BLOCKCHAIN-BASED SECURITY MECHANISMS FOR INTERNET OF MEDICAL THINGS (IOMT)

JAMAL Elhachmi and ABDELLATIF Kobbane

National High School for Computer Science and Systems Analysis (ENSIAS),
Mohammed V University in Rabat, Morocco

ABSTRACT

Traditional standards and security protocols are recognized as unable to solve the security, privacy, and availability of services of the Internet of Medical Things (IoMT) ecosystem, especially during the Coronavirus (COVID-19) pandemic. Blockchain technology has then emerged as a distributed ledger technology that can manage many intelligent transactions and ensure greater security in data management. The Blockchain-based security mechanisms with specific adaptation and additional layers of authentication and verification can offer a complete resources' management system. It has demonstrated it's superlatively as the core component of the Bitcoin cryptocurrency. In this paper, we propose a Three-Tier Blockchain Architecture in a hierarchical clustering network, with a lightweight authentication system-based API Gateway model that provides network and communication security.
Reasonable implementation is proposed and the obtained results demonstrate that our approach shows satisfactory performances in terms of transfer time, energy consumption, and CPU impacts. The traffic analysis also shows that the proposed model can meet the requested security, integrity, and confidentiality of user data.

KEYWORDS

Internet of things, Blockchain, Internet of Medical Things, IoT Security, Data Privacy.

1. INTRODUCTION

The internet of Things ecosystem is composed of a large number of enabled smart devices that cooperate among themselves by using embedded systems to collect, send, and act on data they acquire from their environments [1]. This type of network has become more and more successfully unavoidable in many different areas, such as the scientific, industrial, medical, and military fields. An Internet of Medical Things (IoMT) network as described in Figure.1, consists of a set of heterogeneous smart medical devices such as sensors, wearables, processors, etc., that collect, process, and transmit data to the Smart Gateways Server(SGS) or fog servers, which act as a bridge to the cloud. These data are aggregated, processed, and stored in the cloud and can be used by users including healthcare applications, doctors, and patients to monitor the end nodes online [2].

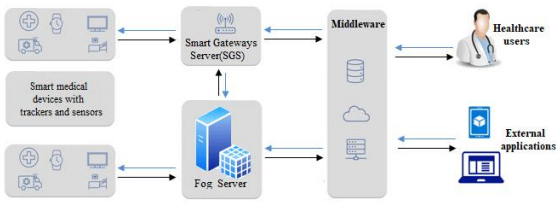


Figure 1. Cloud-based of IoMT application.

However, the cooperative IoMT ecosystems have a number of undesirable characteristics concerning the availability of services, interoperability, data management, the privacy of users, and security. They present a crucial obstacle to the continued growth of IoMT wireless systems and services. Another point of failure that these systems suffer is the dependence on the cloud server, and if the cloud is down for whatever reason, the users are not able to connect to the cloud server, thus causing the unavailability of services.

Background and Motivation :

The unstandardized and centralized character of the IoT network architecture, limitations of traditional standards and security protocol, and the absence of consensus among stakeholders in the resource-constrained IoMT ecosystem have made the availability of services, security, and privacy of this IoMT ecosystem challenging; this makes it vulnerable to cyber-attacks. And given the importance and sensitivity of the data exchange, especially during the CORONA epidemic crisis, and the increasing number of devices and applications, new standardized architectures and security mechanisms are necessary. The security challenges include authentication, access control, privacy, security protocols, software vulnerability, and scalability.

Many studies have affirmed that more than 47 vulnerabilities affecting 23 IoT items from 21 manufacturers were disclosed in 2018. The fourth Biannual Industrial control system (ICS) Risk & Vulnerability Report also has found that vulnerabilities are expanding beyond Operational Technology (OT) to the Extended Internet of Things (XIoT), with 34 % affecting IoT, Internet of Medical Thing (IoMT), and IT assets in late 2021. Cybercrime has cost the world more than $6tn by the end of 2021. And a business company was hit by ransomware every 10 seconds. Norton Security has affirmed that 33 billion records will be stolen by 2023. Security has therefore become one of the main challenges in this kind of ecosystem [3].

So, to ensure the efficiency of communications among interconnected devices in a secure manner with low latency and high throughput, the major involved techniques in recent IoMT network design and their issues, in accordance with Security, integrity, and confidentiality international directives for designing future IoT networks are Blockchain, cryptography, and artificial intelligence (AI).

Blockchain has emerged as the most promising technology to guarantee the security and agility of processes and the use of a safe and reliable IoT network. The most dedicated sources for the technology industry are confident that Blockchain itself become the most powerful secure technology of tomorrow.

Despite its public availability, Blockchain is a decentralized system with a read-only nature, making it mathematically impossible to create and add fraudulent transactions to the blocks. Blockchain has always considered itself a safe, secure, and reliable system to store and execute transactions, without the involvement of any third party [4]. In combination with the significant advance in IoT technology in scaling the networks and filling the blockchain forking problems [2], the Blockchain-based IoMT ecosystem can provide stringent defense solutions against cyber-attacks. To address the partial vulnerability defect of some particular areas a clustering mechanism can be included in the standardized architecture with hierarchical authentication and access control system, which makes all devices less vulnerable and more protected against malicious exploitation attempts. Blockchain-based IoMT technology can offer a complete data management system with specific adaptations and additional mechanisms. Related works can be found in the following sources, but are not restricted to [34]-[60]. Each of the proposed techniques has its own advantages and disadvantages, and none of them can be considered on its own to fully accomplish the security aspects of the IoMT ecosystem.

Contribution: our contributions can be summarized in the following points:

- We propose a comprehensive view of Blockchain-based IoMT approaches for security and privacy resource management in IoMT. The most important literature published in peer-reviewed venues over the two last years that have a high impact.
- We identify the challenges and research directions in the Blockchain-based IoMT ecosystem.
- We develop a novel Blockchain-based IoMT secure method based on the Ethereum blockchain for managing sensors' resources and data in Healthcare Monitoring Systems ; It consists of the creation of a secure virtual group at the Ethereum blockchain level, using the signed token by the Curve Digital Signature Algorithm (ECDSA).

Paper Organization:

The rest of this paper is organized as follows: in Section 2, we take a look at some elementary concepts of Blockchain technology and its model. In Section 3, we review the relevant related works. In Section 4: we present formal modeling of our proposed architecture with a preliminary analysis of the obtained results of initial implementation in Section 5, followed by a conclusion in Section 6.

2. PRELIMINARIES AND DEFINITIONS

2.1. Blockchain

Blockchain is one of the most common and popular kinds of distributed ledger technologies. It is essentially a distributed, decentralized, shared, and the immutable ledger that keeps the information of various transactions that ever happened in a certain peer-to-peer (P2P) network [5]. As shown in figure 2, the group of collected transactions is assigned to a block in the general ledger. Each block has a timestamp and hash function which are used to link the current block to the previous block. This creates chains of blocks, which is why it is called the Blockchain. To store a transaction in this ledger, the majority of nodes in the Blockchain network should record their agreement. Blockchain technology promotes information sharing in which all contributing users/nodes in the blockchain network have a replica of the golden/original ledger so that all users are updated with recently added transactions or blocks [5]. The core components of the Blockchain are:

-The block or item: digitally signed by the owner, it contains a nonce and the ordered list of transactions, a timestamp, and a hash pointer that links to the previous block. A nonce is a random number or bit string that is used to verify the hash.

- Cryptography: It is the key component that plays the most important role in blockchain by linking the blocks in chronological order using the hash function, and providing the security, immutability, and rightful ownership of the transactions being stored on the block [5]. the family of the most used hash functions is the Secure Hash Algorithms (i.e.,SHA1,SHA128, SHA256, SHA512, etc.) [6].

- Smart Contracts: a self-executing contract invented for the first time by Nick Szabo [7] . it contains the terms and conditions of an agreement between the peers. these terms and conditions are written in a code, and all users must come to the same result by executing this code, to validate the smart contract. and enable the sender to create transactions in the shared ledger of the blockchain network.

