Blockchain-Based Security for IoMT Edge Networks

Subjects: Computer Science, Information Systems

Contributor: Filippos Pelekoudas-Oikonomou , Georgios Zachos , Maria Papaioannou , Marcus de Ree , José Ribeiro , , Jonathan Rodriguez

Despite the significant benefits that the rise of Internet of Medical Things (IoMT) can bring into citizens' quality of life by enabling IoMT-based healthcare monitoring systems, there is an urgent need for novel security mechanisms to address the pressing security challenges of IoMT edge networks in an effective and efficient manner before they gain the trust of all involved stakeholders and reach their full potential in the market of next generation IoMT-based healthcare monitoring systems. Blockchain technology has been foreseen by the industry and research community as a disruptive technology that can be integrated into novel security solutions for IoMT edge networks, as it can play a significant role in securing IoMT devices and resisting unauthorized access during data transmission.

IoMT blockchain authentication

1. Introduction

The Internet of Things (IoT) technology has emerged and grown rapidly in the last few years, bringing significant benefits to the healthcare sector by transforming the healthcare industry itself and introducing the Internet of Medical Things (IoMT), where medical devices are interconnected in a way that anyone, anywhere, and anytime may have access to [1][2]. The evolution and rise of IoMT can play a noteworthy role in improving citizens' quality of life by enabling IoMT-based healthcare monitoring systems that provide personalized and user-centric healthcare services overcoming constraints such as time and location [3]. Nevertheless, the wide range of different communication technologies (e.g., WLANs, Bluetooth, Zigbee) and types of IoMT devices (e.g., bio sensors, actuators, wireless access points) in IoMT-based healthcare monitoring systems, as well as the fact that the transmission between patients and healthcare providers of personal and confidential healthcare information (e.g., patient's personal details and vital signs) is done through the internet, are factors that raise many security and privacy challenges [4][5][6][7]. Thus, security solutions that meet the fundamental security requirements (i.e., authentication, authorization/access control, data integrity, data confidentiality, and availability) for IoMT-based healthcare monitoring systems are essential for the acceptance and wide adoption of such systems in the coming next years. Nevertheless, the high resource requirements of complex and heavyweight conventional security mechanisms cannot be afforded by resource-constrained IoMT edge networks which constitute the key underlying components of IoMT-based healthcare monitoring systems [2]. In addition, the centralization approach widely adopted by the state-of-the-art security frameworks is not well applicable to IoMT edge networks due to single point of failure issues [8][9][10]. Last but not least, it is worthwhile highlighting that conventional state-of-the-art defence

mechanisms cannot ensure complete tamper-proof systems for protecting IoMT edge networks [5]. Therefore, there is an urgent need for novel security mechanisms to address the pressing security challenges of IoMT edge networks in an effective and efficient manner before they gain the trust of all involved stakeholders and reach their full potential in the healthcare market [4][5].

2. Blockchain-Based Authentication for IoMT Edge Networks

2.1. Existing Blockchain-Based Authentication Mechanisms for IoMT Edge Networks

R. Akkaoui in [11] proposes a scalable authentication scheme for Internet of Medical Things (IoMT) devices based on smart-contracts, leveraging the physical unclonable function (PUF) as an additional authentication factor. PUF is a random unique device identifier based on the physical characteristics of an electronic circuit. The proposed scheme is designed for authentication and firmware update purposes. The authentication scheme is named smart contract against counterfeit IoMT (SCACIoMT). The certificate generation is possible with the use of ECC, and the scheme is implemented in the Ethereum platform.

The architecture of the proposed scheme consists of the following entities: the authorized nodes, which are semi-trusted nodes responsible for mining transactions, with proof of authority (PoA) consensus and block creation. The manufacturer nodes are authorized nodes. They do not perform block creation, but they are responsible for updating the authenticated devices lists. The patients are the final category of entities in the system, which are the data generators, i.e., the entities that create data and forward them to the blockchain as transactions to be sealed into blocks.

