Design of a Blockchain-based Anomaly-based Intrusion Detection System (AIDS) for IoMT Networks

Georgios Zachos
Instituto de Telecomunicações
Aveiro, Portugal
Faculty of Engineering and Science,
University of Greenwich
Chatham Maritime, UK
g.zachos@av.it.pt

Filippos Pelekoudas-Oikonomou
Faculty of Engineering and Science,
University of Greenwich
Chatham Maritime, UK
f.pelekoudasoikonomou@greenwich.ac.uk

Georgios Mantas
Instituto de Telecomunicações
Aveiro, Portugal
Faculty of Engineering and Science,
University of Greenwich
Chatham Maritime, UK
gimantas@av.it.pt

Kyriakos Porfyrakis
Faculty of Engineering and Science,
University of Greenwich
Chatham Maritime, UK
k.porfyrakis@greenwich.ac.uk

Georgia Sakellari
Faculty of Engineering and Science,
University of Greenwich
Chatham Maritime, UK
g.sakellari@greenwich.ac.uk

Jonathan Rodriguez
Instituto de Telecomunicações
Aveiro, Portugal
Faculty of Computing, Engineering and Science,University of South Wales
Pontypridd, UK
jonathan@av.it.pt

***Abstract*—Over the past few years, the Internet of Things (IoT) has been growing significantly, particularly in the healthcare sector, leading to the introduction of the Internet of Medical Things (IoMT) technology, whose aim is the improvement of the patient's quality of life. Nevertheless, IoMT networks are still vulnerable to a wide range of threats because of their heterogeneity and resource-constrained characteristics. Thus, novel security mechanisms protecting IoMT networks from adversaries are urgently needed. In this context, the industry and research community currently view Anomaly-based Intrusion Detection Systems (AIDSs) and blockchain technology as innovative solutions that could protect IoMT networks. However, so far, and to the best of our knowledge, there is a scarcity of research focusing on blockchain-based AIDSs, specifically designed for protecting IoMT networks. Our aim is to fill this significant research gap and thus, in this paper, we present the design of the system architecture of an energy-efficient Hyperledger Fabric-based AIDS (HF-AIDS) for IoMT networks.**

Keywords—IoMT networks, Anomaly-based Intrusion Detection, blockchain, Hyperledger Fabric

I. Introduction

Over the past few years, the Internet of Things (IoT) technology has been developing significantly, particularly in the healthcare sector. This growth has been assisted by the introduction of the Internet of Medical Things (IoMT) technology that focuses on the improvement of the patient's quality of life by enabling personalized e-health services without limitations on time and location [1]–[3]. However, the wide range of different communication technologies (e.g., WLANs, Bluetooth, Zigbee) and types of IoMT devices (e.g., medical sensors, actuators) incorporated in IoMT networks are vulnerable to various types of security threats, raising many security and privacy challenges for such networks, as well as for the healthcare systems relying on these networks [4]–[7]. Consequently, security solutions protecting IoMT networks from adversaries are crucial for the acceptance and wide adoption of such networks in the coming years.

Nevertheless, the high resource requirements of complex and heavyweight conventional security mechanisms cannot be afforded by (a) the resource-constrained IoMT devices with limited processing power, storage capacity, and battery life, and/or (b) the constrained environment in which the IoMT devices are deployed and interconnected using lightweight communication protocols [8]. Furthermore, the state-of-the-art security solutions widely adopt centralization approaches that suffer from single point of failure issues and cannot ensure complete tamperproof data storage, and thus are not well applicable to IoMT networks [9]–[11]. Therefore, there is an urgent need for novel security mechanisms to address the pressing security challenges of IoMT 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], [12].

In this context, the industry and research community currently view anomaly-based intrusion detection as a promising security solution for protecting IoT networks, as long as novel lightweight Anomaly-based Intrusion Detection Systems (AIDSs) are developed [13]. Furthermore, blockchain technology has also been identified as a disruptive technology capable of integration into innovative security solutions for IoMT networks, as it holds the potential to make substantial contributions by (a) enhancing the security of IoMT devices and (b) ensuring resistance against unauthorized access during data transmission, thereby enabling tamper-proof transmission of medical data [14].

