A Blockchain-based Architecture for Secure IoT-based Health Monitoring Systems

Filippos Pelekoudas Oikonomou
Evotel Informática S.A., Spain
Faculty of Engineering and Science, University of Greenwich
Chatham Maritime, UK
filippos@evotel-info.comt

Georgios Mantas
Faculty of Engineering and Science, University of Greenwich
Chatham Maritime, UK
g.mantas@gre.ac.uk

Phil Cox
Faculty of Engineering and Science, University of Greenwich
Chatham Maritime, UK
p.w.cox@gre.ac.uk

Firooz Bashashi
Evotel Informática S.A., Spain
firooz@evotel-info.com

Felipe Gil-Castiñeira
Universidade de Vigo, Vigo, Spain
xil@gti.uvigo.es

Jonathan Gonzalez
Evotel Informática S.A., Spain
jgonzalez@evotel-info.com

***Abstract*— Although IoT technology brings significant benefits to the healthcare sector and can play a noteworthy role in improving citizens' quality of life by enabling IoT-based health monitoring systems, it also raises many security challenges. Conventional security mechanisms are inadequate to secure IoT-based health monitoring systems as they have high resource requirements, in terms of computational power and energy consumption, and thus they cannot be afforded by the resource-constrained IoT nodes of these systems. On the other hand, blockchain is a promising technology that can be used to enhance the security of IoT-based health monitoring systems due to its decentralized and autonomous nature. Therefore, in this paper, we propose a blockchain architecture, based on the Hyperledger Fabric platform, for securing IoT-based health monitoring systems in a more lightweight manner as Hyperledger Fabric does not apply the consensus protocol of Proof of Work (PoW) that cannot be afforded by IoT devices.**

Keywords—IoT security, blockchain, Hyperledger Fabric, Healthcare

I. INTRODUCTION

Given that healthcare is a part of human life of outmost importance [1], technology has given an effort to provide better healthcare solutions to improve the prevention and treatment of illnesses [2]. Internet of Things (IoT) is a technology that has provided benefits in the healthcare domain and has increased the quality of healthcare services that leads to improvement of quality of human life. This has been succeeded by enabling IoT-based health monitoring systems that grant healthcare services, specifically adjusted to the needs of the patient and by eliminating restrictions such as time and location [3], [4], [5]. Although this technology provides advantages, it causes issues of concern in terms of security, because of the different types of communication protocols that are used (e.g., Bluetooth, ZigBee), the resource-constrained IoT devices (e.g., medical sensors), embedded in the IoT-based health monitoring systems [6], [7], and finally because of the sensitive nature of the data they transmit. Although security solutions do exist, their high resource requirements, in terms of computational power and energy consumption, cannot be afforded by the resource-constrained IoT nodes.

A technology that has recently been used to address security issues and provide novel security solutions to IoT-based healthcare systems is the technology of Blockchain. Blockchain is becoming very popular in adoption, as it is applicable in many security aspects in the healthcare sector (e.g., secure healthcare data storage, secure medical supply chain) [8], [9], [10]. Especially, in the age of Covid-19, decentralization and immediate secure sharing of medical information is critical [11]. Moreover, Blockchain technology, given its decentralized and autonomous nature, can enable the IoT devices to transmit data to each other in a secure manner [12]. Nevertheless, despite the significant benefits that blockchain technology brings into current centralized IoT-based healthcare systems so as to address their security challenges, the resource-constrained IoT devices of these systems cannot afford complex and heavyweight operations (e.g., Proof of Work (PoW)) due to their limited processing power, storage capacity, and battery life [13], [14].

Therefore, in this paper, we propose a blockchain architecture, based on the Hyperledger Fabric platform and consisting of two Blockchain networks, for securing IoT-based health monitoring systems in a more lightweight manner and present a detailed transaction flow of our architecture. In particular, Hyperledger Fabric [15] is an open-source system for deploying and operating blockchains without applying the consensus protocol of Proof of Work (PoW) that cannot be afforded by IoT devices in systems, such as IoT-based health monitoring systems, due to their limited processing power, storage capacity, and battery life. Apart from the fact that the Hyperledger Fabric can enable a more lightweight security architecture for IoT-based health monitoring systems, it also allows the building of permissioned blockchains which is another significant requirement for IoT-based health monitoring systems

This research work has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 876487. The JU receives support from the European Union's Horizon 2020 research and innovation programme and Finland, Spain, Italy, Germany, Czech Republic, Belgium, Netherlands".

