Remote Secured Monitoring Application for Respiratory Ventilator Implementations

Sérgio Branco[1(✉)], Ertugrul Dogruluk[1], Pedro Mestre[1,2,4], Carlos Ferreira[1], Rui Cordeiro[1], Rui Teixeira[1], João Valente[1], Bruno Gaspar[3], and Jorge Cabral[1,4]

[1] CEiiA Centro de Engenharia e Desenvolvimento de Produto, 4450-017 Matosinhos, Portugal
{antonio.branco,ertugrul.dogruluk,pedro.mestre, carlos.ferreira,rui.cordeiro,rui.pteixeira,joao.valente, jorge.cabral}@ceiia.com

[2] Universtity of Trás-os-Montes e Alto Douro, Vila Real, Portugal

[3] NOS Comunicações, 1600-404 Lisboa, Portugal
bruno.gaspar@nos.pt

[4] ALGORITMI Research Centre/LASI, University of Minho, 4800-058 Guimarães, Portugal

https://www.ceiia.com, https://www.utad.pt, https://www.nos.pt/, https://algoritmi.uminho.pt

Abstract. Internet of Things (IoT) applications have recently significantly increased, especially in health-related services. This movement also brings security issues to the applications, especially for those where the life of patients can be put in risk. This work presents the implementation of an application with remote monitoring for real respiratory ventilator implementation scenarios. To provide secure communications for the devices and applications, a custom protocol (Blackwing) was used. This protocol provides integrity and confidentiality to the application and also has as an objective to be lightweight and micro-service oriented. Lastly, communications from the ventilators are integrated using an architecture for IoT based on a mediator that allows the integration with devices that use other communication protocols.

Keywords: IoT · Remote health IoT application · Respiratory Ventilator · IoT Mediator

A. Cunha et al. (Eds.): MobiHealth 2022, LNICST 484, pp. 338–346, 2023.
https://doi.org/10.1007/978-3-031-32029-3_28

1 Introduction

Recently, the interaction between devices and the Internet has increased significantly. The Internet of Things (IoT) technologies attempt to answer these needs by providing various communication designs, methodologies, network technologies, and others. IoT applications can also answer to health-related services such as patient health tracking, medication supply management, hospital/billing records, remote patient health monitoring, etc. [3].

Therefore an area of research that has increasingly been the target of the research community. In fact, in the literature, we can find several health service-related IoT solutions and their applications. For instance, wearable health sensors and intelligent medicine packages (iMedBox and iMedPack) application are proposed by [9]. The work [5] proposed and deployed a health IoT application (IoTM) monitoring cardiopulmonary functions. Authors of [7] proposed a solution to optimize the management of medicines for patients or elderly users. In [2], it is described the mobile health architecture for the IoT technologies and discussed connectivity, low-power-based devices, and wearable health applications to monitor ECG, blood sugar level, etc. The work [6] developed an IoT architecture for remotely monitoring service with the support of efficient software engines such as rapid summarization for effective prognosis (RASPRO) and criticality measure index (CMI), which are deployed at edge IoT services. This remote monitoring tool is deployed in a hospital to be an alternative clinical device for remote monitoring. Last but not least, in [1], it used a user-centered design (UCD) to analyze the users' requirements and intention of usage for the m-health approaches.

In this work, it is proposed a solution, based on IoT technologies, to monitor respiratory ventilators in a medical environment. These ventilators are connected using a custom protocol that is being tested for this type of applications. This protocol is named Blackwing. It is based on standard encryption algorithms, and uses a two phase communication (as we can find in other protocols): in the first phase asymmetric encryption is used to exchange encryption and authentication information, and in the second phase, a symmetric key is used to cipher the information.

To aggregate the information from the ventilators an architecture based on a Mediator is used. This Mediator architecture will allow the integration of other medical devices that can be using other protocols. Also, data from the ventilators are made available for remote access to the medical staff.

This work is organized as follows: Introduction, the current section, summarizes the related works within the motivation of the IoT healthcare services and presents the motivations and objectives for deployment of a secure remote respiratory ventilator application. Section 2 summarizes the literature review on IoT healthcare services architectures and the implementation of remote monitoring tools/applications. Section 3 introduces the main contribution of this paper by presenting the developed work and the results related to the monitoring application and the used security protocol. Finally, Sect. 4 concludes this work's findings.

2 Health Applications in the Internet of the Things

Within increasing to Machine-to-Machine communication and devices is leading to IoT applications to be increased significantly. For instance, healthcare-related IoT applications cover several implementations such as intelligent health patient monitoring, vehicular emerging services tracing, healthcare, structural health, hospital patient records, etc. The health-related applications have the capability or requires to enable real-time or remote patient monitoring [8].

All health-related applications require service, performance, reliability, and integrity to maintain available services, access patient information and health-related platforms or applications.