- Consensus Algorithms: consensus protocols are a set of rules used by the participating nodes in blockchains to achieve agreement on a single state of the data. and decide whether a transaction is valid. This ensures that all participants collectively maintain a common transaction ledger [8]. The two most popular consensus algorithms are proof of work (PoW) and proof of stake (PoS).

- Peer-to-peer (P2P) networks: the Blockchains network is a peer-to-peer unstructured network, without any rules for structurally defining connections and without any central server. peers participate in the network exchange of information regarding peers that are known to them, and When a new neighbor node is required, a node selects one using this node information. it contributes to the storage and processing power for the upkeep of this network[9].

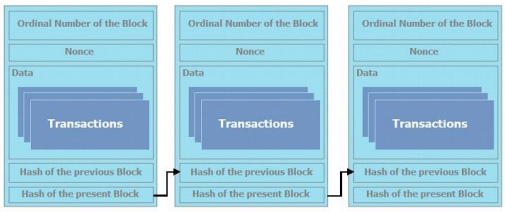


Figure 2. Logical Components of the Blockchain

2.2. Blockchain Model

As a distributed ledger, the blockchain system uses a secure communication analogy based on three principal interconnected elements: hash function, public-private keys, and digital signature [5].

Transactions are added to the blocks by authorized users, and only authorized partes can safely access the stored transaction in the Blockchain system. When each block is identified by a unique "hash" generated by a specific hash function and refers to the previous block with another unique "hash" as shown in Figure.3.

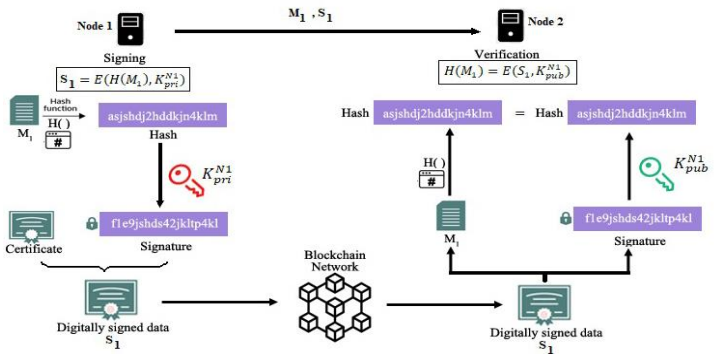


Figure 3. Blockchain-Based Authentication and Authorization model.

The private key and public key are created in pairs, where the private key is used to generate a unique digital signature for every transaction and then create digitally signed data and broadcast it along with the transaction. It ensures the authenticity of the transaction. The authorized owner (sender of the transaction) cannot in any way deny having sent the document. While the public key is used to allow the involved pairs to control these transactions. It ensures the accuracy of the transaction [9].

According to the consensus protocol, all nodes can achieve a common agreement, validate, and aggregate the created block into the chained structure. It ensures that blocks cannot be tampered with or removed without authorization from the structure [9].

3. REVIEW OF LITERATURE

In the last few years, finance has been the most revolutionary use case for Blockchain, and the most important illustrations of this use case were: Bitcoin and Ether. Recently, Some non-financial use cases have been developed, Supply chain management and digital IDs are two examples [4]. Blockchain technology has demonstrated its great ability to create more transparency and fairness while also saving businesses time and money [9]. It can evolve into separate concepts and impact a wide variety of fields. But blockchain technology is still unused in relevant areas. In this section, we provide an overview of the most important blockchain use cases, recent trends, and challenges. We present and compare related works based on specific criteria and from various points of view.

3.1. Blockchain and IoT Interaction:

Data Management :

Blockchain is one of the most dependable decentralized and distributed control systems that can use independent computers. It is considered a suitable technology for data standardization in the economic field. In particular, to control and automate IoT data access for multiple users.

Blockchain technology, which is based on hash functions, provides optimal data management, thereby securing data transfer.

One of the great brings of Blockchain technology is that sensitive data can't be stored directly in the system, but only encrypted data can be.

Another of blockchain technology's strengths is its ability to store data in collaboration with third parties, such as the cloud [9]. This feature has been exploited by the authors in [21] to establish a new approach named "interest groups", allowing the creation of dataset membership groups. Each group can sell, borrow, or rent the data it owns. The authors in [10] have also exploited the potential of Blockchain technology to develop an IoT-ready personal data-sharing prototype. In conformity with the General Data Protection Regulation (GDPR), the prototype can store and protect personal data in a distributed IoT ecosystem[9].

Blockchain technology has proven as a key technology for key financial areas such as automated compliance, compliance, asset rehypothecation, business operation casualty claim processing, proxy voting, and over-the-counter market [11]. Blockchain has also been explored in the context of building a new Blockchain network architecture using a blockchain gateway with the capacity to ensure data security and user privacy [12]. In [13] the authors propose an effective IoT-ready personal data-sharing architecture in compliance with the GDPR, where the Blockchain is used to create the user's data access strategy and manage the consent of these users. Therefore, researchers are inspired to develop several generic prototypes, especially based on Hyperledger Fabric, to ensure higher throughput and low latency for commercial transactions and transfers in other fields [14].

Authentication via the Blockchain-Based Identity :

Blockchain technology has shown the potential to enhance data management for Internet of Things devices because of its openness, trust, truthfulness, immutability, security, and privacy characteristics.

Additionally, Blockchain technology use has been impacted by the rapid progress of IoT networks and smart devices. It has been exploited to add additional trust levels to these devices through the identification and authentication mechanisms. In this context, the physical identities of users are used to build digital identities for efficient processing of transactions (between an individual and a business, between an individual and a machine, or between two machines) with minimal delays and costs.

According to IoT Analytics, by 2025 more than 20 billion gadgets will be linked to the internet, and money will be exchanged between these gadgets, people, and businesses. Most payment transactions will be done by machines in the future [9]. As a result, a totally new payment infrastructure will be needed, and most of the stakeholders (individuals, gadgets, or companies) in this development will have digital identities recorded on blockchain networks [13].

IoT and edge computing architecture:

Blockchain technology has the great potential to create new foundations for a distributed model that can replace the IoT central server model and this is through the setting of legal authentication mechanisms for the completion and validation of transactions, which will subsequently allow the management of billions of operations among different smart devices and reduce the implementing and maintaining costs of the central servers and other types of equipment [15]. According to some researchers, Blockchain-based IoT models can provide robust solutions for privacy and security issues in IoT ecosystems [16]. They are fitted with automatic mechanisms to evaluate cooperatively smart contracts. For example, the authors in [17] have improved the IoT infrastructure by involving Blockchain technology. The authors in [18] proposed an adaptive Blockchain-based IoT design to effectively serve network devices and maximize transaction speed. The research paper [19] has outlined a scheme for securing users' personal data using a combination of Blockchain and an off-Blockchain. Inspired by the Bitcoin concept, the authors in [20] proposed a security Blockchain-based IoT model that uses a proof-of-concept protocol and consists of four layers: objective, model, architecture, and mechanism [9]. In the same context to improve the setting of legal authentication mechanisms for the completion and validation of transactions, recent proposals like [21] and [22] have been inspired by the Namecoin concept to develop models based on the Block stack, as a blockchain-based naming and storage system. These proposals associate a unique name to each user in the Blockchain-based IoT ecosystem. Pinno, et al. [23] developed a new Blockchain-based IoT architecture for access control called Control Chain. Whereas the proposal in [24] developed an IoTChain architecture, that allows secure access and authentication for IoT devices.

Actually, Blockchain, IoT, and AI techniques combination increasingly attract research community interest, due to their robustness and safety policies. The authors in [25] have proposed a Blockchain-driven AI approach to reduce the issue of Blockchain.