Following this introduction, we organise the paper as follows. In section II, we give a brief overview of: a) the function of Hyperledger Fabric, b) recent blockchain-based architectures, and c) Hyperledger Fabric-based architectures for IoT systems. In section III, we present the proposed blockchain-based architecture along with its main system components. In section IV, we present how the proposed architecture functions and how a transaction is handled. In paragraph V, we summarise our current status in terms of implementation. Finally, section VI concludes the paper.

II. Related Work

In this section we give a brief overview of the functionality of Hyperledger Fabric, recent blockchain-based architectures for IoT systems, and Hyperledger Fabric-based architectures for IoT systems.

A. Blockchain - Based Architectures

Dorri et al. [16] present in their work an architecture based on a smart home model. They describe an overlay network consisted of smart homes, service providers, cloud storages and personal computers that operates with Blockchain technology and they introduce the concept of local miner and the Local Blockchain. Although, the work follows the classic example of a Miner-based blockchain, the concept of Proof of Work (PoW) and the need of coins for the Blockchain to function, are eliminated.

Authors in [1] reduce the limitations of Blockchain when implemented in IoT (e.g., high power consumption, computational cost), by introducing a privacy preserving scheme on an overlay decentralised network. Followingly authors in [17], focus on the integration of Blockchain in health-care application. They propose a security scheme where the IoT networks are arranged in clusters and each cluster is led by a cluster head. The cluster head reduces delays and overhead in other nodes.

S. Biswas et al. in [11], propose an architecture that uses Blockchain to interconnect the global healthcare system with the suggestion of an international architecture. The need of a global healthcare system has emerged also by the pandemic of COVID-19. They provide the benefits of this architecture and address the challenges of its implementation.

Authors in [18] use Ethereum Blockchain, and exploit the function of smart contracts, to secure medical data transmission and process, in a timely manner, by updating constantly participants in the chain about requirements, medical information, or test updates, regarding the COVID-19. The proposed solution establishes trust and eliminates the possibility of deceitful transactions or certificates.

B. Hyperledger Fabric

E. Androulaki et al. have described Hyperledger Fabric in [15]. It operates in an execute-order-validate architecture which differs from the regular order-execute one that is commonly used in other blockchains. This way the transaction flow in Hyperledger Fabric is separated in three steps, which are briefly explained as follows and depicted in Figure 1:

1. *Executing a transaction and checking its correctness:* Transactions are issued to the peers to be endorsed according to a specified endorsement policy. Afterwards, the execution of the transaction by specific peers takes place, concluding the step of endorsement. This step corresponds to "transaction validation" in other blockchains.
2. *Ordering through a consensus protocol, regardless of the nature of the transactions*: The ordered sequence of the transactions grouped in blocks is a result of the ordering step which takes place with the aid of a pluggable consensus protocol.
3. *Validating the transaction according to trust assumptions*: The final step is the propagation of the results of the ordering process to the peers where the transactions are validated in the same order and in a deterministic way.

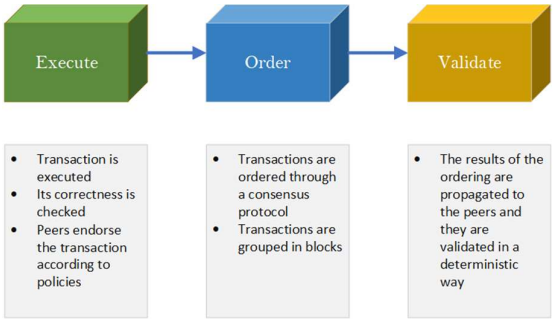

Fig. 1 Execute – Order – Validate architecture

C. Hyperledger Fabric-based Architectures

O. Attia et al. in [19] have proposed a Hyperledger framework focused on distributed technology suitable for IoT networks, which along with previous works [16], [20]eliminates the concept of PoW. In this paper, authors also introduce the term Medical Devices Blockchain as a mechanism to ensure trust among IoT devices.

S. Biswas et al. [21] propose an architecture with the use of Hyperledger Fabric for a permissioned Blockchain for IoT. The architecture follows a design that integrates Hyperledger Fabric, using its functionalities such as Certification Authority (CA) and a local peer that is used as an endorser or validator.