Researchers present a detailed workflow of the architecture; however, a brief description of the authentication scheme is presented in the sequence diagram. The device recovers its properties (i.e., ID, PUF, hash firmware) and sends the data together with the Ethereum address as a transaction to the blockchain initiating the authentication. A manufacturer node then initiates a data verification transaction to validate the provided data. Once the data are validated, the manufacturer node notifies the patient and the patient is able to provide medical data. The authorised nodes update the blockchain accordingly as the final step of the authorisation process. The transactions are held by a series of smart contracts.

Researchers has provided a detailed security and performance analysis regarding the implemented scheme in terms of privacy and confidentiality. The scheme is implemented on a privately built Ethereum-based blockchain using the Geth client, running on an Ubuntu virtual machine v 14.04.6 [11] with the following host machine specifications: Intel i3-3110M, 2.4-GHz, 4-GB 1600-MHz DDR3 [11]. The scheme is evaluated regarding computational cost, communication, and storage cost.

Overall, the present research work provides a detailed implementation methodology and evaluation results, as well as a complete design of the scheme and the algorithms of smart contracts, written in Solidity programming

language. Moreover, it provides solid solutions to security issues such as data privacy and information high jacking, and eliminates the single point of failure with a decentralized architecture. On top of that, the user's credibility is important, and it is also taken into consideration as a factor for the system to function properly.

Fotopoulos et al. in [12] proposed a novel IoMT authentication mechanism for patient data collection, process, and storing in a healthcare environment. They include approaches such as self-sovereign identity (SSI), zero knowledge proof, and blockchain to create a decentralized mechanism for effective authentication of medical devices.

2.2. Potential Blockchain-Based Authentication Mechanisms for IoMT Edge Networks

D. Li et al. [13] proposed a blockchain-based authentication mechanism for IoT in order to eliminate the single point of failure. In their proposed research, they point out the necessity of device authentication without the use of a central authority, which is used in the traditional Public Key Infrastructure mechanisms (PKI). Blockchain technology is suitable in architecture and provides the decentralized network structure.

The system model of the proposed architecture consists of a multi-node network and focuses on device registration and storing the hash of each device's information (i.e., ID, public key) in the blockchain ledger. The hashing of this information also provides the benefit of data integrity, as alterations in data can be detected through it. The system operates in the following functions: the enrolment of devices, the identity authentication, and the integrity verification. Nodes of the network function either as consensus nodes which take part in the consensus process, or non-consensus nodes that are used only for data transferring. The role of each node is defined by the needs of the permissioned chain.

The enrolment process is initiated when a certain device communicates a connection request to the network. For a device to be enrolled, a key pair is generated, from which the private key is encrypted and stored in a local storage while the public key is stored in the blockchain ledger. After the consensus process takes place in the consensus nodes, with the use of Practical Byzantine Fault Tolerance (PBFT) algorithm, a block is generated and propagated to all the nodes of the network (i.e., consensus, non-consensus). The identity authentication takes place under a P2P authentication method.

Integrity check of data is also possible through the proposed mechanism. It is accomplished by nodes that periodically communicate a request for integrity verification to their neighboring nodes. In the case of blockchain-based mechanisms, integrity checks are based on the use of hash encryption techniques rather than traditional methods of asymmetric key encryption.

Researchers have moved forward in the implementation of the blockchain-based authentication mechanism with the use of Raspberry Pi devices and the Hyperledger Fabric platform for system deployment. Hyperledger Fabric's nature permits the creation of multiple channels in an ad-hoc network of IoT nodes, and each node can communicate through each of these channels—if permitted—without interference. As a result of the connection of

the nodes through a blockchain network, the interaction between them takes place in the form of transactions that occur inside the network. These transactions are device enrolment, identity authentication, and integrity check. To generate the keys, the Researchers use a cryptographical secure pseudo-random number generator (CSPRNG) that ensures the randomness of the generated key. The stimulation of the CSPRNG originates from information collected from IoT devices such as CPU clock, number of processes, etc.

