Secure and Privacy-aware Blockchain-based Remote Patient Monitoring System for Internet of Healthcare Things

Bessem Zaabar*†‡, Omar Cheikhrouhou*†, Meryem Ammi§, Ali Ismail Awad¶‖**, and Mohamed Abid*
*Computer Embedded System laboratory CES-ENIS, University of Sfax, Tunisia
†Higher Institute of Computer Science of Mahdia, University of Monastir, Tunisia
‡National Center of Nuclear Sciences and Technologies, Tunisia
Email: bessem.zaabar@enis.tn, omar.cheikhrouhou@isetsf.rnu.tn, mohamed.abid_ces@yahoo.fr
§Forensic Science Department, Criminal Justice College, Naif Arab University for Security Sciences, Saudi Arabia
Email: mammi@nauss.edu.sa
¶Department of Computer Science, Electrical and Space Engineering, Luleå University of Technology, Luleå, Sweden
‖College of Information Technology, United Arab Emirates University, Al Ain P.O. Box 17551, United Arab Emirates
**Faculty of Engineering, Al-Alzhar University, Qena P.O. Box 83513, Egypt
Email: ali.awad@ltu.se, ali.awad@uaeu.ac.ae

***Abstract*—Remote Patient Monitoring (RPM) is a form of telehealth or virtual health that strengthens online medical services and allows delivering healthcare remotely. Nowadays, remote patient monitoring systems (RPMS) are widely used by healthcare providers to remotely monitor the vital signs of patients. As the RPM field expands, concerns about efficient and secure medical data transmission are raised. This kind of patient medical data is collected by the mean of Internet of Healthcare Things (IoHT) or sometimes denoted as Internet of Medical Things (IoMT) devices. The collected data needs to be stored and retrieved with highly assured levels of security and privacy as the data comprises private and critical patients' information. To secure medical data, this paper proposes a blockchain-based architecture to manage access control to medical data and to preserve patient's data privacy. The blockchain-based system is built on Hyperledger Fabric, a permissioned distributed ledger solution, and the ledgers and transactions are stored in the cloud. The proposed architecture is designed to contribute to the robustness of the RPM systems and to avoid recorded security limitations in commonly used permissioned blockchains methods. Performance evaluation has proved the robustness and superiority of the proposed system in terms of data confidentiality, integrity, availability, traceability, scalability, and data privacy while integrated with the RPM services.**

***Index Terms*—Internet of Things (IoT), Internet of Healthcare Things (IoHT), Security and Privacy, Blockchain, Electronic Medical Record (EMR), Electronic Healthcare Record (EHR).**

I. INTRODUCTION

In the healthcare industry, Remote Patient Monitoring (RPM) is one area where IoT is being used [1]. Indeed, The Internet of Things (IoT) results from the interconnection of physical objects with sensing, processing, and communication ability together with the internet [2]. In essence, these physical objects are generally attached to the patient body to collect some vital signs such as respiration rate, body temperature, pulse rate, blood pressure, and more [3]. These wearable smart devices monitor the overall health status of the patient, keep track of his health status, and produce alarms in the event of any suspicious behavior. The security of these new generation e-health services is one of the topmost concerns of different healthcare organizations. Indeed, the reported cyber-attacks against patient healthcare data in recent years have pushed industry and researchers to develop new solutions that can mitigate these attacks and keep patient healthcare data private and secure [4].

This paper proposes a novel Blockchain-based Internet of Medical Things (BC-IoMT) solution for securing remote patient monitoring and allowing patients to manage their medical data. In this solution, Hyperledger Fabric [11] and Hyperledger Composer [12] have been integrated and used to ensure security aspects of the proposed BC-IoMT architecture and increase its performance. Indeed, this proposed solution aims at satisfying the security requirements for RPM, including confidentiality, integrity, authorization, and availability.

The main contribution of this proposed solution is the use of Hyperledger Fabric and Hyperledger Composer with cloud storage, which to the best of the authors' knowledge, has not been tackled previously in the healthcare field. Indeed, the motivation behind such design is to overcome the security concerns in commonly used permissioned Blockchains approaches [13]. The proposed architecture contains four layers: Hyperledger Fabric, Hyperledger Composer deployed within a cloud layer, and finally an RPM application layer. Moreover, one potential aspect inherited from Blockchain architecture is that distributed ledgers and transactions of BC are stored in the cloud which ensures the scalability of the proposed system.