The exploitation of cryptographic techniques in Blockchain-based IoT ecosystems using AI algorithms has extremely enhanced the security of connected IoT devices. For example, the authors in [26] have proposed a new Directed Acyclic graph-based blockchain algorithm (AES – CBC) that periodically changes the private key and initializes the vector (IV) value, The cost and time taken are then reduced by 20%.

In subsequent works, hybrid Blockchain approaches are proposed such as the paper [27], the proposed approach used a deployed blockchain on the 5G MEC smart grid to perform cross-chain communication [9]. The authors present an application-based cross-chain interoperability solution named appXchain which allows interoperability between any architecture type of blockchain network. In [28] the proposed approach introduces a blockchain router to empower blockchains to connect and communicate across chains. New blockchain-based architecture for secure and trustworthy operations in the industrial Internet of Things approach is proposed in [29], it uses a low-power ARM Cortex-M4 processor, and deploys an energy-efficient consensus mechanism proof of authentication (PoAh) in the blockchain network. In [30] the authors used a blockchain-based trust management mechanism (BBTM) to create smart contracts for trust computation and verify the computation process. Fan,et al. [31], unlike the traditional Blockchain, schemes have proposed a secure and efficient authentication and data sharing IoT-based Blockchain scheme, the approach can ensure data sharing and data transmission security. Report that the authors in [32] consider Blockchain Aided Privacy-Preserving Outsourcing Algorithms to secure outsourcing of bilinear pairings of IoT devices. A complete overview of different Blockchain approaches employed in the IoT engine is discussed in [33].

3.2. Blockchain Technology in the Internet of Medical Things

IoMT-based Blockchain is one of the most vital and sensitive applications of IoT ecosystems that has received more attention in the literature to provide privacy, security, access control, and availability of medical data. Consequently, IoMT-based Blockchain has attracted attention of many researchers, and new approaches have been proposed in the literature to investigate the proposed solutions regarding this main focus of them, which are ‘‘security and privacy’’, ‘‘access control’’ and ‘‘scalability’’ perspectives [2].

The comparisons of the most important previous IoMT-based Blockchain approaches, the different objectives, and the used approaches are summarized in Table .1 :

Table 1. Overview of the summarized related work in the IoMT-based Blockchain

main focus	Survey Paper	Year of Publication	Use case / Method(Algorithm)
SECURITY AND PRIVACY ASPECT	[34]	2018	Calculating dyslexic symptoms/Auto-grading algorithms
	[35]	2019	Detecting malicious nodes in medical smartphone networks(MSNs)/ Bayesian inference algorithms
	[36]	2019	Detecting malicious nodes in medical smartphone networks(MSNs) / Consortium Blockchain
	[37]	2019	Ensuring the security transmission between nodes / Electronic Health Records (EHR)
	[38]	2019	Creating secure alerts to authenticated healthcare providers / Reducing the delay and the network overhead.
	[39]	2019	Medical image retrieval with privacy protection/ Feature Vector Selection method (FVS)
	[40]	2019	Monitoring the progression of a neurological disorder / Ethereum blockchain platform using a Test of motor coordination.

	[41]	2019	Electronic medical reports (EMR) / Blockchain-enabled Authentication Key Agreement Protocol for IoMT (BAKMP-IoMT).
	[42]	2019	Remote patient monitoring and AI-assisted diagnosis/ Privacy-preserving federated learning.
	[43]	2020	Automatic stress control mechanisms / IoMT-Cloud Secure Data Storage with Analytics at the Edge
	[44]	2020	Secure management of EHR (Electronic Health Record), EMR (Electronic Medical Records), and PHR (Personal Health Records)/ IoMT-based Blockchain through new medical devices.
	[45]	2021	Secure image transmission and diagnosis / Blockchain-based deep belief network (DBN) algorithm
	[46]	2022	securing the electronic healthcare records storage and sharing / Elliptic Curve Digital Signature Algorithm (ECDSA)
ACCESS CONTROL	[47]	2019	Privacy-preserving access control mechanism for general data Protection regulation/ Practical Byzantine Fault Tolerance (PBFT) voting-based consensus
	[48]	2019	Access control for specific authenticated users/ Permissioned blockchain using Elliptic-curve cryptography (ECC).
	[49]	2019	Large-scale health data privacy-preserving and diagnose uploading/ Interplanetary file system (IPFS)
	[50]	2019	Healthcare services monitoring and treatment/Blockchain with on-chain smart contracts and a proof-of-medical-stake consensus mechanism.
	[51]	2019	Remote Patient monitoring systems/ ARX encryption scheme, Ring signatures, and Diffie-Hellman key exchange
	[52]	2019	Secures the medical data of patients / Access control model named (medical data protection access control)MDPAC based on the Role-based access control (RBAC) model.
	[53]	2019	Monitor patients remotely / Newly designed protocol named GHOSTDAG.
	[54]	2019	Electronic Health Records (EHRs) sharing framework/novel EHRs sharing architecture based on blockchain and IPFS.
	[55]	2020	Handle the COVID-19 healthcare crisis / blockchain-enabled IoMT
	[56]	2020	Security of data transmission between connected nodes/ IoMT-based Blockchain device authentication.

	[57]	2021	Automate medical alerting and services / Selective ring-based access control (SRAC) and other cryptography methods.
	[58]	2021	Patient motioning system/ interplanetary file systems (IPFS) cluster node, Consortium Blockchain.
	[59]	2022	Enabling the secure interoperability of healthcare organizations/ Ethereum blockchain with the proof-of-authority consensus
SCALABILITY ASPECT	[60]	2021	Secure scalability and data accessibility for healthcare environment / blockchain-assisted secure data management framework (BSDMF)
	[61]	2021	Blockchain-based authentication for IoMT devices / the proof of authority (PoA) consensus mechanism.

Table.1 presents a classification of the proposed new approaches according to the main aim and focuses of integrating blockchain technology into the IoMT eco-system, which are ``security and privacy", ``access control" and ``scalability" perspectives. Most of these approaches are private blockchain-based and used Ethereum infrastructure[63]; they were focused on one of the security levels to provide authentication solutions, privacy, data integrity, or confidentiality, and the majority of them implement smart contracts to allow access to only the authorized users based on some attributes of the IoMT ecosystem and their interaction with the users/stakeholders [33]. According to some studies, these solutions lack many technical details to ensure better integration of blockchain technology into the dynamic IoMT ecosystem. They have limitations to manage a high volume of data streams generated by IoMT devices because of resource constraints. Therefore technical adaptations to the Blockchain architecture are necessary to meet these challenges. Motivated by the superior performance of the Blockchain in security assurance, privacy preservation, and data analytics the main advantages of the proposed approach in this paper might be perceived through the following criteria: Three-Tier Blockchain Architecture, Hierarchical clustering network, and an additional level of authentication. approach' decentralized architecture makes it resistant to cyber-attacks.

4. PROPOSED IOMT-BASED BLOCKCHAIN APPROACH

In this section, we describe our approaches as a set of software used to control an IoMT ecosystem.

We first describe our architecture of Blockchain-enabled IoMT composed of four layers and using APIs running on the master device and their major interdependent components. We then present our authentication and access control strategies and details of the main functionalities of each project, technologies, and routines that are used to validate and identify the smart devices in its cluster. We also design smart contracts and transactions to explain the interaction process of each module.

4.1. System Architecture

In its logical representation, the proposed IoMT three-tier architecture contains three main tiers: the Physical tier in charge of data collection from the IoMT sensor devices, the IoMT Cloud Services tier is in charge of data storage in cloud computing, and the Application tier uses the

appropriate model for the treatment of these data. This model conforms to the reference architecture for IIoT proposed by Industrial Internet Consortium (IIC).