The proposed research constitutes a complete work with a generic design that can be applicable in many use case scenarios and can be adapted to other specific architectures. It takes advantage of the decentralized nature of the blockchain and the permissioned aspect of Hyperledger Fabric to create a solid design that overcomes the drawbacks of traditional authentication mechanisms, and it is lightweight in implementation which makes it suitable for IoMT edge networks.

Researchers in [14] propose a blockchain-based distributed authentication mechanism to allow communication among devices from various IoT systems. The system architecture is separated into two layers: Device layer and Fog layer. Device layer contains the IoT systems that themselves contain the smart devices, while the Fog layer contains the blockchain network nodes, which are by definition legitimate and trusted. The proposed architecture provides three types of communication: (i) device-to-fog communication, meant for device registration and authentication, (ii) fog-to-fog communication, meant for synchronization of the authentication data with all the blockchain nodes, and (iii) device-to-device communication, which permits the communication between two already authenticated devices.

The authentication process in the proposed mechanism takes place as follows: blockchain nodes (i.e., located at the Fog layer) are connected to one or many IoT systems of the Device layer. Each IoT system chooses an adjacent blockchain node and the registration is taking place between the IoT system and the corresponding node. The system is registered by using a unique System ID (SID), which is generated by the admin of the system. This SID is provided and validated by the blockchain node. Then the SID, if valid, is stored as a transaction in the blockchain, and correspondingly the blocks are propagated to the other blockchain nodes. After the end of the system registration phase, the system admin is provided with a certificate by the blockchain node, which is sent as a transaction in order to proceed to the device registration. For the generation of the certificate, a private key is used. Then, the device registration phase takes place through a similar process with the generation of registration-token certificates. The device authentication is the last phase of this process, where the already registered devices need to be authenticated through the blockchain network. After the authentication process is completed, the blockchain network is used for device communication between systems.

The proposed mechanism comprises a complete and thorough research work. It is evaluated according to the security requirements and against attacks, as well as in terms of execution time and power consumption. It complies with the necessary security requirements such as integrity, non-repudiation, authentication, and regular attack types that may occur in an IoT network. The implementation is done with the aid of Ethereum Blockchain, which is suitable for the implementation of the system. The evaluation provides results, in terms of execution time and power consumption, demonstrating better performance in comparison with the already established state-of-

the-art techniques. In addition, the proposed mechanism provides better scalability capabilities in terms of number of devices and transactions per time unit. Although the proposed authentication approach targets general purpose IoT networks, it could also be a fitting solution for IoMT edge networks due to its lightweight characteristics.

M. T. Hammi et al. at [15] have proposed a decentralized system for device identification and authentication named bubbles of trust. In their proposed work, they divide the network devices into groups, or zones as it is referred to in the manuscript, that communicate with each other. These zones are named as bubbles and the communication inside the zones takes place as blockchain transactions. The architecture is based on a public blockchain, so it is easier for new users to register.

The lifecycle of the architecture begins with the initialization phase. A device is predefined as a Master device. The rest of the devices that participate in the network are Follower Devices. The Master device creates the group identifier and generates tickets—a certificate equivalent—to be provided to Follower devices so they can be enrolled in the system. The ticket contains information regarding the group and data of the Follower device to be enrolled. The Follower devices generate a private/public key pair themselves with Elliptic Curve Cryptography (ECC). After the initialization phase, the lifecycle continues to the creation of the zone in blockchain level. In this phase, the Master initiates a transaction in order to create the group of devices that will take part in the blockchain. Afterwards, the Follower devices initiate transactions in order to enroll into the blockchain, whose identities are checked through a smart contract, and if they are valid then the devices are added to the network. Then, no further authentication process is needed, and the Follower devices are part of the blockchain group where they can communicate inside the bubble through a series of smart contracts that are also validated in the blockchain.