However, so far, and to the best of our knowledge [15], there is a scarcity of research focusing on blockchain-based AIDSs, specifically designed for protecting IoMT networks. This limited body of work highlights the lack of comprehensive investigations into lightweight blockchain-based security solutions tailored to the unique requirements of IoMT networks. Therefore, our aim is to fill this significant research gap by developing a novel energy-efficient blockchain-based Anomaly-based Intrusion

This research was sponsored by the NATO Science for Peace and Security Programme under grant SPS G5797.

Detection System (AIDS) tailored to the needs of IoMT networks by leveraging the Hyperledger Fabric (HF) blockchain platform [16].

Toward this direction, the current research work presents the design of the system architecture of an energy-efficient HF-based AIDS (HF-AIDS) for IoMT networks. Specifically, the present research work provides the following contributions:

(i) presents an IoMT network consisting of an IoMT Cloud Platform, IoMT Gateways and IoMT Devices (i.e., sensors and/or actuators) with each IoMT Gateway and its connected IoMT Devices forming a group (i.e., IoMT Group).

(ii) integrates multiple local AIDSs in the IoMT network with each AIDS covering one specific IoMT Group. The design of each local AIDS is enhanced with the ability to employ a Federated Learning (FL) approach in combination with other local AIDSs to produce global machine learning (ML) models for intrusion detection purposes.

(iii) incorporates HF blockchain in the IoMT Gateways of the IoMT network. The purpose of HF blockchain is twofold: (a) support FL-based training between the local AIDSs by eliminating the need for a central aggregator server, and (b) record alerts produced by local AIDSs to ensure non-repudiation and tamperproof data storage.

The remainder of this paper is organized as follows. In Section II, we present the related work regarding the AIDS for IoMT networks proposed in [17] and Hyperledger Fabric platform. In Section III, we give a brief overview of the assumed IoMT network. In Section IV, the components and functionalities of the proposed HF-AIDS are described. Section V discusses the security benefits of the proposed HF-AIDS. Finally, Section 6 concludes the paper.

II. Related Work

A. An AIDS for IoMT Networks

The purpose of the AIDS proposed in [17] is the protection of the IoMT network and its IoMT devices and gateway from internal and external threats that may exploit the inherent security vulnerabilities of IoT technology and target the IoMT network, its IoMT devices, or the gateway.

The AIDS leverages host-based and network-based techniques to reliably monitor and collect log files from the IoMT devices and the gateway, as well as traffic from the IoMT network, while at the same time considering the computational cost. The detection process of the AIDS proposed in [17] is performed on the IoMT gateway and relies on Machine Learning (ML) techniques, considering the computation overhead, in order to detect abnormalities in the collected data and thus identify malicious incidents in the IoMT network.

The AIDS proposed in [17] consists of two types of components: (a) a distributed Monitoring and Data Acquisition (MDA) components, and (b) a Central Detection (CD) component (i.e., detection engine). On the one hand, the MDA component runs on each IoMT device (i.e., sensor and/or actuator) connected to the gateway. The MDA component monitors the behavior of the IoMT device hosting it and collects device behavior data. Additionally, the MDA component transmits the collected data to the gateway as an MDA report.

On the other hand, the CD component runs on the gateway of the IoMT network and performs four main operations:

(i) monitors the behavior of the gateway hosting it and collects relevant behavior data,

(ii) monitors the network traffic passing through the gateway and gathers relevant network traffic data,

(iii) receives the reports transmitted by the MDA components running on the IoMT devices that are connected to the gateway, and

(iv) uses the aforementioned data to detect whether an attack incident has occurred in the IoMT network and triggers a corresponding security alert.