By incorporating the blockchain into IoMT systems, the secure IoMT ecosystem architecture occurs in its detailed representation with four layers:

- Layer 1: it is in this layer that we find all the IoMT nodes gathering information from any patient and offloading tasks to the Multi-Access Edges Computing (MEC) server through the small Base Stations. It considred as the « patient » device layer.
- Layer 2: is the Edge computing layer, it composed of the MECs, in a common geographical area, responsible for collecting data from IoMT devices in its coverage area and processes them with its Edge cloud server (ECS). The data is further processed at the fog and at the cloud layer to generate meaningful information [63]. The data is further processed at the fog and at the cloud layer to generate meaningful information. Further, in order to reduce the delay, all interacting parties in the medical eld who have interest in the data related to patients such as hospitals, medical centers, labs, etc... can get the patient data through this router[63].it is the getqay for the fog layer.
- Layer 3 : This is the core layer, The blockchain network layer is the middleware that offer trustworthy management of diverse resources across the underlying layers. it permits the control of the interaction between cloud providers in order to grant access for patient's data to each others wherever it is located.
- Layer 4 : it is the higher layer or the « cloud provider" layer. It is the layer responsible for processing the data using cloud computing, data storage services, and Machine Learning and IA mechanisms[63].

4.2. Blockchain-based Authentication for IoMT ecosystem

The APIs running in Edge and Fog Computing are used to verify the IoMT message's authenticity, using Smart Contracts deployed in the core Ethereum Blockchain.

The API gateway is a collection of micro-services, facilitating data and service requests and delivery. Its principal role is to serve as a single entry point and standardized process for interactions between a group of devices (IoMT) and a Master device. it also handles API usage, data analysis, access control, authentication mechanisms, and other services like rate-limiting [9]. The proposed APIs can additionally have a built-in management plane to identify, authenticate, anonymity, and verify the reputation of messages sent by the trust group of IoMT devices.

The Blockchain and smart contracts are integrated into the background to identify and validate the API Gateway's authenticity and only then the API messages are received by the application's API. API management is a suggested resource, particularly when several devices generate and consume data from a variety of sources. In the next sections, we outline the components of our proposed Registration and Authentication prototype [9].

a. Architecture of the proposed IoMT Blockchain authentication Platform:

Figure .4 illustrates the conceptual scenario of the IoMT blockchain platform.

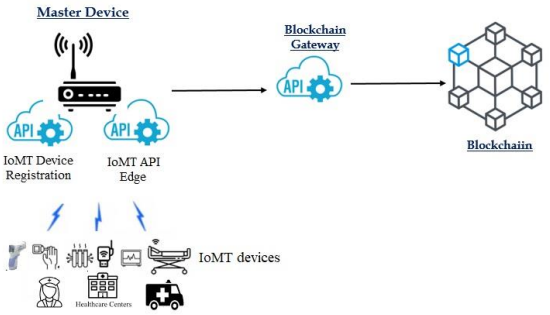


Figure 4. IoMT blockchain platform conceptual scenario

b. Architectural components:

The main components of the proposed system are:

1) Master Device: a device owns a private/public key pair which can be considered similar to a certification authority for IoMT devices.

2) Slave Devices: Each device that is a component of the system is called to as Slave devices. Each Slave generates an Elliptic Curve (EC) private/public key-pair. Then, each Slave device is delivered by a structure called a token, which represents a lightweight certificate of 64 bytes that contains:

- *groupID*: Describes the virtual group that the object will belong.
- *objectID*: Describes the slave device's identifier in the virtual group.
- *publicAddr* : describes the slave device's public address. This public Address represents the first 20 bytes of the Keccak SHA-3 of the slave device's public key.
- Signature: Generated by using the private key of the virtual group's Master to sign signature structure represents the Elliptic Curve Digital Signature . ECDSA is more adapted to IoMT contexts than traditional signature algorithms such as Rivest Shamir Adleman (RSA), especially concerning key sizes and signature times [9]. The Signature covers the Keccack hash of the concatenation of the groupID, the objectID, and the publicAddr.

3) IoMT device Registration: provides for each slave device a token, signed by the Master device after creating a group identifier (groupID). Once the group has been formed, the next step consists of the creation of the virtual group at the Blockchain level [9]. The Master device sends a transaction that contains the Master's identifier and the group identifier to create.
The Blockchain verifies that both the *groupID* and the Master's *objectID* are unique. Then, the virtual group is created.

Algorithm 1: Association roles to slave devices

```
0 : bc : Blockchain
0 : obj : Object
0 : sender : Object
0 : receiver : Object
0 : statut : State
0 : Define Master  : 1
0 : Define Slave  : 0
    Function :  CheckOID( Integer Iod, Blockchain bc)
    /* // check if the object identifier is used in the Blockchain or not      */
    Function : CheckGID( Integer GId, Blockchain bc)
    /* // check if the group  identifier is used in the Blockchain or not      */
    Function : CheckAddr( Integer objId, Blockchain bc)
    /* // check if the object Address  is used in the Blockchain or not      */
   Function : Exception( )
   /* // returns error message  */
begin
    if checkOID(object.Id, bc) = true then
    return Error() ;
    if checkAddr(object.grpId, bc) = true then
    return Error() ;

    if (object.type = Master)  then
        if checkOID(object.grpId, bc) = true then
            return Error() ;
        end
        else  if (object.type = Slave)  then
                    if checkgrpID(object.grpId, bc) = false then
                        return Error() ;
                    end
                    if (bc.tokenVerify(object.token, bc) = failed  then
                        return Error();
                    end
    end
end
```

Using *checkOID( ), checkAddr( )* methods, the Blockchain verifies consecutively if the object identifier and the object Address are used in the Blockchain by another object, if true, the association cannot be saved and validated. Else, and if the object is a Master, it cannot be associated. Otherwise, and if the object is a slave, The Blockchain verifies that both the *groupID* and the *Token* are valid to validate the slave device association request. Then, the slave object is associated with the virtual group.

4) IoMT API Edge: This API is running as a service on the master device to receive requests from slave devices in order to be associated with their virtual group. At the Blockchain level, The smart contract ensures the slave device's identifier is unique (objectID), The slave device's token is then verified for authenticity using the virtual group's Master's public key as illustrated in Algorithm 2 describes different parameters and functions. If at least one of the conditions is not accomplished, the device cannot be added to the group. Once a slave device's first registration request is successful, the latter is no longer required to verify itself using its token [9]. The Communication within the virtual group is illustrated in Figure .5:

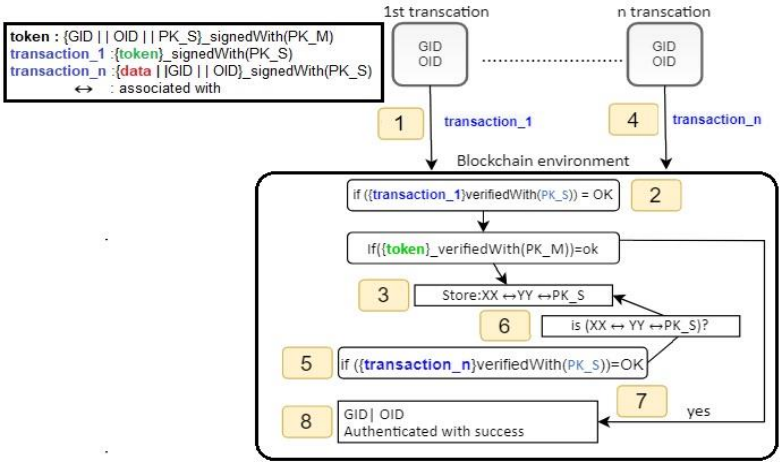


Figure 5. Slave device association

This Example represents a device slave named (S) which received a Master-signed token. Each token consists of: Gid(group ID), Oid (object ID) PKS,(slave device public key).