Researchers have preceded the implementation of the architecture with the use of two HP laptops (OS Ubuntu 14.04) [15] and 1 Raspberry Pi (OS Raspbian 4.9.41) [15] as end nodes and the use of Ethereum blockchain as a framework. The interaction between the nodes takes place through Ethereum smart contracts written in Solidity language. Regarding the interaction between the end-nodes and the blockchain, Researchers have implemented a C++ interface that encodes/decodes data toward/from Ethereum. The implementation is performed in the context of the evaluation of the proposed architecture where the evaluation results present considerable durability against IoT network attacks (e.g., DDoS attacks, message replay, spoofing attacks, sybil attacks). In addition, satisfactory results in terms of time and energy consumption, as well as financial costs, were demonstrated.

The Researchers refer to a future work to: (i) evolve the system to allow controlled communication between a chosen set of bubble, (ii) proceed with the implementation of the architecture, and (iii) design a protocol that optimizes the number of the miners that will work in the system. As open issues, they note the fact that the proposed architecture is not adapted to real time applications, has not had an initialization phase—something that was provided in the other related works [13][14] —and is dependent on the evolution of cryptocurrency rate. Overall, it comprises a complete research work for a blockchain-based authentication mechanism and promises to be applicable to different use cases (e.g., smart house, smart factory, waste management). Furthermore, it is worthwhile mentioning that the design characteristics and evaluation results of the proposed system make it a potential authentication solution to enhance security in IoMT edge networks for healthcare monitoring systems.

M. Zhaofeng et al. propose a decentralized blockchain-based authentication scheme in [16] named BlockAuth. In the scheme, each device on the IoT edge layer is considered as a blockchain network node, which acts as a participant in the blockchain. The scheme is fault-reliable and decentralized to eliminate the single point of failure, and also suitable for identity authentication technologies (e.g., password-based, certificate-based, biotechnology-based). The registration phase is covered by a certificate authority that issues the certificates and it is initiated by a user registration request, which is sent as a transaction through a smart contract. Then, in the authentication phase, the identity and the transaction hash are checked by the blockchain in order to verify the identity of the user. The consensus mechanism used in the scheme is a PBFT algorithm.

Researchers move forward to the evaluation of the scheme through a virtual machine environment by implementing the registration, authentication, and consensus algorithms in order to compare the BlockAuth scheme with already implemented related schemes. The results are satisfying with BlochAuth providing advantages in terms of multi-signature identity data, big fault tolerance, and strong security and reliability. On the other hand, the time complexity of the proposed scheme is higher than the others it is compared with. However, despite its high time complexity, the proposed scheme could still be considered as a solution for IoMT edge networks in healthcare monitoring systems, given its decentralized nature, low power consumption, and strong security features.

Researchers in [17] propose a mutual authentication scheme based on blockchain solutions for IoT network, and, specifically, for the use case of smart home, named HomeChain. They integrate blockchain and group signature to provide anonymous authentication inside the IoT network. The proposed scheme uses public key encryption for the generation and distribution of the keys with the use of an ECC algorithm scheme. The group signatures are used for the signing of the transactions that are held inside the blockchain. The proposed scheme uses a permissioned blockchain, and Practical Byzantine Fault Tolerance (PBFT), as a consensus algorithm. The system includes:

- a user that owns a group of IoT/smart devices functioning as a user node
- a blockchain network with consensus nodes, and
- a smart home network that consists of: (i) a group of smart devices, and (ii) a gateway that connects the smart house to the blockchain network.

The implementation of the system has been held on JUICE (an opened permissioned blockchain service platform) and the evaluation results show reliability on various IoT network attacks (e.g., Man-in-the-Middle Attack, Replay attack, DDoS attack) and sufficient performance in terms of time consumption in comparison with other related works. On top of that, researchers s consider the attribute-based cryptographic approach in order to achieve better access control. In principle, its design characteristics and evaluation results make it a potential authentication mechanism to enhance security in IoMT edge networks for healthcare monitoring systems.