Authors in [14] and in [12] propose a Hyperledger Fabric-based architecture for Blockchain implementation. The architecture introduces a Multi-layer Blockchain Network for IoT with a Local Blockchain scheme that connects different gateways of IoT systems with Base stations and a Global Blockchain and acts as an interconnection networks between them. The authors have implemented their architecture on a VM and with the use of Raspberry Pi and its performance has been evaluated.

In our previous work [22], we proposed a Hyperledger Fabric-based architecture to secure IoT-based health monitoring systems and reduce the storage limitation of IoT devices. We introduced the Reset transaction that transfers Local Blockchain's data off-chain and transfer its hash to a Global Blockchain, decreasing the necessary storage. In this current research we analyse further the interaction between the components and the transaction lifecycles in the Local and Global Blockchain.

III. Proposed Blockchain-based Architecture

The proposed architecture consists of two Blockchain networks: a) a Local one that is a single node (i.e., peer) Blockchain embedded in the Perception Domain (i.e., IoT edge network), and b) a Global one that connects each Perception Domain to a Blockchain (i.e., Global Blockchain) that secures data transfer and data integrity outside the Perception Domain. Our goal is to create an architecture that can be scalable for future connection with other Blockchain systems (e.g., a blockchain network consisted of multiple healthcare providers, or to a health information management system).

A. Local Blockchain - A single node Blockchain

As described in our previous work in [22], a Local Blockchain (LB) is responsible for the security of the transactions that occur inside the IoT network of the Perception Domain, while the Global Blockchain (GB) is deployed in multiple Perception Domains and participating Healthcare providers in order to handle the transactions taking place among them.

The design of the Local Blockchain (LB) in the Perception Domain can be perceived as equivalent to the Cluster architecture proposed in multiple research works such as in [12], [14], and [16], or the overlay network proposed in [1] and [17] with the gateway as a Cluster Head. We need to make clear that the purpose of a single node Blockchain is to cover the need of energy preservation by minimizing the communication distance [12] and the delay of information transfer elicited by the Blockchain consensus delay.

B. Global Blockchain – A multiple node Blockchain

The purpose of GB is to interconnect the Perception Domains with Healthcare Providers and to give them the ability to interact with each other. The Blockchain-based nature of the architecture permits an easy decentralized way of secure communications, providing accountability and eliminating the single point of failure; while at the same time facilitate the storage handling of the Gateways at the Perception Domains. In addition, in GB, a Global Ledger exists and stores the transactions between the stakeholders that take place in the network.

C. System Architecture Components

The proposed blockchain-based architecture consists of the following main components:

Perception Domain: It is part of an IoT-based health monitoring system and interacts with objects (e.g., physical things) through the IoT devices (e.g., sensors, actuators, etc.) of the IoT edge network. This domain aims to connect things into IoT edge network, and to measure, gather and handle the information provided by these things (e.g., patient's body, patient's home environment) through IoT devices (e.g., sensors).

Gateway: It is located at the Perception Domain and is responsible to transmit the gathered information outside the Perception domain (i.e., telecommunication network, Cloud). It contains the Peer and the Local Orderer which are responsible for the functionality of the LB. In the LB the Peer component has the ability to endorse and validate the transactions that are proposed from the sensors while the Local Orderer orders these transactions. This architecture can be described also as a one-node Blockchain. Peer can endorse and validate transactions that are taking place in the GB. Gateway can also function as a Client when it needs to make transactions proposals to the Global Blockchain. The role of the Gateway can be addressed either to the user's smartphone or a specific device with the necessary sub-components embedded in it.

Bio-sensors and context-aware sensors: They are located also inside the Perception Domain and are responsible to gather the vital signs of the user-patient (e.g., blood pressure, body temperature, electrocardiogram) and context information from the user-patient environment (e.g., air pressure, humidity, sound, etc.). Perception domain's sensors are the Clients of LB submitting transaction proposals for execution to Endorser located in the Gateway.

Global Ordering Service (GOS): It is a network of Orderers, trusted from all the participants in the GB network and registered to the Certification Authority of the proposed architecture. GOS orders the transactions originating from all the Perception Domain Gateways that are part of GB.