The process of group association request is illustrated in Figure.6

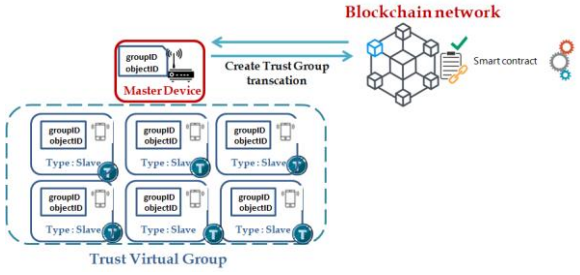


Figure. 6. Creation of virtual group at the blockchain

The next actions are presented as follows:

i) The association request is the first transaction, the token and device slave private key are signed in the transmitted message.

ii) Once the Blockchain get the action, it checks its validity by comparing the signature to the public key of the slave device. The tokens of the device slave are validated using the Master's public key

iii) When the token is valid and authentic, the Blockchain stores an association saves the values (*Gid*, *Oid*, and *PKS*);

iv) Transaction *n* is the case when (S) sends another transaction. This transaction includes the following elements: The data, *Gid*, *Oid*, The signature of the combination of the preceding fields, which is performed using the private key of the slave device.

v) The Blockchain validates the transaction's integrity by verifying the signature to the slave device's public key.

vi) When the signature is valid, the Blockchain checks that the public key used to verify the transaction is saved and associated with the transaction's *groupID* and *objectID*.

vii) When the association is successfully saved and validated, the device is authenticated.

5) The token Signature: To decrease computing power, and enhance performance in terms of latency and energy efficiency, the proposed approach uses a Curve Digital Signature Algorithm (ECDSA) to sign the token and device slave private key in the transmitted message. This alternative approach is also used to encrypt and decrypt messages. It can obtain high primary numbers faster and more effectively than the traditional method. It depends on the algebraic structure of the elliptical curves over finite fields.

The signature structure using the private key of the zone group's Master is:

Signature = PrK_M(Gid, Oid,pubAddr) , Where: *PrK_M* is the Master device private key.

6) Blockchain Gateway: Blockchain API Gateway is the software model (group of microservices) in charge of data communication and validation between the IoMT API Edge Network devices and the Blockchain. Through this API the master device can create a virtual group by making transactions to a smart contract that contains rules to achieve this action and also validate slave device association requests [9].

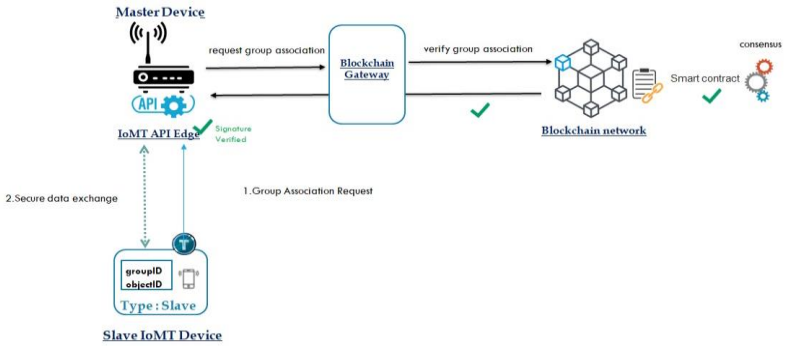


Figure 7. Creation of virtual groups at the Blockchain.

7) Smart Contract: To improve the overall performance of the system, and facilitate the cooperation between partners of our Blockchain-based IoMT ecosystem, the virtual group will be created, and the communication protocol will be governed by the "Smart Contracts". In this case, the smart contract integrated into the background of the private Ethereum blockchain covers the all rules to validate the API Gateway's authenticity and the rules to be checked before launching the inspection of the devices and also to validate the slave device association requests [9]. The smart contract algorithm rules are described as follows:

Algorithm 3 : Smart contract algorithm rules

```
1 if checkOID(sender.Id, bc) = false or checkOID(receiver.Id, bc) = false then
2       return Error( );
3 if (sender.Id ≠ bc) then
4       return Error( );
5 if (bc.SignVeri(sender.msg)= failed ) then
6       return Error( );
7 Secure data exchange finished with success
```

5. VALIDATION AND EVALUATION

The system test of our Blockchain-based IoT approach is implemented using a laptop (Configuration: Intel i7-3770 CPU at 3.40 GHz, 8 GB of memory) and two Raspberry Pi, where

the laptop plays the role of the master device and the Raspberry Pi cards are considered as slave devices. A series of numerical simulation experiments have been done using a private Ethereum blockchain and smart contracts written in the Solidity programming language. The purpose is to evaluate our approach regarding its execution time, energy consumption, and network traffic analysis.

The IoT Api Edge runs on the master device and is developed using Node.js to simulate the interactions between the master device as a server and the slave devices.

The slave devices are also simulated using the node.js program as a web client to interact with IoT Api Edge. The interactions are realized using JSON over HTTP protocol.

For this experimentation, we measure :

- The needed time to prepare a request for the association.
- The needed time to prepare a data message.
- The consumption power of the CPU required to prepare an association request.
- The CPU power consumption required to prepare a data message.

The exchanged data between the master device and the slave device is analyzed with a sniffer application to evaluate communication privacy.

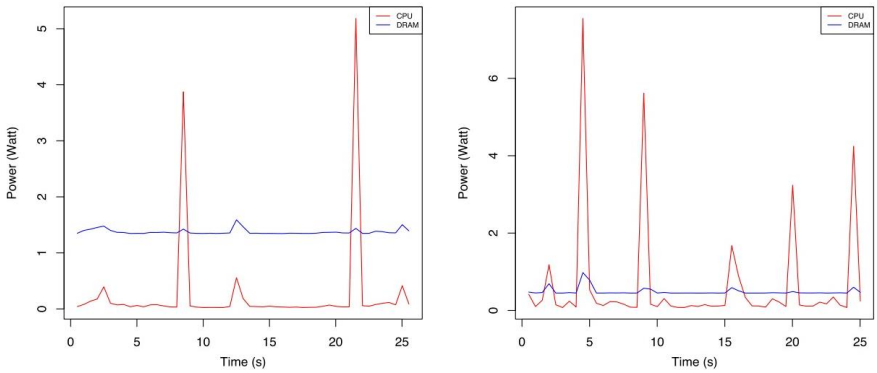
5.1. Time and Energy consumption

For all experiments, we remark that the association request is more complicated than sending a simple message. And as shown in Table 2, the performance in terms of the time consumption difference between the average and the standard deviation is extremely impacted by the complexity of the association request in comparison to the sending operation of a data message.

Table 2. Statistics Time and Energy consumption

Devices		**Laptop**	**Raspberry Pi 3(Model B)**	**Raspberry Pi 4(Model B)**
Assoc Time(ms)	Av.	1.03	2.1	1.7
	SD	0.12	0.034	0.029
Data time(ms)	Av.	0.13	0.9	0.6
	SD	0.001	0.025	0.029
CPU Pow Assoc(mWatt)	Av.	9.76	50.4	48.4
	SD	2.04	1.02	0.8
CPU Pow Data msg (mWatt)	Av.	3.30	16.33	15.09
	SD	0.80	1.08	0.9

Another important measure is the impact of messages' sending on the CPU and the Dynamic Random Access Memory (DRAM) energy consumption for the tested devices. As shown in figure 8, there are three principles phases of the system functioning: (1) an idle phase; (2) the execution of a loop that sends 100 messages where there is a break of 100 ms between each message, and (3) the return to the idle phase.



(a) (b)

Figure 8. The impact of message processing: (a) Laptop , (b) Raspberry Pi

The measures were realized using the RAPL measurement tool. Figure 8(a) describes the laptop's results where the loop is executed at the 12th second. The energy consumption, in this case, does not exceed 0.5 watts, which is shown by the third peak. Figure 8(b) illustrates Raspberry Pi's results, where the loop is executed at the 15th second. The energy consumption, in this case, does not exceed 1 watt, which is shown by the third peak. Even if the results are close and quite similar for both models of the Raspberry cards, the illustrated results here concern the Raspberry Pi 4 Model B. In both cases, one can note that the impact of the loop is really negligible. The other existing peaks are related to the operating system activity, and without any impact on energy consumption once the system is running.