Q. Fan et al. in [18] propose an ID-based signature authentication and secure data sharing scheme for IoT. The scheme has been deployed in a three-layer IoT model (i.e., Perception Layer, Network Layer and Application Layer) with the use of a blockchain layer that is also divided into two sublayers—consensus layer and propagation layer. Researchers present detailed algorithms for the different phases of the authentication and the key generation. The scheme has been evaluated and meet the security requirements of an IoT network as well as being resilient to common IoT network attacks and threats. Although the research work provides improved and satisfactory result in the evaluation of the scheme, a particular blockchain platform has not been mentioned to be used for this evaluation. The present research work is in its early stages, since a specific blockchain platform has not been used for the mechanisms to be implemented, however, it is a promising scheme that could be adapted to a healthcare monitoring system, relying on an IoMT edge network.

Researchers in [19] present a blockchain-based multi-WSN (wireless sensor network) authentication scheme for IoT with the use of a private blockchain. To establish the scheme, notable assumptions have been made that can easily be verified:

- each IoT node has a unique Ethernet address
- cluster head nodes and base stations have certain storage and computing capabilities, and smart contract can be deployed
- as a node manager in a single network, base station is trusted by the nodes in the network
- the process of initialization of the nodes is secure

The network model consists of base stations, cluster head nodes, ordinary nodes, and the end user. The authentication working cycle includes an initialization phase and researchers have proceeded into the implementation of the scheme. The scheme provides novelty in terms of the hierarchical multi-WSN network design, the hybrid model of the blockchain, and a mutual authentication scheme for IoT nodes that enhances the scalability of the IoT authentication. The evaluation proves durability of the scheme against IoT network attacks and meets the security requirements of such schemes. Therefore, it could comprise an option for ensuring blockchain-based authentication in IoMT edge networks.

3. Blockchain-Based Authorization for IoMT Edge Networks

Ronghua Xu et al. [20] highlighted that access authorization comprise one of the top security and privacy challenges that IoT has to address for its wide adoption in order to ensure secure resource and information sharing. They discuss that the centralized authorization server of traditional access control (AC) may be the single point of failure or the performance bottleneck. Towards the direction, researchers designed and developed a prototype of a capability-based decentralized mechanism (BlendCAC) using Blockchain technology which uses token management for various actions (e.g., permissions or revocations on access authorization) making the

authorization decision. Capability-based access control is an access control model commonly used in the distributed architectures, where the access control logic is embedded and distributed into the end devices and not into a central authority [20][21][22][23]. These devices, also referred to as “smart things” or “smart objects” [23], are being enabled with capabilities that make them able to obtain, process, and send information about the access control rights of the entities of the system to other entities and/or services [23]. Thereby, the “smart things” are able to carry out the authorization process, without requiring a central authority.

The aim of the proposed BLockchain-ENabled Decentralized Capability-based Access Control or BlendCAC, is the facilitation of effective access control processes for devices, services, and information in large-scale IoT systems [20]. Based on the blockchain network, researchers propose a capability delegation mechanism for access permission propagation. On top of that, the mechanism takes advantage of a smart contract for registration, propagation, and revocation of the access authorization, creating a robust identity-based capability token management strategy. In the proposed BlendCAC scheme, IoT devices are not overseen by a centralized authority. On the contrary, they are their own master to control their resources, which is the main idea of capability-based systems. The proposed BlendCAC system architecture is illustrated under the use case scenario of two isolated IoT-based service domains without pre-establishing a trust relationship between them. Each domain has a domain owner which has the ownership of several IoT devices, and thus it is able to enforce predefined security policies to manage all the domain related devices and subsequent services. At this point, it is important to observe that, essentially, every domain involves a domain owner which, after all, is a centralized entity; this might cause issues such as single point of failure, bottleneck, performance degradation, etc. similarly to centralized approaches. Finally, every domain owner maintains a local chain with the transactions that happened in their domain, which then must be periodically synchronized with the global Blockchain.

Researchers implemented and tested their proposed scheme on a local private blockchain network, using devices such as Raspberry Pi and laptops/desktops. Their experimental results showed the feasibility of BlendCAC to offer a lightweight, scalable, decentralized, and fine-grained access control solution for large-scale IoT systems.