Ledger: It is a tamper-proof database that stores the transactions. The Gateway, through the Peer, has permission to read/write on the ledger. Ledger data cannot be altered or deleted. It can be separated in two entities, Global and Local Ledger, Global Ledger stores the blocks of transactions that are taking place in the GB while Local Ledger stores the block of transactions that are taking place in LB, in a Perception Domain.

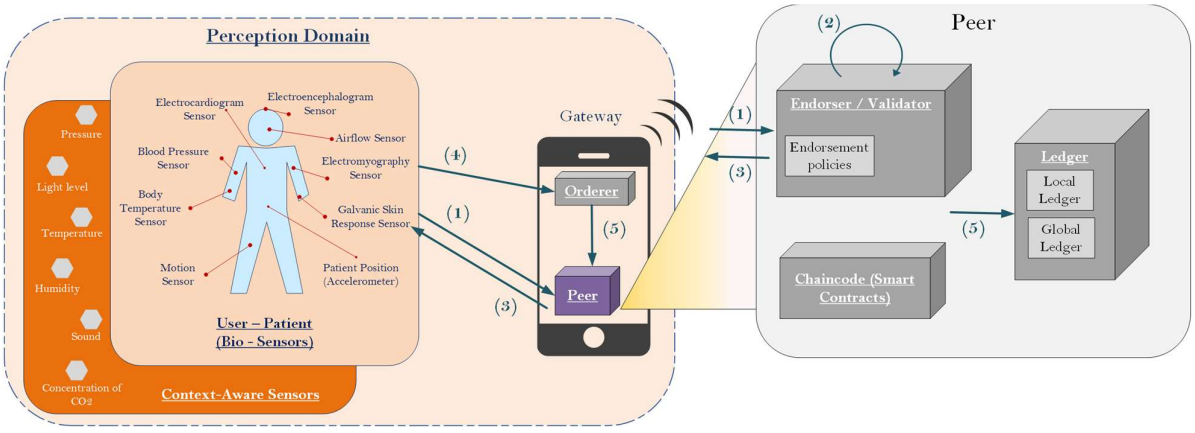

Fig. 2 Transaction Lifecycle in Local Blockchain

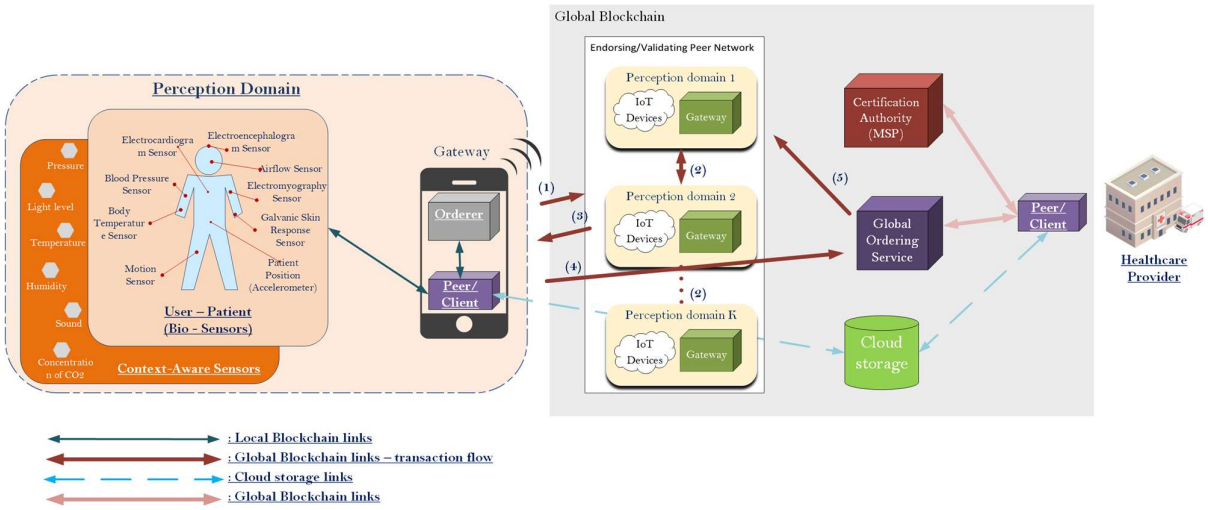

Fig. 3 Transaction Lifecycle in Global Blockchain

Certification Authority (CA): It contains the identities of the Peers, Orderers, and Clients (i.e., Perception Domain sensors). It is the equivalent to the Membership Service Provider (MSP) of the Hyperledger Fabric. It issues certificates and credentials for the purpose of authentication and authorization of the nodes (i.e., clients, peers, and orderers) [15].