The remainder of this paper is as follows. Section II outlines the existing literature related to the use of Blockchain in the healthcare field. Section III presents in details the proposed architecture. Section IV illustrates the development environment

978-1-6654-2854-5/21/$31.00 ©2021 IEEE

TABLE I: Summary of the common reviewed state-of-the-art research that highlights the security, operational and privacy research aspects. ● means fully covered and ☐ means uncovered.

	Security Triad (CIA)			Operational and Privacy			
Reference	Confidentiality	Integrity	Availability	Traceability	Scalability	Privacy	Contributions
Košt'ál et al. [5]	●	●	☐	●	☐	●	Management of IoT devices configuration via Hyperledger composer
Griggs et al. [6]	●	●	●	●	☐	●	Blockchain-based smart contracts to secure RPM
Shen, Guo, and Yang [7]	●	●	●	●	☐	☐	Healthcare data sharing via Blockchain
Attia et al. [8]	●	●	●	●	☐	●	Healthcare monitoring via Fabric Blockchain
Dwivedi et al. [9]	●	●	●	☐	●	●	cryptographic techniques over healthcare Ethereum Blockchain
Wang [10]	●	●	●	●	●	☐	IoT, Ethereum Blockchain, and cloud-based healthcare system

and the case study implemented. Performance evaluation in light of the security and privacy requirements is discussed in Section V. Section VI provides a comparative analysis with the existing Blockchain-based similar systems. Finally Section VII concludes the paper and sets a road map for future research.

II. RELATED WORK

Recently, Blockchain technology has emerged as a promising technology that provides several security services including access control, privacy, and integrity [14], [15]. Due to its inherent characteristics such as transparency, distribution, and immutability, Blockchain technology is attracting more and more cybersecurity researchers in several fields including healthcare [16].

Košt'ál et al. in [5] introduced an architecture to monitor and track the modification of IoT devices configuration. They adopted a private blockchain in which they saved the device's configuration files and any modification that might occur. The history of adjustment is preserved and made available for the administrators. Therefore, this model fosters security through monitoring and auditing IoT device configuration.

Griggs et al. [6] used a private Ethereum Blockchain. In the designed system, sensors interact with a smart device (smartphone or tablet) that communicates directly to smart contracts. The latter analyzes the provided data and triggers alerts to patients and healthcare providers. Note that collected data is not kept into Blockchain but only transactions of occurred events are kept in the ledger. Thus, a secure remote patient monitoring system is proposed thanks to Blockchain features. However, the time of data transmission from the smart device to Blockchain nodes presents a major limitation to the proposed system.

To store the physiological states of patients, the research was done by Shen, Guo, and Yang in [7] proposed "MedChain" as a session-based healthcare data sharing system based on Blockchain. MedChain allows the management and sharing of not only the Electronic Healthcare Records (EHRs) of patients but also their physiological parameters collected from the IoMT devices attached to their bodies.

Attia et al. [8] proposed a Blockchain-based architecture for remote healthcare monitoring of patients out of hospitals. They proposed two separate Blockchains, one for medical devices and the other for consultation that holds all the history of patients' records. Besides, a monitoring system is used for real-time tracking and immediately sends alerts in case of an emergency. Moreover, medical wearable devices collect information that will be saved in the medical devices Blockchain. To retrieve data from the patient sensors, the authors suggest the NDN paradigm [17]. The proposed architecture is implemented using the Hyperledger Fabric Framework.

To provide anonymity and authenticity, Dwivedi et al. in [9] proposed to use a lightweight privacy-preserving ring signature scheme [18]. Ring signature allows a signer to sign data without revealing its identity, that is the signature is mixed with other groups (named ring), and no one (except the actual signer) knows which member signed the message. Moreover, for scalability purposes, the authors eliminate the use of the PoW consensus algorithm and introduced the concept of clustering the Blockchain network. More precisely, nodes are organized into clusters and in each cluster, the cluster head is responsible for the addition of a new block. However, the authors did not precise how clusters are formed and did not evaluate their work.