In [22], the researchers examined the BlendCAC scheme [23], identified its limitations, and tried to address them. In particular, they pointed out that in BlendCAC, a subject cannot obtain rights from more than one subject. This is because the BlendCAC scheme manages the capabilities of subjects and their delegation relationships with each object by using a delegation tree. If subject A is the parent of subjects B and C, then subject A can give access rights to subjects B and C for the objects that belong to subject A. However, subject B, as it is not actually the parent of subject C, is not able to give any access rights to subject C for the objects that belong to subject B. In addition, to complete a delegation, the related tokens, namely ICap and IDC tokens, must be updated synchronously. This requirement is not always feasible to be fulfilled in the blockchain system, taking into consideration the difference of the times when the two transactions for updating the tokens are included into the blockchain.

Therefore, researchers in [22] proposed a novel smart contract-based CapBAC scheme enabled with more flexible capability delegation and more fine-grained capability management in order to deal with the limitations of the

BlendCAC scheme. More specifically, the researchers firstly define the capability tokens in units of authorized actions. In this way, they achieve having one token per action rather than one token per subject, as it is in the BlendCAC scheme. To address the second limitation, researchers introduce the usage of one single type of token to summarize the information of capabilities and delegation relationship so as to be feasible to update this information simultaneously when needed. On top of that, to enable more flexible capability delegation, researchers manage the delegation relationship of the different subjects by a delegation graph as opposed to the delegation tree introduced in the BlendCAC scheme. Their novel proposed scheme also supports the functionality of adding new authorized actions, which is not possible in the BlendCAC scheme.

Overall, researchers in [22] propose a Capability-Based Access Control (CapBAC) scheme by applying the emerging Ethereum blockchain technology. Their scheme makes use of Ethereum smart contracts (i.e., executable codes residing in the blockchain) to store and manage the capability tokens (i.e., special data structures that define the permitted actions of a user, also referred to as subject, on a certain resource, and also referred to as object). Their scheme provides more fine-grained access control and more flexible token management, defining capability tokens in units of actions. On top of that, for storing the token delegation relationship among the different subjects, they deploy a delegation graph. Most of the existing smart contract-based CapBAC schemes use the delegation tree, including the BlendCAC. Their scheme enables object owners with the capability to verify the ownership and validity of the capability tokens of the subjects by storing the tokens and the delegation graph in smart contracts. Finally, researchers constructed a local Ethereum blockchain network and conducted extensive experiments demonstrating the feasibility of the proposed scheme large-scale and trustless nature of the Internet of Things (IoT), showing promising results for its deployment in IoT-based Healthcare applications. In this regard, this Capability-Based Access Control (CapBAC) scheme shows potential applicability in the IoMT edge networks.

In [24], researchers combine the blockchain smart contract technology and the attribute-based access control (ABAC) model and propose a novel distributed and reliable access control framework for smart cities. It is important to highlight that ABAC refers “to an access control approach in which access is mediated based on attributes associated with subjects (requesters) and the objects to be accessed” [25]. In particular, each object and subject are associated with a set of attributes, such as time of creation, location, access rights, etc., and the access to an object is then authorized/denied depending upon whether the required (e.g., policy-defined) correlation can be made between the attributes of that particular object and of the requesting subject.

The proposed framework consists of:

- a Policy Management Contract (PMC) that is responsible for managing the ABAC policies
- a Subject Attribute Management Contract (SAMC) that is responsible for managing the attributes of subjects (i.e., entities gaining access to resources/objects)
- an Object Attribute Management Contract (OAMC) that is responsible for managing the attributes of objects (i.e., resources being accessed), and

- an Access Control Contract (ACC) that is responsible for performing the access control.

Researchers construct a local private Ethereum blockchain system in order to deploy the four smart contracts, conduct extensive experiments to evaluate the monetary cost and, finally, compare the performance evaluation of the proposed framework with existing access control list (ACL)-based scheme. The experimental results showed feasibility of the integration of the proposed framework in large-scale IoT environments, making it a promising potential solution for the IoMT edge networks in IoMT-based healthcare monitoring systems. Although the proposed framework introduces a larger deployment cost at the deployment stage, compared to other ACL-based schemes, it introduces less monetary cost during the system running, especially for large-scale IoT systems consisting of a large number of subjects and objects with common attributes. Smart cities comprise a typical example of such systems. However, although the prototype demonstrates the feasibility of the proposed framework, it can hardly reflect the performance of the framework in large-scale IoT applications such as smart manufacturing or healthcare.