Cloud Storage: This part of the architecture keeps the data (i.e., sensing data, and state data of Local Ledger after Reset[22]) stored off-chain. Healthcare Providers, via Peer/Client devices, request access to the cloud storage data in order to read or process them. Data access and modification by the Healthcare Providers require authorization and are recorded as transactions inside the GB.

IV. Operation of the Proposed Blockchain-based Architecture

In this section, after we defined the LB and GB as well as the system components, we are going to present how our proposed architecture functions and how a transaction is handled, from the perspective of the LB and the GB.

A. Local Blockchain Operation

The steps of the transaction lifecycle inside the LB are the following, as also depicted in Figure 2:

1. Initially, a sensor captures the sensing data of the feature that it monitors. A Client located in the sensor makes a transaction proposal to the Peer (i.e., Endorser) located in the Gateway of the Perception Domain in order to confirm the origin of the data.
2. The Peer component (i.e., Endorser) of the Gateway receives the proposal and endorses it if the proposal is valid, according to a pre-specified endorsement policy that is satisfied by only one endorsing Peer.
3. After the Peer (i.e., Endorser) endorses the transaction proposal, it returns the endorsement along with the metadata to the Client.
4. The Client then creates the transaction and sends it to the Orderer component of the Gateway for ordering.
5. After the ordering process is completed and the block is created, the Orderer sends the new block to be validated in the Peer component (i.e., Validator). If the transactions in the block are valid then the block is appended to the Local Ledger. Finally, the LB's state is updated.

B. Global Blockchain Operation

The steps of the transaction lifecycle inside the GB are the following, as also depicted in Figure 3:

1. After a certain amount of sensing data being collected, the Client of the Gateway initiates a transaction proposal to send the collected data to the Cloud Storage where they can be stored, analyzed and accessed by a Healthcare Provider any time.
2. This transaction proposal will be endorsed by Peers located in other Endorsing Peer Network depending on the pre-defined endorsement policy.
3. Then the Client inside the Gateway gathers the necessary endorsements from the endorsing Peers in the Endorsing Peer Network of the GB.
4. When the endorsements are collected, the transaction will be created and sent, by the Client, to the Global Ordering Service to be ordered.
5. After the ordering, the block created by the Global Ordering Service is returned to the Validating Peer Network to be validated and committed, in the GB. The Peers which validate the block of transactions are not the same as the Endorsing peers per se.

C. Healthcare Provider Transactions in Global Blockchain

In this part we describe, as shown in Figure 4, the process of a transaction proposed by a Healthcare Provider,

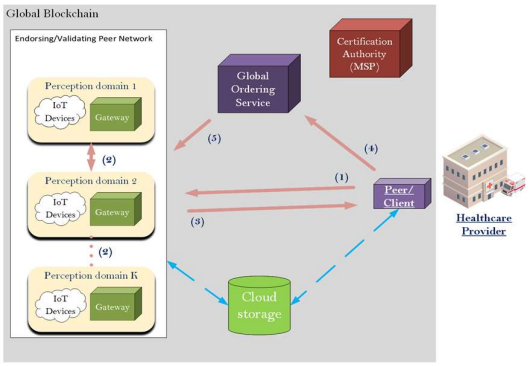

Fig. 4 Healthcare Provider's Transaction Lifecycle in Global Blockchain

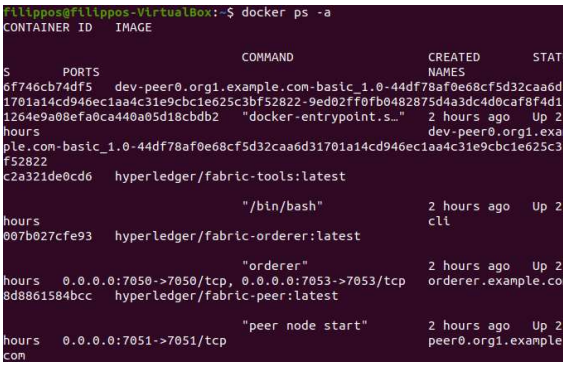

Fig. 5 Docker Container of Hyperledger Fabric with one Peer, one Orderer

via Peer/Client devices, in order to access, retrieve and/or process patient's sensing data from the Cloud Storage.