B. Hyperledger Fabric

Hyperledger Fabric (HF) [16] is a distributed ledger platform specifically designed for building applications with a modular architecture [18]. HF's unique characteristics are:

(i) the modular architecture that allows for the development of scalable and customizable applications tailored to the specific needs of IoMT systems,

(ii) the HF's pluggable consensus protocols, particularly PBFT-based, that ensure secure and efficient transaction processing within the network,

(iii) the private-permissioned blockchain model, which is crucial for maintaining privacy and control over sensitive data,

(iv) the platform's ability to accommodate changeable trust assumptions that remains well-suited for IoMT deployments involving multiple stakeholders with varying degrees of trust,

(v) the platform's ability to create customizable applications using the chaincode, that will enable the integration of IDS with the blockchain network, and;

(vi) HF is suitable for implementations for IoMT networks due to its lightweight nature [19]. Compared to other popular blockchain platforms like Ethereum, the HF platform offers a more energy-efficient blockchain-based security architecture for IoMT-based health monitoring systems. This advantage stems from the fact that the HF platform does not employ the resource-intensive Proof of Work (PoW) consensus protocol, which would be impractical for resource-constrained IoMT devices, due to their limited processing power, storage capacity, and battery life.

Overall, these qualities make HF suitable for IoMT, enabling secure and scalable solutions in the healthcare domain.

For better understanding the terminology of HF, the main components of HF that will be referred in the proposed design are presented here:

Peer: The peer is a central component within the blockchain network, responsible for hosting the blockchain ledger and chaincode. It also provides a platform for hosting SDKs and APIs, allowing network users to interact with applications and services.

Orderers: It is a dedicated node or set of nodes that perform the task of ordering transactions in the context of HF, in a deterministic manner, separate from the endorsement process, which occurs within the peers.

Chaincode: In the context of HF, chaincode, is a piece of code that serves as an application within the established blockchain network. It provides specific functionalities and operations, encapsulated within a Docker container.

State database: State databases in HF, are distributed databases (e.g., CouchDB) that play a crucial role in storing and managing the current state of the blockchain network. The state database represents the most recent version of the data and facilitates efficient querying and retrieval operations.

III. Overview of an IoMT Network

To begin with, we assume an IoMT network consisting of an IoMT Cloud Platform, IoMT Gateways and IoMT Devices (i.e., sensors and/or actuators) as shown in Fig. 1.

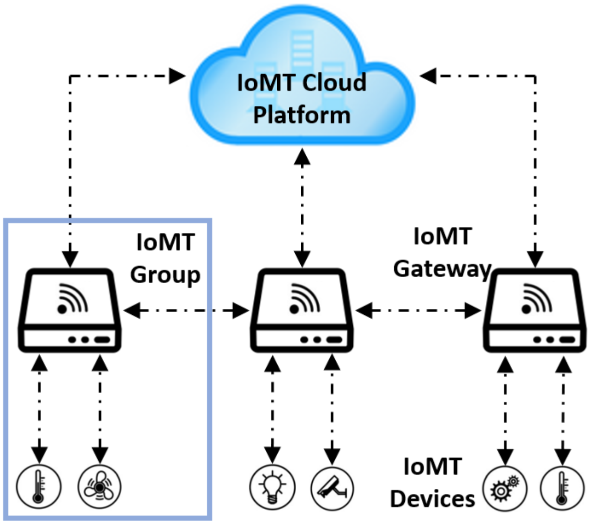

Fig. 1. The IoMT network with IoMT Cloud Platform, IoMT Gateways and IoMT Devices.

In general, the IoMT devices possess limited computational and communication capabilities. On the one hand, an IoMT device (e.g., an IoMT sensor device) may operate as a source of sensing data that are relevant to the wellbeing of a patient or environment around a patient. On the other hand, an IoMT device (e.g., an IoMT actuator device such as an insulin pump) may function as a receiver of data. In this case, the received data may contain commands which are required to be executed by the IoMT device in order to perform an action (e.g., the injection of insulin into the body of a patient).