Recently, Wang in [10] used Ethereum Blockchain for healthcare tracking. They proposed a healthcare system based on four layers: application layer, Blockchain-based services layer, cloud layer, and IoT devices layer. The healthcare data is stored in a Blockchain distributed ledger which is stored in the cloud. Data access and management are assumed by a smart contract. The performance of the proposed system is measured by comparing the effectiveness of the Hybrid Etherum Blockchain with other existing approaches. The results show that the proposed healthcare system is much better in terms of latency, processing overhead, and scalability.

Table I summarizes the related work concerning security triad and operational and privacy aspects. Although the table highlights that most of the related work has covered the security triad, it also shows that no single solution has covered all concerned aspects, which validates the need for new research contributions.

III. PROPOSED BLOCKCHAIN-BASED RPM SYSTEM ARCHITECTURE

In this section, we present a novel architecture for securing Remote Patient Monitoring (RPM) based on Blockchain technology. The proposed architecture for our secure remote patient monitoring system is described in Fig. 1.

The proposed system in this study aims to secure the data transferred within the patient environment through a Blockchain-based architecture. Indeed, BC ensures the secure transactions of digital assets recorded through its decentralized

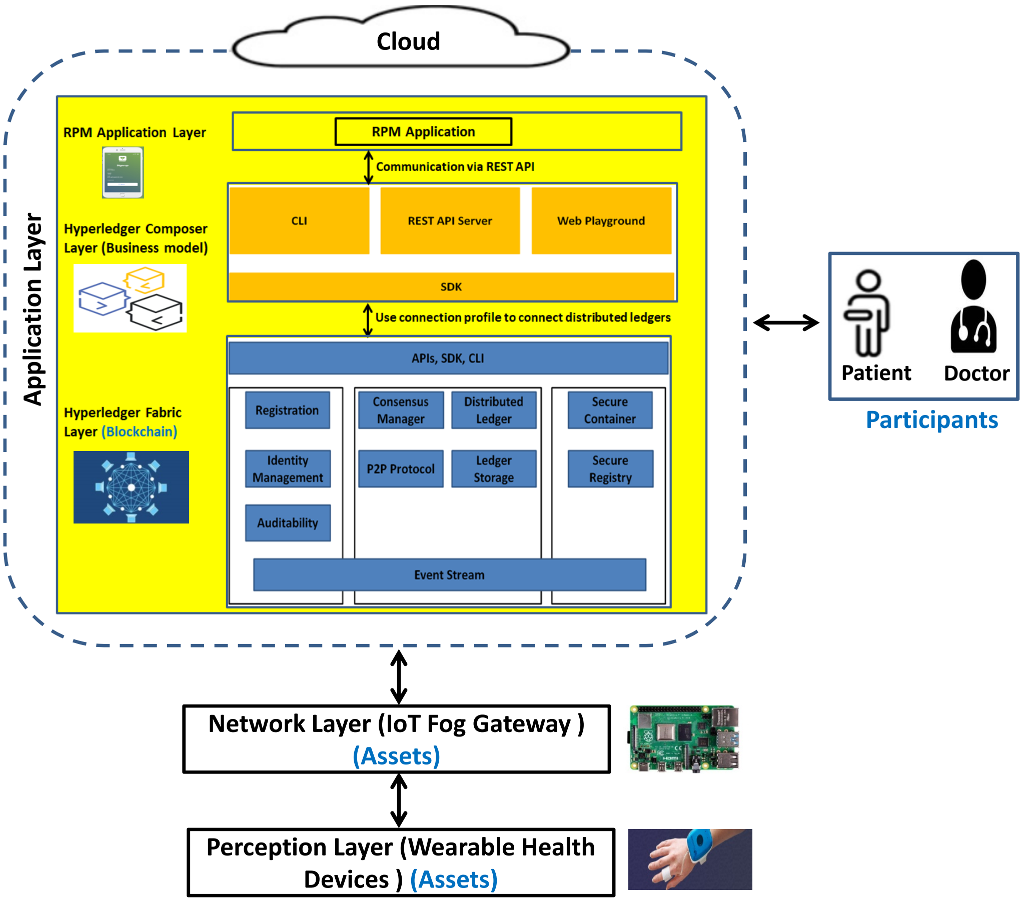


Fig. 1: The overall architecture of the proposed RPM system. The proposed system is implemented in IoHT application layer.

