a laboratory or pharmacy, to complete the task.

B. Medical IoT –Blockchain Applications

Smart healthcare applications have many challenges, such as integration, data overload, accuracy, and cost. Briefly, data security and privacy is also a major concern. Data is sensitive and vulnerable to various security risks such as eavesdropping, hijacking, denial of service, and tampering. Therefore, the need emerged for methods or techniques to solve security challenges and protect data. Recently, there is an increasing trend in deploying Blockchain in the healthcare sector (e.g., public healthcare management, counterfeit drug prevention, and clinical trial) [22].

In the medical IoT applications, private Blockchain is used which mean just known persons (Known identities) can access to the network. As shown in Figure 1, the patient from house send symptoms over the network to the doctor. The doctor will then send it to another unit such as a laboratory, consultant or sometimes emergency unit . As a result, will get a diagnosis and then sent it to pharmacy that sends a medicine to the patient. Any person (node) in the network has a medical ledger. It contains a copy of the same medical records for all transactions in the network and automatically updates it when any transaction is sent across the network. The transactions (blocks) are immutable. Therefore, the Blockchain is considered as the best way to protect medical records or personal information.

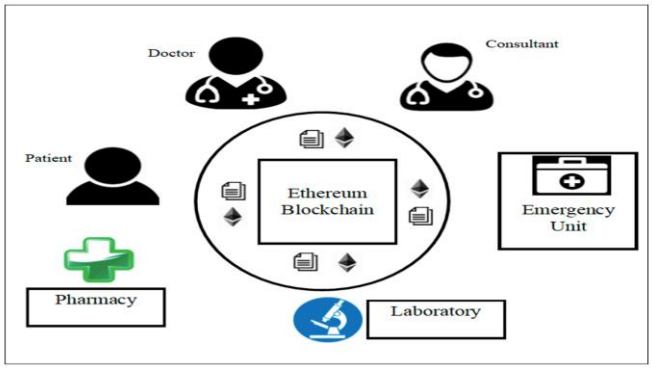

Figure 1: Blockchain-based healthcare system.

The advantages of applying Blockchain in the healthcare field (Medical IoT (healthcare) are as follows:

- Easier access to medical data: Because healthcare information's sensitivity is crucial, the costly overhaul of information technology systems and the overall regulatory environment and privacy concerns block its development. Blockchain technology may offer a solution by helping patients to get easy access to their data. Instead of navigating through multiple laws and processes of medical service providers to retrieve the information, this can be easy by utilizing the distributed ledger and the ability to maintain privacy through the public and private key. Furthermore, easiness for identifying the user and granting access to the appropriate medical records while keeping the overall data is ensured. Moreover, Blockchain thereby eliminates the centralized aspect where information is stored with one provider, as information is shared and accessible across all stakeholders upon the request.
- Facilitated sharing of medical records: The medical profession's problem is that medical data are extremely valuable for research purposes, and the improvement of overall medical conditions and operations is crucial. However, at the same time, this information is highly sensitive and faces massive legal hurdles with regards to sharing and aggregating the information from the various sources. Blockchain can solve this issue by allowing the patient's medical data to anonymize while keeping intact all pertinent medical information and rendering it serviceable in the aggregate. By using Blockchain, the patient would remain anonymous by keeping his/her private key secure and only sharing their information via their public key. In the meantime, the information remains publicly available for research purposes without the risk of revealing the patient's identity.
- Unification of medical records: In the case of using Blockchain, the medical information would be

decentralized thereby rendering it available directly to the patient, who can leverage the asymmetric encryption of the Blockchain to share their medical data with their physician while maintaining anonymity. Furthermore, the Blockchain system would allow for a standardized data format that would make it easier to share and communicate with different physicians. Lastly, users can choose to participate anonymously in medical research by offering their data to studies without the risk of personal identification [23].

V. PROPOSED SOLUTION

As mentioned earlier, the goal of this paper is to ensure healthcare data privacy and decentralized storage by using Blockchain technology. Due to the limited block size, privacy leakage and the increase of computational overhead, the EHR systems cannot upload the medical records and store them directly in the Blockchain. Therefore, to tackle these issues, few solutions have been proposed. Many applications use a cloud server as a third party. However, this solution has the risk of a single point of failure that means if any node is down the user cannot retrieve data of this node. Also, some curious cloud servers may collect sensitive patient data without consent. Therefore, in this paper, a decentralized peer-to-peer file system named InterPlanetary File System (IPFS) is used to avoid the risk of a single point of failure. IPFS is a decentralized file-sharing platform that identifies files through their content. It relies on a Distributed Hash Table (DHT) to retrieve file locations and node connectivity information. In a P2P network such as IPFS, if one node is down, other nodes in the network can serve needed files. According to [22], this approach is considered as the best solution to prevent a single point of failure in addition to other advantages, such as high storage throughput and faster data retrieval.