Moreover, the IoMT Gateway is meant to function as a relay node. On the one hand, the IoMT Gateway acts as a receiver of the sensing data of the connected IoMT devices and subsequently, transmits the sensing data to the IoMT Cloud Platform. On the other hand, the IoMT Gateway may receive IoMT device commands from the IoMT Cloud Platform. These commands are in turn sent by the IoMT Gateway to the connected IoMT devices to be executed. At this point, it is worthwhile mentioning that multiple IoMT devices are grouped under one IoMT Gateway as shown in Fig. 1. A group consisting of an IoMT Gateway and its connected IoMT devices would be referred to as an IoMT Group. In addition, for our proposed design, we make the assumption that the various IoMT Gateways are interconnected and can communicate between them and subsequently, they can also participate in a HF blockchain network as blockchain nodes.

As far as the IoMT Cloud Platform is concerned, its main purposes are the following: (i) receive the data from the IoMT devices through the Gateway, (ii) process further the received data, (iii) send appropriate commands back to the IoMT devices through the Gateway, and (iv) provide visualization services regarding the received data.

IV. Proposed Blockchain-based IDS for IoMT Networks

Fig. 2 depicts the proposed HF-AIDS on the IoMT network.

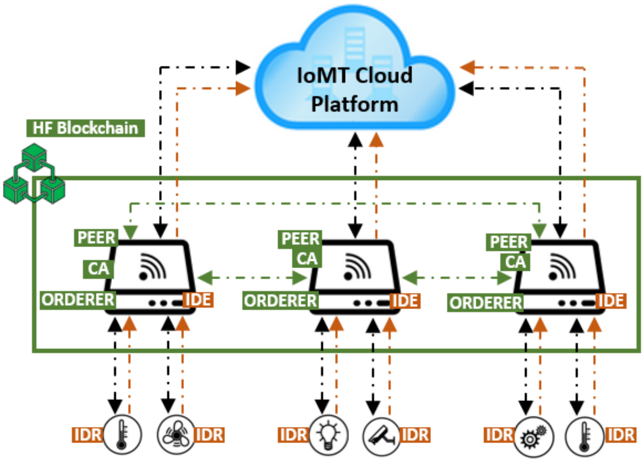

Fig. 2. Proposed HF-AIDS on the IoMT network.

A. Local Anomaly-based Intrusion Detection Systems

The IoMT network described in Section III is equipped with multiple local AIDSs and each local AIDS is meant to cover one specific IoMT Group. The architecture of each local AIDS shares common components and functionalities with the AIDS for IoMT Networks that was proposed in [17]. Fig. 3 shows the components of a local AIDS in an IoMT Group (i.e., an IoMT Gateway and its connected IoMT Devices).

The first component of each local AIDS is the Intrusion Detection Reporter (IDR) residing on an IoMT device. Its purposes are similar to the MDA component mentioned in subsection II.A, meaning that the IDR (a) monitors the behavior of the IoMT device hosting it, (b) collects device behavior data and (c) sends the collected data to the gateway as an IDR report.

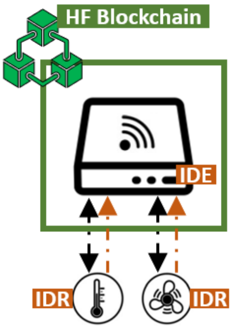

Fig. 3. Components of a local AIDS in an IoMT Group.

The second component of each local AIDS is the Intrusion Detection Engine (IDE) residing on an IoMT Gateway. Its purposes are similar to the CD component mentioned in subsection II.A, meaning that the IDE is responsible to:

(a) monitor the behavior of the gateway hosting it and collect relevant behavior data,

(b) monitor the network traffic passing through the gateway and gather relevant network traffic data,

(c) receive the reports transmitted by the IDR components running on the IoMT devices that are connected to the gateway,

(d) leverage the aforementioned three types of received data to train ML models in a federated learning (FL) manner in collaboration with the IDEs running on other connected IoMT Gateways, and

(e) use the aforementioned three types of received data and trained ML models to detect whether an attack incident has occurred in the IoMT network, and send a corresponding security alert to the IoMT Cloud Platform.