and distributed ledger. These transactions are validated by all nodes. Moreover, hyperledger Fabric is a BC-based platform that suits the use of permissioned BC. The motivation behind using permissioned BC is the need to ensure the patient's data privacy. The use of Hyperledger Fabric is motivated by its modularity architecture' nature, which facilities its customization depending on the user's preferences related to encryption, consensus, and ordering service. Moreover, Hyperledger Fabric is known for its ability to handle identity management and its high-performance [19]. Besides, Fabric architecture is intended to convey high degrees of privacy, versatility, adaptability, and scalability [20].

As a result, the proposed architecture has allowed securing data in motion, data at rest, and data in use. More precisely, the proposed architecture consists of the following layers :

The cloud storage layer: the use of cloud storage is to facilitate the storage and processing the information collected from Wearable Health Devices (WHDs) and processed between the different nodes of the BC network. More specifically, the data collected from WHDs will be sent to the IoT Fog Gateway (GW). The latter is as well playing temporary storage of the collected information in case any disconnection happened with the cloud service.

Hyberledger Fabric Layer: this layer represents the BC network. The fabric architecture comes with three main services: membership, Blockchain, and chaincode.

— *Membership service*: issues certificates to different peers (enrollment certificates, transactions certificates).

— *Blockchain service*: provides a distributed immutable ledger that stores transactions after validation based on a consensus protocol mechanism. Changes made on our chaincode asset are distributed using the P2P protocol.

— *Chaincode service*: encapsulates the smart contracts which are associated usually with an endorsement policy. Hence, the chaincode processes and validates the transactions.

Hyperledger Composer layer (Business Model): the composer layer supports the hyperledger Fabric layer by facilitating a faster business network for the execution of the application. Indeed, the business network description is transmitted as an archive (.bna file) when it is set to be deployed. Therefore, in our proposed application, the description of the network is comprised of three primary files: script, model, and access control.

— The script file: outlines the different transactions in the system by using JavaScript scripting language and works on the transaction logic.

— The model file: is in charge of describing the organi-

TABLE II: Definition and example of model in Blockchain business network.

	Definition	**Example**
Asset	The resources of value that are owned and managed by the network	— Wearble Healthcare Devices (WHDs) — IoT Fog Gateway (GW) — Medical Data
Participants	The actors owning or acting on the assets	— Patient (owner of WHDs) — Patient (Owner of IoT Fog GW) — Doctor (Validate IoT Fog GW and WHDs) — Doctor (Request collected medical data)
Transactions	The executed activities on the assets on behalf of the participants	— WHDs enrollment transaction — IoT Fog GW enrollment transaction — Vital Signs Collection transaction

zation of the network. The model file has three major chunks: transactions, assets, and participants. Noting that these segments own different properties as will be explained in table II .

- The access control file: defines the specific clients access included in the business network.

Moreover, Hyperledger Composer incorporates the Composer REST-Server to create REST API automatically for the business network.

RPM Application layer: consists of remote patient monitoring web application that enables patients and doctors to benefit from the secure and efficient collection and monitoring of medical data.

IV. SYSTEM IMPLEMENTATION

This section gives an overview of the technologies and tools adapted to implement the proposed architecture. The development environment of the suggested system is divided into four parts:

- The configuration of wearable healthcare devices used for sensing patient's vital signs and an IoT gateway used for collecting sensed medical data.
- The implementation of a permissioned Blockchain network built on Hyperledger Fabric. Besides, the implementation of a business model for the proposed architecture using Hyperledger composer.
- The implementation of a web application (RPMApp) used by patients and doctors to benefit from RPMApp services.
- The implementation of cloud storage used for saving distributed ledger and transactions.

In this study, a permissioned Blockchain has been implemented using Hyperledger Fabric framework. The peers of this Blockchain network are representatives of a patient and a physician. Moreover, Hyperledger Composer tools have been used for building the Blockchain business network. The business network definition includes data model, transaction logic, and access control rules.