The results in table 1 concern 100 experiments and present the average and standard deviation of the association request, data message preparation times, and energy consumption needed by the CPU in order to realize the association request and send a data message. According to the previous results on energy consumption, the association request is more complicated than sending a simple message. In contrast, the time consumption difference between the average and the standard deviation is based on the complexity of the association request compared to the sending operation of a data message.

5.2. Network Traffic Analysis

The network traffic analysis between the master device and the slave objects using the Wireshark network traffic analysis application, show that the data captured by the sensors of the slave device is sent encrypted, ensuring the fundamentals of security: authentication, confidentiality, integrity, and availability.

Figure.9 shows the request from a slave device to the master for the purpose of sharing encryption keys. The slave object calls the API endpoint "keySession" by passing the data in JSON format consisting of a public key (ECDSA) and object ID (oid). The master device responds with a JSON object.

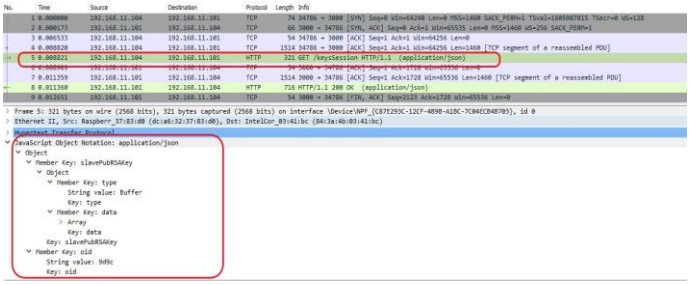


Figure 9. Retrieve security token (Slave request)

Figure .10, contains the session key encrypted by the public key of the slave device, which allows both the confidentiality of the key and also the authentication of the slave device. After the encryption key sharing session, all communication between the master and slave devices will be encrypted.

Figure 10. Encryption key session (Master response)

In Figure .11 shown, the slave device requests a master device token by calling the API endpoint ”GET /getTicket” sending its encrypted object ID (oid) and the public key.

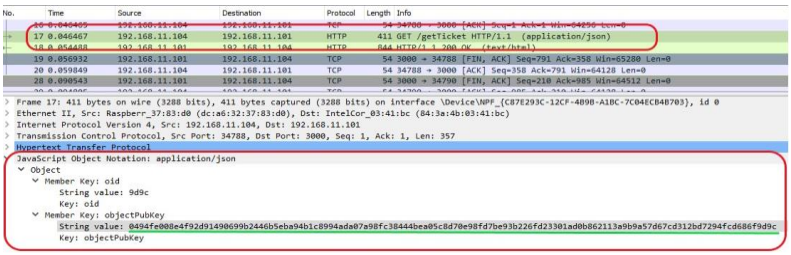


Figure 11. Retrieve security token (Slave request)

Figure.12 shows the master’s response as a token encrypted with the session key. Then the slave can decrypt and retrieve the clear text information in JSON format containing group id (GID), object id, public address key, and the preceding field’s ECDSAsignature concatenated.

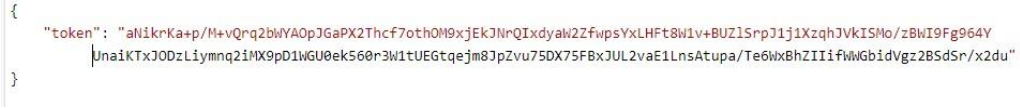


Figure 12. Encrypted token (Master response)

From the moment that the slave device has a token, it can be associated with the trust group by sending an association request to the slave device. As shown in Figure .13 the slave device sends

its object id (oid) and encrypted token to the master device. The latter checks the integrity of the token and checks the access conditions at the blockchain level. If the conditions are verified, then the master authorizes the access and, therefore, the slave can send the data.

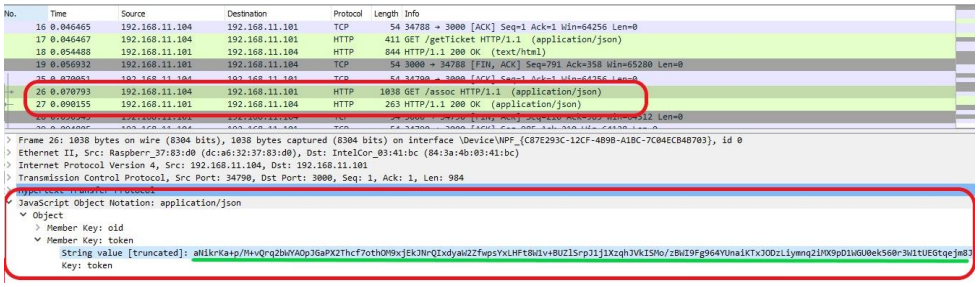


Figure 13. Slave device association Captured Data

Finally, we can say that the slave device can transfer the data to the master in an encrypted way. The slave device sends its object Id so that the master device always checks its group membership and the encrypted data.

6. CONCLUSIONS

The Internet of Things technology has overwhelmed the entire fields in our daily lives, especially in the health sector. The use of this great emerging sector resulted in the creation of numerous IoMT devices and services. However, the limited character of the available resources and the vulnerability of devices present a crucial obstacle to the continued growth of IoMT ecosystems. Access to these devices and their communication exchanges should often be secured.

In this work, we proposed Three-Tier Blockchain architecture as a solution for the secure communication exchanges of data between the various parties involved in an IoMT ecosystem. And using a hierarchical clustering network we have suggested a method for creating a group of trustworthy devices by establishing safe virtual zones in which devices can connect in an entirely secure manner. An additional level of security is added through the adoption of a robust authentication and access technique.

This proposed method has been evaluated and found to be capable of satisfying the desired security criteria as well as being resistant to cyberattacks.

In the future, we will extend our approach to develop a more efficient technique in a large-scale IoMT network with additional privacy and security concerns. we will integrate machine learning techniques as federated learning to manage the big datasets created by tremendously varied IoMT networks, thereby further enhancing the trust of IoMT systems.

CONFLICTS OF INTEREST

The authors declare no conflict of interest.

REFERENCES

[1] Hong, S. (2020). AN EFFICIENT IOT APPLICATION DEVELOPMENT BASED ON INTEGRATED IOT KNOWLEDGE MODULES. Issues in Information Systems, 21(3).

[2] Jolfaei, A. A., Aghili, S. F., & Singelee, D. (2021). A Survey on Blockchain-Based IoMT Systems: Towards Scalability. Ieee Access, 9, 148948-148975.