As it can be observed, the proposed IDE component receives three different types of data and uses these data in two different manners. The first manner relates to the training operation of each IDE where each of the three types of received data are used to produce one trained global ML model through FL [20]. According to federated learning, three local ML models would be initially trained on each IDE using the data received from the IoMT devices connected to that specific IDE. Then, the three types of locally trained ML models of all the IDEs participating in FL would be transmitted to an aggregator server that would combine the locally trained ML models into three global ML models. The three global ML models would then be sent back to the IDEs to be used for detection purposes. However, as it will be described in the next subsection, in our proposed design, the use of HF blockchain eliminates the need for an aggregator server.

On the other hand, after the three global ML models are produced, they can be used for intrusion detection purposes. Each of the three types of data received by connected IoMT devices is provided as an input to the corresponding trained global ML model. Depending on the used ML model, the output is the decision describing whether an intrusion has been detected on (i) the IoMT Gateway, (ii) the network consisting of the IoMT Gateway and its connected IoMT devices, or (iii) a specific IoMT device connected to the IoMT Gateway. In case an intrusion is detected, a corresponding security alert is triggered and sent to the IoMT Cloud Platform. In addition, as it will be described in the next subsection, in our proposed design, the HF blockchain is used to record the security alerts before they are sent to the IoMT Cloud Platform.

B. Hyperledger integration on the IoMT network

The key component for the incorporation of HF blockchain technology in the existing IoMT network in which the local AIDSs are integrated, is the Gateway of the IoMT network. The gateway is the enabling device that contains the HF's components (e.g., Peer, Certificate Authority, Orderer) that ensure its proper functionality as a blockchain node, as well as the necessary components of the AIDS (i.e., IDE).

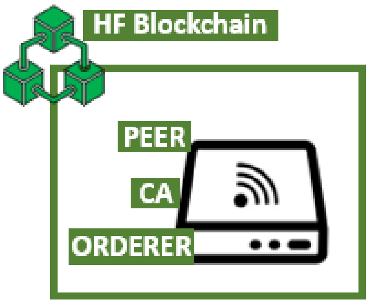

Fig. 4. Components of HF in an IoMT Gateway.

In HF, data storage is implemented through two essential components: the blockchain ledger and the state database [21]. The blockchain ledger maintains a distributed, append-only record of transactions across the network, ensuring an ordered and immutable history of all transactions. This decentralized ledger is replicated among multiple participating nodes, providing data redundancy and fault tolerance. On the other hand, the state database captures the current state of the system, serving as a key-value store for efficient data retrieval and querying. This separation of the ledger and state database enables scalability and performance, as the ledger captures the complete transaction history while the state database facilitates quick validation and execution of transactions based on the current data state.

In the context of incorporating a local AIDS with HF, the data provided by the local AIDS can be stored within the HF following a similar approach as previously described (i.e., the data are stored in the state database). On the one hand, HF needs to support the FL approach used by the local AIDSs to train the ML models used for intrusion detection purposes. In this case, the locally trained ML models of each local AIDS are stored in the state database instead of being sent to an aggregator server. As every IoMT Gateway is participating in the HF blockchain network, it uses its installed Peer component to access the state database and queries the necessary information (i.e., all locally trained ML models) that can be utilized to produce the global ML models that every local AIDS will use for intrusion detection purposes. On the other hand, when a local AIDS detects and generates alerts for potential intrusions or security threats within the network, the relevant data, such as intrusion events, timestamps, and associated metadata, can be captured and securely stored in the state database. After the alert are stored in the state database, they can be transmitted to the IoMT Cloud Platform for further processing.