To describe our proposal illustrated in Figure 2 , we use a case scenario where a patient sends medical data to the EHR system and a health provider, such as a doctor or pharmacist, to request or retrieve these data. Our proposal uses a private blockchain network (permissioned network). In this type of network, the identities of participants are known and users are authenticated previously. Let us suppose that all the nodes such Local Healthcare Managers (LHM) and Electronic Healthcare Managers (EHM) have received a pair of private and public keys.

The patient is wearing some sensors and has a smartphone (or a PDA) to receive medical data from the sensors. The following steps show how patient's healthcare data will be registered and then accessed by a medical staff (healthcare provider):

1) Wearable sensors in the patient's body send data to a mobile phone.
2) The mobile sends these data to a LHM (e.g., pc device) which collects these data. This device works as a medical wallet.
3) The LHM gets the hash value H1 of the data , which will be stored in the decentralized peer-to-peer file system IPFS and sends a transaction to store this hash value in the Blockchain. As mentioned above, data is not stored in the Blockchain but only its hash value.
4) The Blockchain provides EHM with the value of H1 and this hash value will be considered as an index of the data to be stored in IPFS.
5) When H1 reaches the EHM, LHM encrypts its medical records whit the public key of EHM and signs this data using its private key. Then, LHM sends the data to EHM. Confidentiality of Data is ensured through encryption process and authenticity and integrity are provided by the signature. The EHM verify the signature with LHM public key and then decrypts the received data with its private key. From this data, it computes the hash value named H2. Smart contracts are triggered to verify if H1 is equal to H2. If it is the case, the received data is considered as valid data to be stored in IPFS. If not, data will not be stored and step 6 will not be executed.
6) EHM encrypts the medical data using its public key and sent it to IPFS to be stored.
7) Next, a new transaction will be sent to the Blockchain network, and then the ledgers of all the nodes are updated.

To retrieve specific medical Data from the system, a health provider must do the following tasks:

- It sends a transaction to the Blockchain network to fetch the required data index. Then, the index is sent to EHM. At this point, the EHM will request the data from IPFS system and compare between the index and hash value of the requested data. Smart contract is executed to ensure the validity of the data by comparing the two hash values. If they are equal, the EHM will retrieve data. Otherwise, the system will discard the request.
- Lastly, the EHM decrypts the medical data with its private key and then encrypts it again using the health provider's public key and finally, it sends it to the health provider. Health provider receives the required data and decrypts it using its private key. After that, the EHM will update the Blockchain. Additionally, LHMs and
- health provider's records will also be updated because each node has a copy of the Blockchain.

VI PERFORMANCE EVALUATION

This section describes the implementation process of the proposed system to evaluate its performance . In our scenario, we use a Blockchain network based on Quorum. It consists of seven nodes representing actors in the proposed system, such as patients, doctors and pharmacies, etc.

Quorum is an Ethereum-based distributed ledger protocol that has been developed to add the ability to create private Blockchain between selected participants and adds transaction privacy on normal Ethereum transactions [24]. It uses Raft consensus algorithm , which supposes that the consotium members are known and provisioned into the system. A leader is responsible for generating new blocks. RAFT need 2f+1 nodes to be setup in the network to have the capability to tolerate f faulty nodes [25].