Apart from the monetary cost, another major concern of the proposed ABAC framework in [24] is the throughput issue. In particular, this concern refers to the total number of access requests that can be processed per unit time (e.g., second). The throughput of the proposed framework depends greatly on the throughput of the underlying blockchain systems (i.e., number of transactions included in the blockchain per second). In their implementation, Researchers deployed Ethereum 1.0 as the underlying blockchain system, the throughput of which is about 15 transactions per second [26]. Additionally, further latency is introduced to the access control process, reducing the throughput of the framework since the ACC (i.e., access request processing unit) needs to communicate with other contracts through messages. Actually, the consensus algorithm is one of the main reasons for the throughput being low. Their implementation is based on the widely used Proof-of-Work (PoW) algorithm, which involves a vast number of calculations to add one block of transactions into the blockchain. Researchers also highlight that Ethereum 2.0 comprises a promising solution, which changes the consensus algorithm from PoW to Proof of Stake (PoS) and adopts the method of sharing to greatly enhance the throughput performance [27]. It is expected that Ethereum 2.0 will enable 64 to several hundred times more throughput than Ethereum 1.0.

References

1. Oikonomou, F.P.; Pelekoudas; Ribeiro, J.; Mantas, G.; Bastos, J.M.C.S.; Rodriguez, J. A Hyperledger Fabric-based Blockchain Architecture to Secure IoT-based Health Monitoring Systems. In Proceedings of the 2021 IEEE International Mediterranean Conference on Communications and Networking (MeditCom), Athens, Greece, 7–10 September 2021.
2. Oikonomou, F.P.; Mantas, G.; Cox, P.; Bashashi, F.; Gil-Castineira, F.; Gonzalez, J. A Blockchain-based Architecture for Secure IoT-based Health Monitoring Systems. In Proceedings of the IEEE 26th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), Porto, Portugal, 25–27 October 2021; pp. 1–6.

3. Papaioannou, M.; Karageorgou, M.; Mantas, G.; Sucasas, V.; Essop, I.; Rodriguez, J.; Lymberopoulos, D. A Survey on Security Threats and Countermeasures in Internet of Medical Things (IoMT). Trans. Emerg. Telecommun. Technol. 2020, 23, e4049.
4. Gope, P.; Hwang, T. BSN-Care: A Secure IoT-Based Modern Healthcare System Using Body Sensor Network. IEEE Sensors J. 2015, 16, 1368–1376.
5. Khezr, S.; Moniruzzaman, M.; Yassine, A.; Benlamri, R. Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research. Appl. Sci. 2019, 9, 1736.
6. Makhdoom, I.; Abolhasan, M.; Lipman, J.; Liu, R.P.; Ni, W. Anatomy of Threats to the Internet of Things. IEEE Commun. Surv. Tutor. 2019, 21, 1636–1675.
7. Neshenko, N.; Bou-Harb, E.; Crichigno, J.; Kaddoum, G.; Ghani, N. Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations. IEEE Commun. Surv. Tutor. 2019, 21, 2702–2733.
8. Seliem, M.; Elgazzar, K. BIoMT: Blockchain for the internet of medical things. In Proceedings of the 2019 IEEE International Black Sea Conference on Communications and Networking, BlackSeaCom, Sochi, Russia, 3–6 June 2019.
9. Sicari, S.; Rizzardi, A.; Grieco, L.A.; Coen-Porisini, A. Security, privacy and trust in Internet of Things: The road ahead. Comput. Netw. 2015, 76, 146–164.
10. Catarinucci, L.; De Donno, D.; Mainetti, L.; Palano, L.; Patrono, L.; Stefanizzi, M.L.; Tarricone, L. An IoT-Aware Architecture for Smart Healthcare Systems. IEEE Internet Things J. 2015, 2, 515–526.
11. Akkaoui, R. Blockchain for the Management of Internet of Things Devices in the Medical Industry. IEEE Trans. Eng. Manag. 2021, 1–12.
12. Fotopoulos, F.; Malamas, V.; Dasaklis, T.K.; Kotzanikolaou, P.; Douligeris, C. A Blockchain-enabled Architecture for IoMT Device Authentication. In Proceedings of the 2020 IEEE Eurasia Conference on IOT, Communication and Engineering (ECICE), Yunlin, Taiwan, 23–25 October 2020.
13. Li, D.; Peng, W.; Deng, W.; Gai, F. A Blockchain-Based Authentication and Security Mechanism for IoT. In Proceedings of the 27th International Conference on Computer Communication and Networks (ICCCN 2018), Hangzhou, China, 30 July—2 August 2018; pp. 1–6.
14. Khalid, U.; Asim, M.; Baker, T.; Hung, P.C.K.; Tariq, M.A.; Rafferty, L. A decentralized lightweight blockchain-based authentication mechanism for IoT systems. Clust. Comput. 2020, 23, 2067–2087.
15. Hammi, M.T.; Hammi, B.; Bellot, P.; Serhrouchni, A. Bubbles of Trust: A decentralized blockchain-based authentication system for IoT. Comput. Secur. 2018, 78, 126–142.