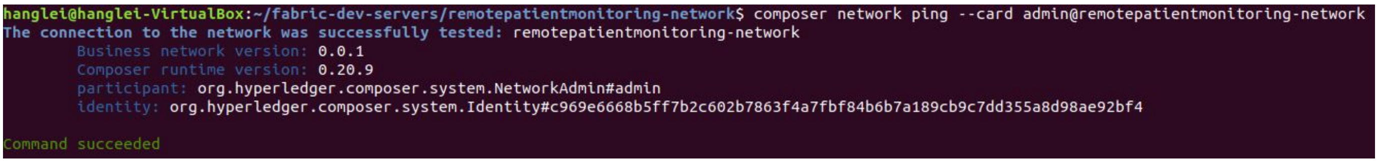
Table II depicts a definition and example of the model in the remote patient monitoring Blockchain business network. Furthermore, the transaction logic comprises transaction processor functions that detail the JavaScript logic to execute the transactions defined in the model. Furthermore, the access control rules precise permissions granted to participants regarding transactions and assets. It is worth mentioning that hyperledger composer playground is used to test the business network definition. After the Business Network Definition (BND), a Business Network Archive (BNA) represented by a (.bna) file has been created. This file is used to package the BND and deploy it to the instance of Hyperledger Fabric. During this process, an admin identity for the business network is issued. Figure 2 shows that the BNA has been deployed successfully.

Based on the business network, Hyperledger Composer is used for generating a REST Server. The latter includes Representational State Transfer (REST) Application Programming Interfaces (APIs) used for the creation of web services as illustrated in Fig. 3.

V. SECURITY ANALYSIS

This section also explains how the proposed system satisfies the security and privacy requirements.

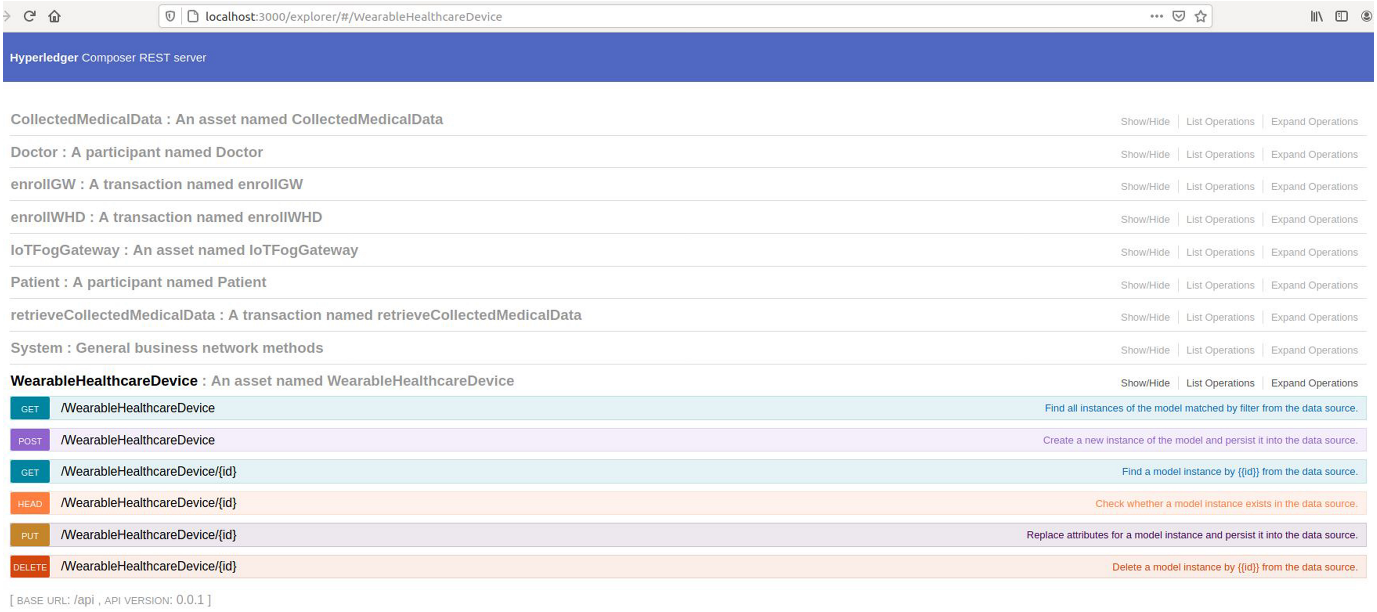
- **Data integrity:** The vital signs data are encrypted and stored into chained blocks. Those blocks constitute an immutable distributed ledger as each block stores the hash value of the previous block. Since all the blocks are linked, any modification in the original data will result in a change in its hash value and, therefore, it is computationally difficult to alter the ledger.
- **Confidentiality:** In the context of healthcare, confidentiality concerns the non-disclosure of patient data. This sensitive data must not be accessed by unauthorized stakeholders. In the proposed system, only the permissioned or authenticated participants can have access to the medical data of a specific patient for a particular session. Since we have adopted a patient centric approach in which the patient manage his private data, the confidential nature of health data is preserved.
- **Availability:** The proposed system guarantees that authenticated and allowed participants can access data whenever they request it. Using decentralized and distributed nodes to handle patient medical data produces a system with no single point of failure. In consequence, no single node of the system can stop the entire from working. This proposed approach ensures continuous uptime and healthcare business continuity.
- **Traceability:** Blockchain network can trace and record all the transactions related to enrolling assets and participants. It also allows participants to visualize the



```
hanglei@hanglei-VirtualBox:~/fabric-dev-servers/remotepatientmonitoring-network$ composer network ping --card admin@remotepatientmonitoring-network
The connection to the network was successfully tested: remotepatientmonitoring-network
        Business network version: 0.0.1
        Composer runtime version: 0.20.9
        participant: org.hyperledger.composer.system.NetworkAdmin#admin
        identity: org.hyperledger.composer.system.Identity#c969e6668b5ff7b2c602b7863f4a7fbf84b6b7a189cb9c7dd355a8d98ae92bf4

Command succeeded
```