[3] Mohammad, A. S., Brohi, M. N., & Khan, I. A. (2021). Integration of IoT and Blockchain.
[4] Roeck, D., Sch¨oneseiffen, F., Greger, M., and Hofmann, E. (2020). "Analyzing the potential of DLT-based applications in smart factories," in Blockchain and Distributed Ledger Technology Use Cases – Applications and Lessons Learned, eds H. Treiblmaier and T. Clohessy, 245–266.
[5] Singh, S. K., & Kumar, S. (2021). Blockchain technology: introduction, integration and security issues with IoT. arXiv preprint arXiv:2101.10921.
[6] Di Pierro, M.(2017).What is the blockchain?. Computing in Science & Engineering,19(5),92-95.
[7] Szabo, N. (1997). Formalizing and securing relationships on public networks. First monday.
[8] Alzahrani, N., & Bulusu, N. (2018, October). Towards true decentralization: A blockchain consensus protocol based on game theory and randomness. In International conference on decision and game theory for security (pp. 465-485). Springer, Cham.
[9] Karafiloski, E., & Mishev, A. (2017, July). Blockchain solutions for big data challenges: A literature review. In IEEE EUROCON 2017-17th International Conference on Smart Technologies (pp. 763-768). IEEE.
[10] [10] Dorri, A., Kanhere, S., and Jurdak, R. (2017). "Towards an Optimized BlockChain for IoT," in Proceedings of the IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (Piscataway, NJ: IEEE), 173–178.
[11] IoT Analytics (2020). Industrial AI Market Report 2020-2025.
[12] Rantos, K.; Drosatos, G.; Kritsas, A.; Ilioudis, C.; Papanikolaou, A.; Filippidis, A.P. A blockchain-based platform for consent management of personal data processing in the IoT ecosystem. Secur. Commun. Netw. 2019, 2019, 1431578.
[13] Agarwal, R.R.; Kumar, D.; Golab, L.; Keshav, S. Consentio: Managing consent to data access using permissioned blockchains. In Proceedings of the 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Toronto, ON, Canada, 2–6 May 2020.
[14] Aldred, N.; Baal, L.; Broda, G.; Trumble, S.; Mahmoud, Q.H. Design and Implementation of a Blockchain-based Consent Management System. arXiv 2019, arXiv:1912.09882.
[15] iot-framework-gui. 2013. Available online: https://github.com/EricssonResearch/iot-framework-gui (accessed on 30 December 2020).
[16] Huh, S., Cho, S., and Kim, S. (2017). "Managing IoT devices using blockchain platform," in Proceedings of the 19th International Conference on Advanced Communication Technology (Piscataway, NJ: IEEE), 464–467.
[17] Dorri, A., Kanhere, S., and Jurdak, R. (2017). "Towards an Optimized BlockChain for IoT," in Proceedings of the IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (Piscataway, NJ: IEEE), 173–178.
[18] Zyskind, G., Nathan, O. and Pentland, A., 2015. Decentralizing Privacy: Using Blockchain to Protect Personal Data. 2015 IEEE Security and Privacy Workshops.
[19] Ouaddah, A., Abou Elkalam, A. and Ait Ouahman, A., 2016. FairAccess: a new Blockchain-based access control framework for the Internet of Things. Security and Communication Networks, 9(18), pp.5943-5964.
[20] Ali, M., Nelson, J., Shea, R. and J. Freedman, M., 2016. « Blockstack: A Global Naming and Storage System Secured by Blockchains. In: 2016 USENIX Annual Technical Conference (USENIX ATC '16). [online] USENIX. Available at: <https://www.usenix.org/conference/atc16/technical-sessions/presentation/ali> (Accessed 13 December 2021).
[21] Pavithran, D. and Shaalan, K., 2019. Towards Creating Public Key Authentication for IoT Blockchain. 2019 Sixth HCT Information Technology Trends (ITT).
[22] Kalodner, H., Carlsten, M., Ellenbogen, P., Bonneau, J. and Narayanan, A., n.d. An empirical study of Namecoin and lessons for decentralized namespace design. [online] Cs.princeton.edu.Availableat: <https://www.cs.princeton.edu/~arvindn/publications/namespaces.pdf> [Accessed 8 September 2021].
[23] Pinno, O., Gregio, A. and De Bona, L., 2017. ControlChain: Blockchain as a Central Enabler for Access Control Authorizations in the IoT. GLOBECOM 2017 - 2017 IEEE Global Communications Conference.
[24] Alphand, O., Amoretti, M., Claeys, T., Dall'Asta, S., Duda, A., Ferrari, G., Rousseau, F., Tourancheau, B., Veltri, L. and Zanichelli, F., 2018. IoTChain: A blockchain security architecture for the Internet of Things. 2018 IEEE Wireless Communications and Networking Conference (WCNC).
[25] Singh, S., Rathore, S. and Park, J., 2020. BlockIoTIntelligence: A Blockchain-enabled Intelligent IoT Architecture with Artificial Intelligence. Future Generation Computer Systems, 110, pp.721-743.

[26] Lee, S. and Sim, K., 2021. Design and Hardware Implementation of a Simplified DAG-Based Blockchain and New AES-CBC Algorithm for IoT Security. Electronics, 10(9), p.1127.
[27] Madine, M.; Salah, K.; Jayaraman, R.; Al-Hammadi, Y.; Arshad, J.; Yaqoob, I. Application-Level Interoperability for Blockchain Networks. TechRxiv 2021, Preprint. [CrossRef]
[28] Wang, H.; Cen, Y.; Li, X. Blockchain Router: A Cross-Chain Communication Protocol. In Proceedings of the 6th International Conference on Informatics, Environment, Energy and Applications, Jeju, Korea, 29–31 March 2017; pp. 94–97.
[29] Latif, S.; Idrees, Z.; Ahmad, J.; Zheng, L.; Zou, Z. A blockchain-based architecture for secure and trustworthy operations in the industrial Internet of Things. J. Ind. Inf. Integr. 2021, 21, 100190. [CrossRef]
[30] Wu, X.; Liang, J. A blockchain-based trust management method for Internet of Things. Pervasive Mob. Comput. 2021, 72, 101330. [CrossRef]
[31] Fan, Q.; Chen, J.; Deborah, L.J.; Luo, M. A secure and efficient authentication and data sharing scheme for Internet of Things based on blockchain. J. Syst. Archit. 2021, 117, 102112. [CrossRef]
[32] Zhang, H.; Tong, L.; Yu, J.; Lin, J. Blockchain Aided Privacy-Preserving Outsourcing Algorithms of Bilinear Pairings for Internet of Things Devices. arXiv 2021, arXiv:2101.02341. [CrossRef]
[33] Abdelmaboud, A .; Ahmed, A.I.A. ; Abaker, M.; Eisa, T.A.E.; Albasheer, H. ; Ghorashi, S.A.; Karim, F.K.; , (2022) Blockchain for IoT Applications: Taxonomy, Platforms, Recent Advances, challenges and Future Research Directions., Electronics 2022, 11, 630. https://doi.org/10.3390/ electronics11040630.
[34] M. A. Rahman, E. Hassanain, M. M. Rashid, S. J. Barnes, and M. S. Hossain, ‘‘Spatial blockchain-based secure mass screening framework for children with dyslexia,’’ IEEE Access, vol. 6, pp. 61876–61885, 2018.
[35] W. Meng, W. Li, and L. Zhu, ‘‘Enhancing medical smartphone networks via blockchain-based trust management against insider attacks,’’ IEEE Trans. Eng. Manag., vol. 67, no. 4, pp. 1377–1386, Nov. 2020.
[36] K. A. Kumari, R. Padmashani, R. Varsha, and V. Upadhayay, ‘‘Securing Internet of Medical Things (IoMT) using private blockchain network,’’ in Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm. Springer, 2020, pp. 305–326.
[37] N. Dilawar, M. Rizwan, F. Ahmad, and S. Akram, ‘‘Blockchain: Securing Internet of Medical Things (IoMT),’’ Int. J. Adv. Comput. Sci. Appl., vol. 10, no. 1, pp. 82–89, 2019.
[38] A. D. Dwivedi, L. Malina, P. Dzurenda, and G. Srivastava, ‘‘Optimized blockchain model for Internet of Things based healthcare applications,’’ 2019, arXiv:1906.06517. [Online]. Available: http://arxiv. org/abs/1906.06517.
[39] M. Shen, Y. Deng, L. Zhu, X. Du, and N. Guizani, ‘‘Privacy-preserving image retrieval for medical IoT systems: A blockchain-based approach,’’ IEEE Netw., vol. 33, no. 5, pp. 27–33, Sep. 2019.
[40] D. C. Nguyen, K. D. Nguyen, and P. N. Pathirana, ‘‘A mobile cloud based IoMT framework for automated health assessment and management,’’ in Proc. 41st Annu. Int. Conf. IEEE Eng. Med. Biol. Soc. (EMBC), Jul. 2019, pp. 6517–6520.
[41] N. Garg, M. Wazid, A. K. Das, D. P. Singh, J. J. P. C. Rodrigues, and Y. Park, ‘‘BAKMP-IoMT: Design of blockchain enabled authenticated key management protocol for Internet of Medical Things deployment,’’ IEEE Access, vol. 8, pp. 95956–95977, 2020.
[42] D. Polap, G. Srivastava, A. Jolfaei, and R. M. Parizi, ‘‘Blockchain technology and neural networks for the Internet of Medical Things,’’ in Proc. IEEE INFOCOM Conf. Comput. Commun. Workshops (INFOCOM WKSHPS), Jul. 2020, pp. 508–513.
[43] Rachakonda L., Bapatla A. K., Mohanty S. P. and Kougianos E., Sayopillow: A blockchain-enabled, privacy-assured framework for stress detection, prediction and control considering sleeping habits in the IoMT, 2020. Available: arXiv:abs/2007.07377.
[44] Girardi F., De Gennaro G., Colizzi L. and Convertini N., “Improving the healthcare effectiveness: The possible role of EHR, IoMT and blockchain,” Electronics, Vol. 9, no. 6, pp. 884, 2020.
[45] B. A. Y. Alqaralleh, T. Vaiyapuri, V. S. Parvathy, D. Gupta, A. Khanna, and K. Shankar, ‘‘Blockchain-assisted secure image transmission and diagnosis model on Internet of Medical Things environment,’’ Pers. Ubiquitous Comput., pp. 1–11, Feb. 2021, doi: 10.1007/s00779-021-01543-2.
[46] Amanat, A., Rizwan, M., Maple, C., Zikria, Y. B., Almadhor, A. S., & Kim, S. W. (2022). Blockchain and cloud computing-based secure electronic healthcare records storage and sharing. Frontiers in Public Health, 2309.
[47] K. M. Hossein, M. E. Esmaeili, T. Dargahi, and A. Khonsari, ‘‘Blockchain-based privacy-preserving