 ISBN: 978-1-61208-862-4

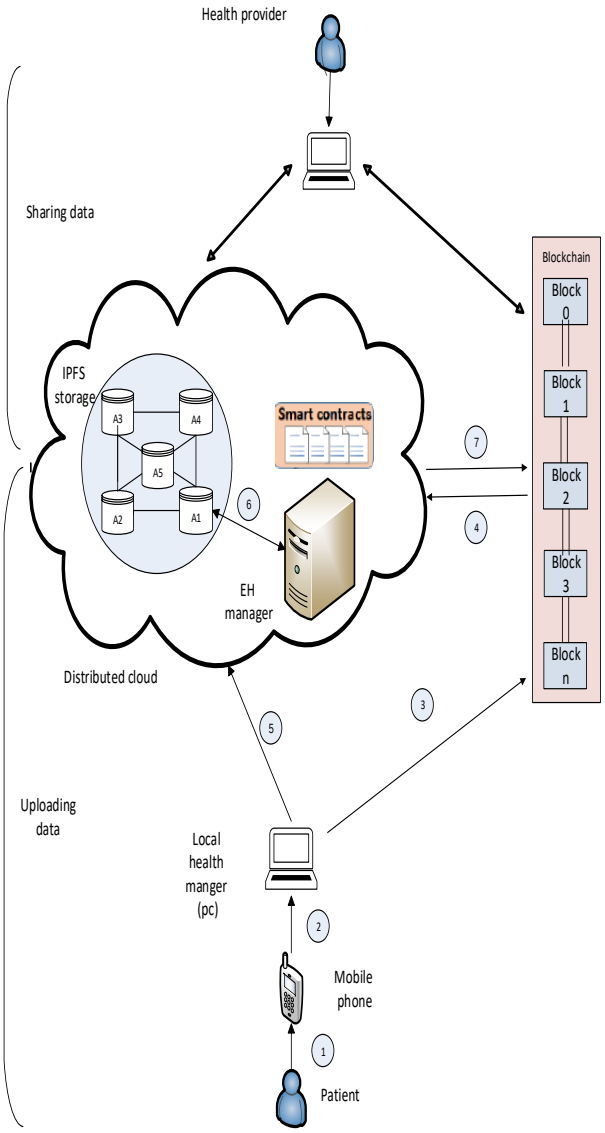

Figure 2: The proposed system architecture

We led the simulation for fifteen minutes, from minute 45 to 60, and during this period thirteen transactions are sent. Each transaction contains a medical data hash. The quorum profiling tool is used to benchmark network statistics on our quorum network. We focus on memory usage and CPU time as performance metrics. First, we calculate the average amount of memory usage in all the nodes. From Figure 3, it can be seen that the memory usage increases with the creation of new transactions and reaches the top when the time reaches 55 minutes. Specifically, at the beginning of this experiment, there weren't any transactions. Then, more transactions are exchanged and new blocks are added to the Blockchain. Therefore, more data is cached in the memory , which explain the memory overhead. We stop sending transaction at 55 minutes and accordingly, the memory usage becomes almost constant.

The results of the second experiment are illustrated by Figure 4. We evaluated the average amount of CPU time when the 13 transaction are processed. In the beginning, the CPU usage increases as the nodes create transactions and encrypt/decrypt data. Then. after the minute number 55 of the experiments, no more transactions are created and consequently, the average amount of CPU time decreases at the end of the experiment.

VII. CHALLENGES IN BLOCKCHAIN –IoT INTEGRATION

This section studies the main challenges that can be addressed when the Blockchain is applied technology to the IoT domain. The Blockchain is technically designed for an Internet scenario with a powerful computer; however, this characteristic is far from IoT's nature. Briefly, the exiting challenges are as follows:

- Storage capacity and scalability: In IoT healthcare applications, devices can generate gigabytes (GBs) of data in real-time, representing a significant barrier to its integration with Blockchain. It is known that some current Blockchain implementations can only process a few transactions per second. Furthermore, Blockchain is not designed to store large amounts of data like those produced in the IoT.
- Legal issues: The IoT implementation in the medical domain is affected by countries' laws or regulations regarding data privacy and protection. Laws that deal with information privacy and handling are a big challenge to be tackled in IoT and will be an even more significant challenge if used in combination with Blockchain.
- Security: One of the main challenges in the integration of the medical IoT with Blockchain is IoT data's reliability. Blockchain can ensure that data in the chain are immutable and can identify their transformations. Nevertheless, when data arrives already corrupted in the Blockchain, they stay corrupt. Corrupt medical IoT data can arise from many situations apart from malicious ones [26].
- Smart contracts: Providing a secure and reliable processing engine for IoT applications, filtering, and group mechanisms should be complemented smart contracts. Consequently, enabling applications to address the IoT depending on the context and requirements. Mining is still a key challenge in IoT applications due to its limitations. IoT is mainly composed of resource-constrained devices; however, globally the IoT has potentially huge processing power. The consensus algorithms of Blockchain technology, such as Proof of Work (PoW), consumes a lot of node energy, which is an additional challenge [27].