Fig. 2: Deployment of business network archive.



localhost:3000/explorer/#/WearableHealthcareDevice

Hyperledger Composer REST server

CollectedMedicalData : An asset named CollectedMedicalData

Doctor : A participant named Doctor

enrollGW : A transaction named enrollGW

enrollWHD : A transaction named enrollWHD

IoTFogGateway : An asset named IoTFogGateway

Patient : A participant named Patient

retrieveCollectedMedicalData : A transaction named retrieveCollectedMedicalData

System : General business network methods

WearableHealthcareDevice : An asset named WearableHealthcareDevice

GET /WearableHealthcareDevice — Find all instances of the model matched by filter from the data source.

POST /WearableHealthcareDevice — Create a new instance of the model and persist it into the data source.

GET /WearableHealthcareDevice/{id} — Find a model instance by {{id}} from the data source.

HEAD /WearableHealthcareDevice/{id} — Check whether a model instance exists in the data source.

PUT /WearableHealthcareDevice/{id} — Replace attributes for a model instance and persist it into the data source.

DELETE /WearableHealthcareDevice/{id} — Delete a model instance by {{id}} from the data source.

[BASE URL: /api , API VERSION: 0.0.1]

Fig. 3: Hyperledger composer REST server for RPM application.

current state database which represents the latest key values known to the channel. It is worth noting that all transactions are immutable and timestamped.

- **Scalability:** The proposed system stores distributed ledgers and transactions in cloud storage. Hence, the proposed system is capable of processing large datasets at low latency. Thereby, this approach resolves the scalability issue in the existing techniques.
- **Data privacy:** The proposed RPM system provides proper handling of patient medical data. Initially, we have used a permissioned consortium Blockchain in order to allow only specific participants to benefit from the proposed healthcare services. Also, we have implemented access control policies for those participants. In essence, access control permission rules precise who is allowed and to which sensitive data has access. Besides, We have adopted a patient centric approach system where the patient has full control to grant or deny access permissions to the authorized parties.

VI. COMPARATIVE ANALYSIS AND DISCUSSIONS

This section provides a comparative analysis of the proposed Blockchain-based RPM system against the existing similar Blockchain based implementations reviewed in the related work section such as [5], [6], [7], [8], [9] and [10]. The comparative analysis focuses on major security and privacy requirements such as data integrity, confidentiality, availability, traceability, data privacy and scalability.