In our proposed design with the aid of HF's chaincode functionality, the necessary information (i.e., ML models and alerts) will be stored in the state database in the format shown in Fig. 5.

```
Object AIDSdata {
    this.GwIndex = -1; // Unique ID of the IoMT Gateway
    this.modelParams = [ ]; // Array to store model parameters
    this.alerts = [ ]; // Array to store alerts
    this.metadata = [ ]; // Array to store metadata
  }
```

Fig. 5. Chaincode format of the stored data

V. Discussions

In the proposed HF-AIDS, each separate component (i.e., local AIDSs, blockchain) offers specific security benefits:

(i) A local AIDS receives three different types of data and using its trained ML models, it can detect whether an intrusion has been detected on (i) the IoMT Gateway, (ii) the network consisting of the IoMT Gateway and its connected IoMT devices, or (iii) a specific IoMT device connected to the IoMT Gateway. Thus, a local AIDS can identify from where an attack originates or which device (i.e., IoMT device or gateway) is compromised.

(ii) The local AIDSs employ FL in order to produce global ML models that take into account the training occurring on all the local AIDSs of the IoMT network. As a result, the produced global ML models can exhibit better performance in comparison to ML models that had been locally trained.

(iii) The use of HF eliminates the need for an aggregation server. Instead, data can be directly recorded on the distributed ledger by the participating IoMT Gateways. Each IoMT Gateway maintains a copy of the ledger, ensuring redundancy and fault tolerance. As a result, the removal of the aggregation server significantly improves the system's resilience, reduces the risk of a single point of failure, and enhances the overall reliability of the proposed design.

(iv) By leveraging blockchain inherent properties, such as immutability and consensus mechanisms, the proposed HF-AIDS guarantees non-repudiation, making it impossible for any party to deny their involvement or actions recorded on the blockchain. Additionally, the tamperproof storage ensures that once data is recorded, it remains secure and immutable, providing a high level of trust and integrity to the system.

(v) HF's lightweight nature makes it suitable to support resource-constrained IoMT devices, and ensures efficient utilization of limited processing power, storage capacity, and battery life.

VI. Conclusion

In this paper, we presented details of the system architecture of an energy-efficient HF-based AIDS (HF-AIDS) for IoMT networks. We explained the use of multiple local AIDSs that are meant to (a) train ML models in a FL manner, and to (b) detect intrusions on the IoMT Gateways, IoMT devices or the IoMT network by employing the trained ML models. In addition, we described the incorporation of HF blockchain in the local AIDSs. The proposed HF-AIDS provide specific security benefits: (i) identification of the origin of an attack or of the compromised device (i.e., IoMT device or gateway), (ii) improvement of the intrusion detection accuracy through FL, (iii) elimination of the need for a central aggregator server, (iv) tamperproof data storage and non-repudiation, and (v) lightweight functionality suitable for IoMT networks.

As future work, we plan to proceed with the implementation of the proposed HF-AIDS. In addition, our aim is to evaluate various ML algorithms and select the optimum among them to be trained by the local AIDSs and then used for their intrusion detection purposes. In this context, we will also test different consensus algorithms for the blockchain between the IoMT Gateways and select the most optimum consensus algorithm in terms of consumed computation and communication resources. Finally, after selecting the ML algorithms to be used for intrusion detection and the consensus algorithm to be employed in the HF blockchain network, the performance of the implemented HF-AIDS will be evaluated in terms of (a) detection accuracy, (b) computational complexity, (c) communication overhead, and (d) robustness of the HF blockchain network.

References

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

[2] 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.

[3] S. M. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, and K. S. Kwak, "The internet of things for health care: A comprehensive survey," *IEEE Access*, vol. 3, pp. 678–708, 2015, doi: 10.1109/ACCESS.2015.2437951.

[4] P. Gope and T. Hwang, "BSN-Care: A Secure IoT-Based Modern Healthcare System Using Body Sensor Network," *IEEE Sens. J.*, 2016, doi: 10.1109/JSEN.2015.2502401.

[5] S. Khezr, M. Moniruzzaman, A. Yassine, and R. Benlamri, "Blockchain technology in healthcare: A comprehensive review and directions for future research," *Appl. Sci.*, 2019, doi: 10.3390/app9091736.