VIII. CONCLUSION AND FUTURE WORK

In this paper, the most important aspects of IoT and Blockchain technologies have been investigated. For a concise presentation, we first introduced Blockchain definition, types and fundamental characteristics. Next, we clarified the process of Blockchain work. This paper demonstrated next many issues related to the EHR systems. These systems cannot protect medical data from theft tampering, and other malicious activities. Therefore, the use

 ISBN: 978-1-61208-862-4

of a distributed storage system (IPFS) with Blockchain could protect the sensitive medical data from malicious attacks and security threats.

To achieve that, we proposed a system that consists of two-part: uploading medical data of patients and sharing or retrieving data by healthcare providers (doctors, hospitals, etc.). Finally, performance evaluation in terms of memory and CPU overhead is conducted. As presented by the implementation results, the proposal system allows users to share medical data in a reliable and quick manner. To achieve the desired level of patient privacy and network security, it uses different keys for encryption and decryption of medical data and prevents unauthorized access to the e-health system. Additionally, the proposal system decrease consumption of network resources and computational overhead by storing actual medical data in a distributed storage system (IPFS). We believe that our solution is a step towards effective management of e-health records , which is promising and important in most applications of healthcare.As future work, we will expand our system and implement it on more complex senarios.

REFERENCES

[1] M. Wazid, A. K. Das, Joel J. P. C. Rodrigues, S. Shetty, and Y. Parky, "IoMT Malware Detection Approaches: Analysis and Research Challenges", IEEE Access, Vol. 7, Nº 1, December 2019.

[2] H. Rathore, A. Mohamed, and M. Guizani, "A Survey of Blockchain Enabled Cyber-Physical Systems", Sensors, Vol. 20, Issue. 1, January 2020.

[3] S. Vashi, J. Ram, J. Modi, S. Verma, and C. Prakash, "Internet of Things (IoT) A Vision, Architectural Elements, and Security Issues" International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam. India, 10-11 Feb. 2017, ISBN:978-1-5090-3244-0.

[4] B. Ali, A. I. Awad, "Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes", Sensors, Vol. 18, Issue. 3, March 2018.

[5] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "DdoS in the IoT: Mirai and Other Botnets", Computer, Vol. 50, Issue. 7, pp .80 – 84, July 2017.

[6] V. Hassija, et al, "A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures", IEEE Access, Vol. 7, pp. 82721 – 82743, June 2019.

[7] M. Ammar, G. Russello, and B. Crispo, "Internet of Things: A survey on the security of IoT frameworks", Journal of Information Security and Applications, Vol. 38, pp.8-27, February 2018.

[8] M. Frustaci, P. Pace, G. Aloi, and G. Fortino, "Evaluating Critical Security Issues of the IoT World: Present and Future Challenges", IEEE Internet of Things Journal, Vol. 5, Issue. 4, pp. 2483 – 2495, Aug. 2018.

[9] A. Panarello, N. Tapas,G.Merlino, F. Longo, and A. Puliafito, "Blockchain and IoT Integration: A Systematic Survey", Sensors, Vol. 18, Issue. 8, August 2018.

[10] A. Dorri, S.S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT Security and Privacy: The Case Study of a Smart Home", IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Kona, HI, USA, 13-17 March 2017, ISBN:978-1-5090-4339-2.

[11] L.Yang, N. Elisa, and N.Eliot, "Privacy and Security Aspects of E-Government in Smart Cities", Smart Cities Cybersecurity and Privacy, pp. 89-102 , 2019.

[12] C. Li, L. J. Zhang, "A Blockchain Based New Secure Multi-Layer Network Model for Internet of Things", IEEE International Congress on Internet of Things (ICIOT), Honolulu, HI, 25-30 June 2017, ISBN. 978-1-5386-2011-3.

[13] Md. A. Uddin, A. Stranieri, I. Gondal, and V.Balasubramanian, "Blockchain leveraged decentralized IoT eHealth framework", Internet of Things, Vol. 9, March 2020.

[14] A. Roehrs, et al, "Analyzing the performance of a blockchain-based personal health record implementation", Journal of Biomedical Informatics, Vol. 92, April 2019.

[15] T. Hyla, J. Pejaś, "eHealth Integrity Model Based on Permissioned Blockchain", 2019 Cybersecurity and Cyberforensics Conference (CCC), Melbourne, VIC, Australia ,8-9 May 2019, ISBN. 978-1-7281-2600-5.