In fact, the authors of [5] focused on a secure configuration management and monitoring of IoT devices using Blockchain to control access to dowloading and uploading IoT devices configuration. Note that the research paper deals with IoT devices in general and in particular the proposed approach could be applied to Healthcare IoT devices. For Security requirements, the proposed approach ensures that only authenticated and authorized users can handle IoT devices configuration. So, configuration integrity , data confidentiality and privacy are satisfied. But the availability and scalability of the proposed solution are not justified by the proposed approach. In addition, the authors of [6] used Ethereum Blockchain and solidity language to implement the smart contract which is different to the technologies adopted for our proposed system. Moreover, the secure automated remote patient monitoring system proposed has a major limitation in scalability context as collected data is stored in a specific hospital.

In [7], the authors proposed a consortium Blockchain based on Java implementation for healthcare data sharing. Despite using encryption, privacy is not totally fulfilled as medical data is stored in local databases with the frequent intervention of healthcare providers is needed.

The authors of [8] proposed two separate Blockchains: one for the IoT devices and the second for medical consultation.

They stored collected medical data directly in the Blockchain which issued a major problem of scalability as the ledger has a limited capacity of storage. In [9], the authors proposed advanced cryptographic techniques deployed over the Ethereum Blockchain network to secure data and transactions. In the proposed model, security requirements consisting of integrity, confidentiality, availability, data privacy and scalability are addressed. But traceability is not evaluated by the authors.

In [10], a hybrid Ethereum Blockchain was integrated with IoT and cloud to built secure remote patient monitoring. Data integrity is assured through a distributed ledger. Confidentiality is addressed as only authenticated and authorized users have access to the Blockchain network. Availability is assured as no single point of failure due to the decentralized services. Scalability is satisfied through cloud storage which is extensible. Traceability is ensured via timestamped transactions. But, data privacy is not totally satisfied as the adopted Blockchain is hybrid and many healthcare providers can view patient data.

The comparison of the proposed method against other methods in state-of-the-art with respect to security, operational and privacy research aspects as depicted in Table I gives a piece of evidence that the proposed RPM system overcomes some limitations of some existing systems, specifically in scalability and data privacy, while accomplishing the standard security requirements according to the CIA security triad.

An attacker to the proposed Blockchain-based solution might be a malicious node in the application network layer that sniffs, alters or denies the communication between a doctor and its patient. An attacker might be also a malicious node from the perception layer or the network layer that creates false transactions. It might be also a part of cloud storage that changes or deletes stored medical data. The proposed solution aims to mitigate or prevent different kinds of attacks such as sniffing attacks, man-in-the-middle attacks, distributed denial-of-Service attacks, and data breaching attacks.

VII. CONCLUSIONS AND FUTURE WORK

This study has designed and deployed a Blockchain-based solution for a secure and privacy-aware remote patient monitoring (RPM) system. In the proposed solution, a patient's medical data is collected from wearable healthcare devices through an IoT Fog gateway. The Wearable Health Devices (WHD) and the IoT Fog Gateway (GW) are considered assets for a permissioned Blockchain that is built on Hyperledger Fabric. To define and deploy the business model in Hyperledger Fabric, Hyperledger Composer has been used to generate a REST API consumed by a Mobile Web Application (RPMApp). All transactions and distributed ledger of a Blockchain network are stored in the cloud to provide faster service and scalability.

The proposed system addresses security issues such as spoofing attacks through using fabric certificates, tampering threats thanks to cryptographic measures deployed, and repudiation threats using fabric digital signatures. Moreover, the proposed RPM system is considered patient-centred that increases data confidentiality and privacy. The proposed RPM system has been evaluated against reviewed prominent systems available in the literature. The initial results have proved that the proposed system ensures security requirements, data privacy, and scalability. The possible future tendencies of this work are to test the interoperability of the proposed system with different IoT frameworks.

REFERENCES

[1] T. Frikha, A. Chaari, F. Chaabane, O. Cheikhrouhou, and A. Zaguia, "Healthcare and fitness data management using the iot-based blockchain platform," *Journal of Healthcare Engineering*, vol. 2021, 2021.

[2] M. Ijaz, G. Li, L. Lin, O. Cheikhrouhou, H. Hamam, and A. Noor, "Integration and applications of fog computing and cloud computing based on the internet of things for provision of healthcare services at home," *Electronics*, vol. 10, no. 9, p. 1077, 2021.