1. Initially, the Healthcare Provider makes a transaction proposal to access data, which is created by their and sent to the Endorsing Peer Network for endorsement.
2. The Peers in the Endorsing Peer Network receive the transaction proposal and endorse it according to the endorsement policies.
3. The Endorsing Peer Network sends back to the Client the necessary endorsements.
4. The Client sends the transaction to the GOS for the ordering process.
5. The GOS orders the transaction and forms a block of transaction which is propagated to the Validating Peer Network, to be validated and then committed in the GB.

After this process takes place, the Healthcare Provider is able to access, retrieve and/or process the chosen data from the Cloud Storage.

V. Implementation

To evaluate the functionality and the performance of the proposed architecture, we have been implementing it with Hyperledger Fabric release 2.2 on a virtual machine. For the virtual environment we used Ubuntu 18.1 on Oracle VM Virtual Box with 8 GB RAM and Intel(R) Core(TM) I5-1035G1 CPU @ 1.19 GHz. Hyperledger Fabric release 2.2 provides a platform ready for testing chaincodes.

Due to the complexity of the Hyperledger Fabric platform, we started the implementation phase of the proposed architecture by testing a specific single node network equivalent to our LB architecture. In order to proceed with the implementation, we modified the code provided by Hyperledger Fabric so it could fit to our scenario. In particular, we have created a node network on the Hyperledger Fabric platform with one Peer node and one Orderer that resembles the architecture of LB. The node network is deployed on our VM, and it runs on a Docker container, as shown in Figure 5.

VI. Conclusion & Future Work

In this work we proposed a Blockchain-based architecture consisting of i) a LB for each Perception Domain of an IoT-based health monitoring system, and ii) a GB interconnecting the LBs of the Perception Domains and Healthcare Providers. The LB of each Perception Domain is responsible to secure the transactions taking place into the given Perception Domain, and the GB aims at i) facilitating decentralized accountability, and ii) eliminating single point of failure, while at the same time ensuring data integrity, availability, and non-repudiation at the global level. Furthermore, we have presented how the proposed architecture functions and how a transaction is handled, from the perspective of the LB and the GB. As future work, we aim to move forward with the implementation of the proposed architecture in a virtual environment and evaluate it in terms of performance metrics such as transaction throughput, resource consumption, communication overhead and latency.

References

[1] A. D. Dwivedi, G. Srivastava, S. Dhar, and R. Singh, "A decentralized privacy-preserving healthcare blockchain for IoT," *Sensors (Switzerland)*, vol. 19, no. 2, pp. 1–17, 2019, doi: 10.3390/s19020326.

[2] L. Zhang, M. Peng, W. Wang, Y. Su, S. Cui, and S. Kim, "Secure and efficient data storage and sharing scheme based on double blockchain," *Comput. Mater. Contin.*, vol. 66, no. 1, pp. 499–515, 2021, doi: 10.32604/cmc.2020.012205.

[3] M. Papaioannou *et al.*, "A Survey on Security Threats and Countermeasures in Internet of Medical Things (IoMT)," *Trans. Emerg. Telecommun. Technol.*, 2020, doi: 10.1002/ett.4049.

[4] J. J. P. C. Rodrigues *et al.*, "Enabling Technologies for the Internet of Health Things," *IEEE Access*, 2018, doi: 10.1109/ACCESS.2017.2789329.

[5] M. Neyja, S. Mumtaz, K. M. S. Huq, S. A. Busari, J. Rodriguez, and Z. Zhou, "An IoT-based e-health monitoring system using ECG signal," *2017 IEEE Glob. Commun. Conf. GLOBECOM 2017 - Proc.*, vol. 2018-January, pp. 1–6, Jul. 2017, doi: 10.1109/GLOCOM.2017.8255023.

[6] J. Ribeiro, F. B. Saghezchi, G. Mantas, J. Rodriguez, S. J. Shepherd, and R. A. Abd-Alhameed, "An Autonomous Host-Based Intrusion Detection System for Android Mobile Devices," *Mob. Networks Appl.*, vol. 25, no. 1, pp. 164–172, 2020, doi: 10.1007/s11036-019-01220-y.