16. Zhaofeng, M.; Jialin, M.; Jihui, W.; Zhiguang, S. Blockchain-Based Decentralized Authentication Modeling Scheme in Edge and IoT Environment. IEEE Internet Things J. 2021, 8, 2116–2123.
17. Lin, C.; He, D.; Kumar, N.; Huang, X.; Vijayakumar, P.; Choo, K.-K.R. HomeChain: A Blockchain-Based Secure Mutual Authentication System for Smart Homes. IEEE Internet Things J. 2020, 7, 818–829.
18. 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. Arch. 2021, 117, 102112.
19. Cui, Z.; Xue, F.; Zhang, S.; Cai, X.; Cao, Y.; Zhang, W.; Chen, J. A Hybrid BlockChain-Based Identity Authentication Scheme for Multi-WSN. IEEE Trans. Serv. Comput. 2020, 13, 241–251.
20. Xu, R.; Yu, C.; Blasch, E.; Chen, G. Blendcac: A Blockchain-Enabled Decentralized Capability-Based Access Control for Iots. In Proceedings of the IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 30 July–3 August 2018; pp. 1027–1034.
21. Gusmeroli, S.; Piccione, S.; Rotondi, D. A capability-based security approach to manage access control in the internet of things. Math. Comput. Model. 2013, 58, 1189–1205.
22. Nakamura, Y.; Zhang, Y.; Sasabe, M.; Kasahara, S. Capability-based access control for the internet of things: An ethereum blockchain-based scheme. In Proceedings of the 2019 IEEE Global Communications Conference (GLOBECOM), Waikoloa, HI, USA, 9–13 December 2019.
23. Hernández-Ramos, J.L.; Jara, A.J.; Marin, L.; Skarmeta, A.F. Distributed capability-based access control for the internet of things. J. Internet Serv. Inf. Secur. 2013, 3, 1–16.
24. Zhang, Y.; Yutaka, M.; Sasabe, M.; Kasahara, S. Attribute-Based Access Control for Smart Cities: A Smart-Contract-Driven Framework. IEEE Internet Things J. 2020, 8, 6372–6384.
25. Hu, V.C.; Ferraiolo, D.; Kuhn, R.; Schnitzer, A.; Sandlin, K.; Miller, R.; Scarfone, K. Guide to Attribute Based Access Control (ABAC) Definition and Considerations. Publication 2014, 800, 1–54.
26. Sharding-FAQs|Ethereum Wiki. Available online: https://eth.wiki/sharding/Sharding-FAQs (accessed on 25 January 2022).
27. Ethereum 2.0 FAQ|ConsenSys. Available online: https://consensys.net/knowledge-base/ethereum-2/faq (accessed on 25 January 2022).