[3] O. Cheikhrouhou, R. Mahmud, R. Zouari, M. Ibrahim, A. Zaguia, and T. N. Gia, "One-dimensional cnn approach for ecg arrhythmia analysis in fog-cloud environments," *IEEE Access*, 2021.

[4] G. Tripathi, M. A. Ahad, and S. Paiva, "S2hs-a blockchain based approach for smart healthcare system," in *Healthcare*, vol. 8, no. 1. Elsevier, 2020, p. 100391.

[5] K. Košt'ál, P. Helebrandt, M. Belluš, M. Ries, and I. Kotuliak, "Management and monitoring of IoT devices using blockchain," *Sensors*, vol. 19, no. 4, p. 856, 2019.

[6] K. N. Griggs, O. Ossipova, C. P. Kohlios, A. N. Baccarini, E. A. Howson, and T. Hayajneh, "Healthcare blockchain system using smart contracts for secure automated remote patient monitoring," *Journal of medical systems*, vol. 42, no. 7, p. 130, 2018.

[7] B. Shen, J. Guo, and Y. Yang, "Medchain: efficient healthcare data sharing via blockchain," *Applied sciences*, vol. 9, no. 6, p. 1207, 2019.

[8] O. Attia, I. Khoufi, A. Laouiti, and C. Adjih, "An iot-blockchain architecture based on hyperledger framework for healthcare monitoring application," in *2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*. IEEE, 2019, pp. 1–5.

[9] A. D. Dwivedi, G. Srivastava, S. Dhar, and R. Singh, "A decentralized privacy-preserving healthcare blockchain for iot," *Sensors*, vol. 19, no. 2, p. 326, 2019.

[10] H. Wang, "IoT based clinical sensor data management and transfer using blockchain technology," *Journal of ISMAC*, vol. 2, no. 03, pp. 154–159, 2020.

[11] H. Fabric, "A blockchain platform for the enterprise," 2018.

[12] "Hyperledger-Composer," https://www.investopedia.com/terms/h/hyperledger-composer.asp, accessed: 2021-02-17.

[13] F. Jamil, O. Cheikhrouhou, H. Jamil, A. Koubaa, A. Derhab, and M. A. Ferrag, "Petroblock: a blockchain-based payment mechanism for fueling smart vehicles," *Applied Sciences*, vol. 11, no. 7, p. 3055, 2021.

[14] A. Derhab, M. Guerroumi, M. Belaoued, and O. Cheikhrouhou, "Bmc-sdn: blockchain-based multicontroller architecture for secure software-defined networks," *Wireless Communications and Mobile Computing*, vol. 2021, 2021.

[15] A. Allouch, O. Cheikhrouhou, A. Koubâa, K. Toumi, M. Khalgui, and T. Nguyen Gia, "Utm-chain: blockchain-based secure unmanned traffic management for internet of drones," *Sensors*, vol. 21, no. 9, p. 3049, 2021.

[16] A. Allouche, A. Koubaa, M. Khalgui, and O. Cheikhrouhou, "Blockchain-based solution for internet of drones security and privacy," Jul. 8 2021, uS Patent App. 16/733,451.

[17] M. Amadeo, C. Campolo, A. Molinaro, and N. Mitton, "Named data networking: A natural design for data collection in wireless sensor networks," in *2013 IFIP wireless days (WD)*. IEEE, 2013, pp. 1–6.

[18] L. Malina, J. Hajny, P. Dzurenda, and S. Ricci, "Lightweight ring signatures for decentralized privacy-preserving transactions," in *ICETE (2)*, 2018, pp. 692–697.

[19] M. Dabbagh, M. Kakavand, M. Tahir, and A. Amphawan, "Performance analysis of blockchain platforms: Empirical evaluation of hyperledger fabric and ethereum," in *2020 IEEE 2nd International Conference on Artificial Intelligence in Engineering and Technology (IICAIET)*. IEEE, 2020, pp. 1–6.

[20] D. Li, W. E. Wong, and J. Guo, "A survey on blockchain for enterprise using hyperledger fabric and composer," in *2019 6th International Conference on Dependable Systems and Their Applications (DSA)*. IEEE, 2020, pp. 71–80.