[16] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT. Challenges and opportunities", Future Generation Computer Systems, Vol. 88, Pages 173-190, November 2018.

[17] S. Makridakis, K.Christodoulou, "Blockchain: Current Challenges and Future Prospects Applications", Future Internet, Special Issues, October 2019 .

[18] D. Puthal, N. Malik, S.P. Mohanty, E. Kougianos, and G. Das, "Everything You Wanted to Know About the Blockchain: Its Promise, Components, Processes, and Problems", IEEE Consumer Electronics Magazine, Vol. 7, Issue. 4, pp. 6 – 14, July 2018.

[19] T. M. Fernández-Caramés, P. F.Lamas, "A Review on the Use of Blockchain for the Internet of Things" IEEE Access, Vol. 6, pp. 32979 – 33001, May2018.

[20] J. Yang, S. He, Y. Xu, L. Chen, and Ju Ren "A Trusted Routing Scheme Using Blockchain and Reinforcement Learning for Wireless Sensor Networks", Sensors, Vol. 19, Issue. 4, February 2019.

[21] Z. Zeng, et al, "Blockchain Technology for Information Security of the Energy Internet: Fundamentals, Features, Strategy and Application", Energies, Vol. 13, Issue 4, February 2020.

[22] S. Shi, D. He, Li Li, N. Kumar, M. K. Khan, and K.K. R. Choo, "Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey", Computers & Security, Vol. 97, October 2020.

[23] J. A. Jaoude, R. G. Saade, "Blockchain Applications Usage in Different Domains", IEEE Access, Vol. 7, pp. 45360 – 45381, March 2019.

[24] J. P. Morgan Chase,"A Permissioned Implementation of Ethereium", GitHub repository https://github.com/jpmorganchase/quorum, 2021.

[25] D. Ongaro, J. Ousterhout, "In Search of an Understandable Consensus Algorithm", USENIX Annual Technical Conferences, Philadelphia. PA, 17-20 June 2014.

[26] M. Andoni, V. Robu, D. Flynn, S. Abram, D. Geach, D. Jenkins, P. McCallum, A. Peacock, and A. Peacockd, "Blockchain technology in the energy sector: A systematic review of challenges and opportunities", Renewable and Sustainable Energy Reviews, Vol. 100, pp.143-174, February 2019.

[27] Z. Zheng, S. Xie, H. N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: a survey", International Journal of Web and Grid Services (IJWGS), Vol.14, No.4, pp.352 - 375, October 2018.

 ISBN: 978-1-61208-862-4

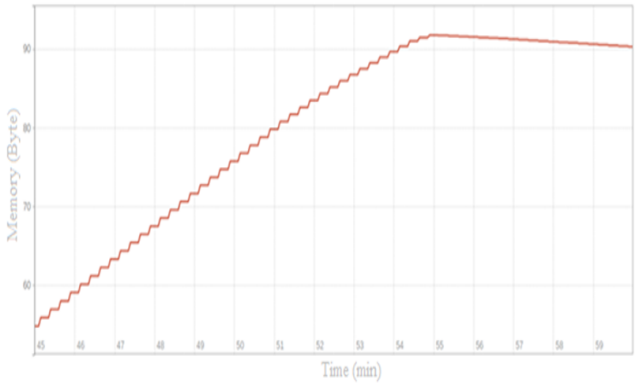

Figure 3: The average memory usage

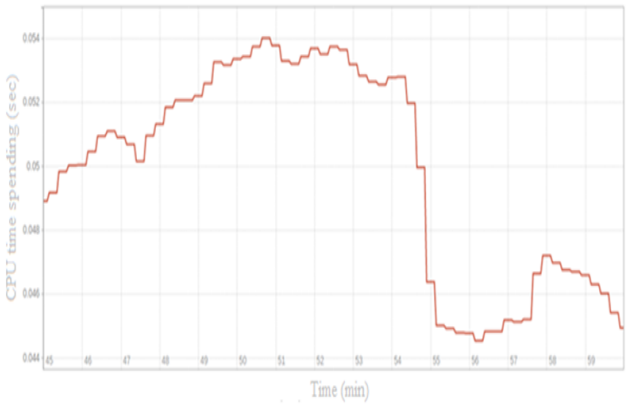

Figure 4: The average amount of CPU time.

 ISBN: 978-1-61208-862-4