[6] I. Makhdoom, M. Abolhasan, J. Lipman, R. P. Liu, and W. Ni, "Anatomy of Threats to the Internet of Things," *IEEE Commun. Surv. Tutorials*, vol. 21, no. 2, pp. 1636–1675, 2019, doi: 10.1109/COMST.2018.2874978.

[7] M. Karageorgou, G. Mantas, I. Essop, J. Rodriguez, and D. Lymberopoulos, "Cybersecurity attacks on medical IoT devices for smart city healthcare services," in *IoT Technologies in Smart Cities: From sensors to big data, security and trust*, Institution of Engineering and Technology, 2020, pp. 171–187.

[8] 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.

[9] M. Seliem and K. Elgazzar, "BIoMT: Blockchain for the internet of medical things," 2019, doi: 10.1109/BlackSeaCom.2019.8812784.

[10] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of things: The road ahead," *Computer Networks*. 2015, doi: 10.1016/j.comnet.2014.11.008.

[11] L. Catarinucci *et al.*, "An IoT-Aware Architecture for Smart Healthcare Systems," *IEEE Internet Things J.*, 2015, doi: 10.1109/JIOT.2015.2417684.

[12] F. Alsubaei, A. Abuhussein, and S. Shiva, “Security and Privacy in the Internet of Medical Things: Taxonomy and Risk Assessment,” *Proc. - 2017 IEEE 42nd Conf. Local Comput. Networks Work. LCN Work. 2017*, no. 6, pp. 112–120, 2017, doi: 10.1109/LCN.Workshops.2017.72.

[13] J. Asharf, N. Moustafa, H. Khurshid, E. Debie, W. Haider, and A. Wahab, “A review of intrusion detection systems using machine and deep learning in internet of things: Challenges, solutions and future directions,” *Electronics (Switzerland)*, vol. 9, no. 7. MDPI AG, p. 1177, 2020, doi: 10.3390/electronics9071177.

[14] M. A. Khan and K. Salah, “IoT security: Review, blockchain solutions, and open challenges,” *Futur. Gener. Comput. Syst.*, vol. 82, pp. 395–411, 2018, doi: 10.1016/j.future.2017.11.022.

[15] F. Pelekoudas-oikonomou *et al.*, “Blockchain-Based Security Mechanisms for IoMT Edge Networks in IoMT-Based Healthcare Monitoring Systems,” 2022.

[16] E. Androulaki *et al.*, “Hyperledger fabric,” 2018, doi: 10.1145/3190508.3190538.

[17] G. Zachos, I. Essop, G. Mantas, K. Porfyrakis, J. C. Ribeiro, and J. Rodriguez, “An Anomaly-Based Intrusion Detection System for Internet of Medical Things Networks,” *Electron. 2021, Vol. 10, Page 2562*, vol. 10, no. 21, p. 2562, Oct. 2021, doi: 10.3390/ELECTRONICS10212562.

[18] “Introduction — hyperledger-fabricdocs main documentation.” https://hyperledger-fabric.readthedocs.io/en/release-2.5/blockchain.html?highlight=modular architecture#introduction (accessed Jul. 16, 2023).

[19] F. P. Oikonomou, Pelekoudas, J. Ribeiro, G. Mantas, J. M. C. S. Bastos, and J. Rodriguez, “A Hyperledger Fabric-based Blockchain Architecture to Secure IoT-based Health Monitoring Systems,” 2021, Accessed: Jan. 20, 2022. [Online]. Available: https://ieeexplore.ieee.org/document/9647521/.

[20] T. Li, A. K. Sahu, A. Talwalkar, and V. Smith, “Federated Learning: Challenges, Methods, and Future Directions,” *IEEE Signal Process. Mag.*, vol. 37, no. 3, pp. 50–60, 2020, doi: 10.1109/MSP.2020.2975749.

[21] “CouchDB as the State Database — hyperledger-fabricdocs main documentation.” https://hyperledger-fabric.readthedocs.io/en/release-2.5/couchdb_as_state_database.html?highlight=database (accessed Jul. 16, 2023).