[7] J. Ribeiro, G. Mantas, F. B. Saghezchi, J. Rodriguez, S. J. Shepherd, and R. A. Abd-Alhameed, "Towards an Autonomous Host-based Intrusion Detection System for Android Mobile Devices," in *Proceedings of the 9th EAI International*

Conference on Broadband Communications, Networks, and Systems (BROADNETS2018), 2018, pp. 139–148.

[8] A. Farouk, A. Alahmadi, S. Ghose, and A. Mashatan, "Blockchain platform for industrial healthcare: Vision and future opportunities," *Computer Communications*. 2020, doi: 10.1016/j.comcom.2020.02.058.

[9] A. Dorri, S. S. Kanhere, and R. Jurdak, "Towards an optimized blockchain for IoT," *Proc. - 2017 IEEE/ACM 2nd Int. Conf. Internet-of-Things Des. Implementation, IoTDI 2017 (part CPS Week)*, pp. 173–178, 2017, doi: 10.1145/3054977.3055003.

[10] S. Singh, A. S. M. Sanwar Hosen, and B. Yoon, "Blockchain Security Attacks, Challenges, and Solutions for the Future Distributed IoT Network," *IEEE Access*, vol. 9, pp. 13938–13959, 2021, doi: 10.1109/ACCESS.2021.3051602.

[11] S. Biswas, F. Li, Z. Latif, K. Sharif, A. K. Bairagi, and S. P. Mohanty, "GlobeChain: An Interoperable Blockchain for Global Sharing of Healthcare Data - A COVID-19 Perspective," *IEEE Consum. Electron. Mag.*, pp. 1–5, 2021, doi: 10.1109/MCE.2021.3074688.

[12] M. A. Rashid and H. H. Pajooh, "A security framework for iot authentication and authorization based on blockchain technology," *Proc. - 2019 18th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. IEEE Int. Conf. Big Data Sci. Eng. Trust. 2019*, pp. 264–271, 2019, doi: 10.1109/TrustCom/BigDataSE.2019.00043.

[13] I. Essop, J. C. Ribeiro, M. Papaioannou, J. Rodriguez, G. Zachos, and G. Mantas, "Generating datasets for anomaly-based intrusion detection systems in iot and industrial iot networks," *Sensors*, vol. 21, no. 4, pp. 1–31, 2021, doi: 10.3390/s21041528.

[14] H. H. Pajooh, M. Rashid, F. Alam, and S. Demidenko, "Hyperledger fabric blockchain for securing the edge internet of things," *Sensors (Switzerland)*, vol. 21, no. 2, pp. 1–29, 2021, doi: 10.3390/s21020359.

[15] E. Androulaki *et al.*, "Hyperledger fabric," 2018, doi: 10.1145/3190508.3190538.

[16] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," *2017 IEEE Int. Conf. Pervasive Comput. Commun. Work. PerCom Work. 2017*, pp. 618–623, 2017, doi: 10.1109/PERCOMW.2017.7917634.

[17] A. D. Dwivedi, L. Malina, P. Dzurenda, and G. Srivastava, "Optimized blockchain model for internet of things based healthcare applications," *arXiv*. IEEE, pp. 135–139, 2019.

[18] H. R. Hasan *et al.*, "Blockchain-Based Solution for COVID-19 Digital Medical Passports and Immunity Certificates," *IEEE Access*, vol. 8, pp. 222093–222108, 2020, doi: 10.1109/ACCESS.2020.3043350.

[19] O. Attia, I. Khoufi, A. Laouiti, and C. Adjih, "An IoT-Blockchain architecture based on hyperledger framework for healthcare monitoring application," *2019 10th IFIP Int. Conf. New Technol. Mobil. Secur. NTMS 2019 - Proc. Work.*, 2019, doi: 10.1109/NTMS.2019.8763849.

[20] A. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchain in Internet of Things: Challenges and Solutions."

[21] S. Biswas, K. Sharif, F. Li, B. Nour, and Y. Wang, "A scalable blockchain framework for secure transactions in IoT," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4650–4659, 2019, doi: 10.1109/JIOT.2018.2874095.

[22] F. Pelekoudas Oikonomou, J. Ribeiro, G. Mantas, J. Bastos, and J. Rodriguez, "A Hyperledger Fabric-based Blockchain Architecture to Secure IoT-based Health Monitoring Systems," IEEE International Mediterranean Conference on Communications and Networking 7–10 September 2021, accepted.