healthcare architecture,'' in Proc. IEEE Can. Conf. Electr. Comput. Eng. (CCECE), May 2019, pp. 1–4.
[48] H. D. Zubaydi, Y.-W. Chong, K. Ko, S. M. Hanshi, and S. Karuppayah, ''A review on the role of blockchain technology in the healthcare domain,'' Electronics, vol. 8, no. 6, p. 679, Jun. 2019.
[49] J. Xu, K. Xue, S. Li, H. Tian, J. Hong, P. Hong, and N. Yu, ''Healthchain: A blockchain-based privacy preserving scheme for large-scale health data,'' IEEE Internet Things J., vol. 6, no. 5, pp. 8770–8781, Oct. 2019.
[50] V. Malamas, T. Dasaklis, P. Kotzanikolaou, M. Burmester, and S. Katsikas, ''A forensics-by-design management framework for medical devices based on blockchain,'' in Proc. IEEE World Congr. Services (SERVICES), Jul. 2019, pp. 35–40.
[51] G. Srivastava, J. Crichigno, and S. Dhar, ''A light and secure healthcare blockchain for IoT medical devices,'' in Proc. IEEE Can. Conf. Electr. Comput. Eng. (CCECE), May 2019, pp. 1–5.
[52] M. A. Habib, C. M. N. Faisal, S. Sarwar, M. A. Latif, F. Aadil, M. Ahmad, R. Ashraf, and M. Maqsood, ''Privacy-based medical data protection against internal security threats in heterogeneous Internet of Medical Things,'' Int. J. Distrib. Sensor Netw., vol. 15, no. 9, Sep. 2019, Art. no. 155014771987565.
[53] G. Srivastava, R. M. Parizi, A. Dehghantanha, and K.-K. R. Choo, ''Data sharing and privacy for patient IoT devices using blockchain,'' in Proc. Int. Conf. Smart City Informatization. Guangzhou, China: Springer, 2019, pp. 334–348.
[54] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, ''Blockchain for secure EHRs sharing of mobile cloud based E-health systems,'' IEEE Access, vol. 7, pp. 66792–66806, 2019.
[55] H.-N. Dai, M. Imran, and N. Haider, ''Blockchain-enabled Internet of Medical Things to combat COVID-19,'' IEEE Internet Things Mag., vol. 3, no. 3, pp. 52–57, Sep. 2020.
[56] F. Fotopoulos, V. Malamas, T. K. Dasaklis, P. Kotzanikolaou, and C. Douligeris. "A blockchain-enabled architecture for IoMT device authentication," in 2020 IEEE Eurasia Conference on IoT, Communication and Engineering (ECICE), Yunlin, Taiwan, 2020, pp. 89–92.
[57] B. S. Egala, A. K. Pradhan, V. Badarla, and S. P. Mohanty, ''Fortifiedchain: A blockchain-based framework for security and privacy-assured Internet of Medical Things with effective access control,'' IEEE Internet Things J., vol. 8, no. 14, pp. 11717–11731, Jul. 2021.
[58] R. Kumar and R. Tripathi, ''Towards design and implementation of security and privacy framework for Internet of Medical Things (IoMT) by leveraging blockchain and IPFS technology,'' J. Supercomput., pp. 1–40, 2021.
[59] Rana, S. K., Rana, S. K., Nisar, K., Ag Ibrahim, A. A., Rana, A. K., Goyal, N., & Chawla, P. (2022). Blockchain Technology and Artificial Intelligence Based Decentralized Access Control Model to Enable Secure Interoperability for Healthcare. Sustainability, 14(15), 9471.
[60] A. Abbas, R. Alroobaea, M. Krichen, S. Rubaiee, S. Vimal, and F. M. Almansour, ''Blockchain-assisted secured data management framework for health information analysis based on Internet of Medical Things,'' Pers. Ubiquitous Comput., pp. 1–14, Jun. 2021, doi: 10.1007/s00779-021-01583-8.
[61] R. Akkaoui, ''Blockchain for the management of Internet of Things devices in the medical industry,'' IEEE Trans. Eng. Manag., early access, Jul. 29, 2021, doi: 10.1109/TEM.2021.3097117.
[62] Jánoky, L. V., Levendovszky, J., & Ekler, P. (2020). Client Performance Predictions for Private Blockchain Networks. International Journal of Computer Networks & Communications (IJCNC) Vol, 12.
[63] Ferreira, Célio Marcio Soares, et al. "IoT Registration and Authentication in Smart City Applications with Blockchain." Sensors 21.4 (2021): p6.

AUTHORS

Jamal Elhachmi obtained the license in physics in 2004, the research M.S. degree in computer science telecommunication, and multimedia from Mohammed V-Agdal University, Rabat, Morocco, in 2006, received the Ph.D. degree in computer science from EMI School of Engineering, University Mohammed V. Since 2012, he has been an associated member of the research team of Smart Communications—ERSC (formerly known as LEC) as part of the research center in engineering sustainable and smart systems at the EMI School of Engineering, University Mohammed V. He is currently an assistant Professor with the Ecole Nationale Suprieure d'Informatique et d'Analyse des Systemes, Mohammed V University, Rabat, Morocco. His current research interests are Telecommunication, Artificial intelligence (AI), systems

information and communication, intelligent antenna, cognitive radio, mobile computing, mobile social networks, cyber security and blockchain technology.
He can be contacted at email: jamal.elhacimi@ensias.um5.ac.ma.

Abdellatif Kobane (Senior Member, IEEE) received the research M.S. degree in computer science telecommunication, and multimedia from Mohammed V-Agdal University, Rabat, Morocco, in 2003, and the Ph.D. degree in computer science from EMI School of Engineering, Rabat, Morocco, in September 2012. Since 2009, he has been a Full Professor with the Ecole Nationale Suprieure d'Informatique et d'Analyse des Systemes, Mohammed V University, Rabat, Morocco. He is also an Adjunct Professor with L2TI laboratory, Paris 13 University, Villetaneuse, France. His research interests include wireless networking, performance evaluation using advanced technique in game theory, and MDP in wireless mobile network: IoT, SDN, and NFV, 5G networks, resources management in wireless mobile networks, cognitive radio, mobile computing, mobile social networks, caching and backhaul problem, and beyond 5G and future networks.