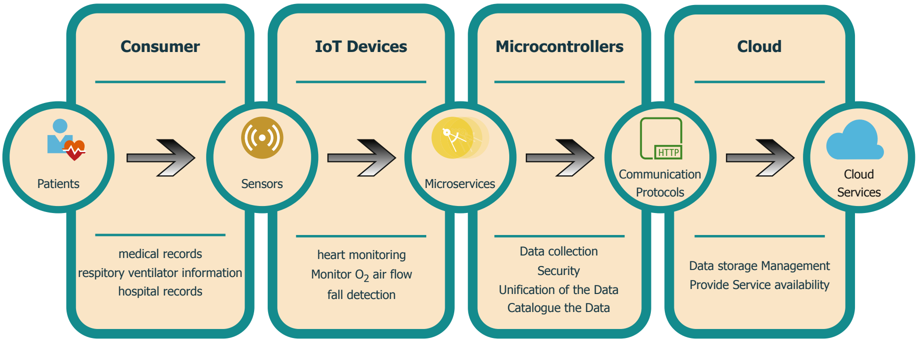

Fig. 1. Health IoT structure

Figure 1 illustrates the health IoT system architecture. The system starts by receiving patient or health data (respiratory ventilator, hospital/patient records, emergency service tracing, etc.) through IoT devices (sensors). Then, micro-services granted lightweight protocols to bring health IoT services independent of other complex architectures. Finally, using communication protocols (HTTP, NB-IoT, and others), the health IoT data or services are secured and maintained by cloud providers. Additionally, some cloud providers can support service availability (*e.g.* Kubernetes) to maintain the services up and running.

2.1 Design a Mobile Secured Respiratory Monitoring Architecture

The recent movement of IoT architectures brings smart and easy accessibility to applications. These services can be to tracking the emergency services, monitoring the patient health records, alarming depending on the patient situation, etc. Because these IoT services are crucial and must be reliable, security and other related services matter.

In this work, we have created a secured application to monitor real respiratory ventilator devices remotely. The application supports a user-friendly interface to analyze patient data. A protocol also secures this architecture for the application at the application layer, which will be explained next.

3 Remote Respiratory Ventilator Application

Other works propose several monitoring applications for IoT implementations. However, secure remote application on the specific m-health IoT implementation is a lack in the literature.

Fig. 2. Health IoT structure

A remote monitoring service or application is required in hospitals or other related services. In this work, the application was created to monitor and analyze the patient parameters in real-time. This health IoT application analyzes respiratory ventilator devices using Internet Protocol.

Fig. 3. Defining the parameters for the respiratory ventilator machine

Figure 2 illustrates the application dashboard interface. The application mainly illustrates the following main parameters: - Pressure, Flow, Volume, PPeak, PEEP, MVe, TVe, and RR from the respiratory ventilator device, which is called Atena.

Figures 3 and 4 illustrate the inserting of the auxiliary parameters for the device (respiratory ventilator). These parameters include the ventilation modes/settings, Alarms, and Patient details (sex, age, weight, and height). The PSV backup settings include 1;E, Rate, Positive end expiratory pressure (PEEP), and inspiratory pressure (Plnsp). Under the setting also ventilator setting includes parameters the Insp/Exp hold, O_2, and Flow calibrations.

Fig. 4. Defining the parameters for the respiratory ventilator machine

In device modes, the Fraction of inspired oxygen (F_iO_2), PEEP, Rate, Tidal Volume, transpulmonary pressure (TP_i), Flow, inspiratory time: expiratory time (I: E), Pinssp, Slope, Trigger Flow, and other settings for the ventilator.

Figure 5 illustrates the secured application on the remote device. This application is synchronized with the Atena respiratory device in real-time. The application also supports remotely setting the patients' data. The remote application was tested to meet the requirement to be accessed remotely through the Internet.

3.1 Securing the Monitoring Application

This work considers all IoT-related services critical and must be secured to maintain the services' integrity. To do so, we have used a specific security protocol at the application layer to maintain the application service integrity. This security tool is called Blackwing and uses encryption between endpoints. Blackwing protocol uses both asymmetric and symmetric encryption to secure data transmission. In the initial phase, RSA is used to cipher the initial communication parameters and to cipher an AES key negotiated between the client and the server. In all other transactions, communications are encrypted using that key [4].

Fig. 5. Application with the Atena Respiratory Ventilator

Blackwing works based on a micro-service architecture. When a client sends information to the server, it specifies which micro-service will handle that request. In this work setup, the Blackwing tool is used to secure the data between Atena (respiratory ventilator device) and Application device micro-services.

The remote secured application we developed supports monitoring/managing multiple devices in this work. Figure 6 illustrates the real-time application dashboard for the five ventilator devices. Each ventilator device can be managed remotely by setting the parameters of the patient, device, and others.

Figure 7 illustrates the application performance with a network analyzing tool on real Atena ventilator devices. We deployed five respiratory ventilator devices in this experiment, as presented previously. The results are obtained for Packets/sec. for the application dashboard. As expected during the application dashboard, the traffic is increasing, and 150 packets/s are obtained from five ventilators.

3.2 Integration with an IoT Mediator

Using devices from different IoT manufacturers and applications can be challenging when integrating devices and applications. Distinctive IoT health brands, databases, communication protocols, and others can be problematic in communicating with other health IoT architectures. For example, various data sets, patient billing, ventilator records, tracing patient information, etc., can increase the complexity of health-related IoT architectures.

Fig. 6. Multiple Atena Respiratory Ventilators in the Application

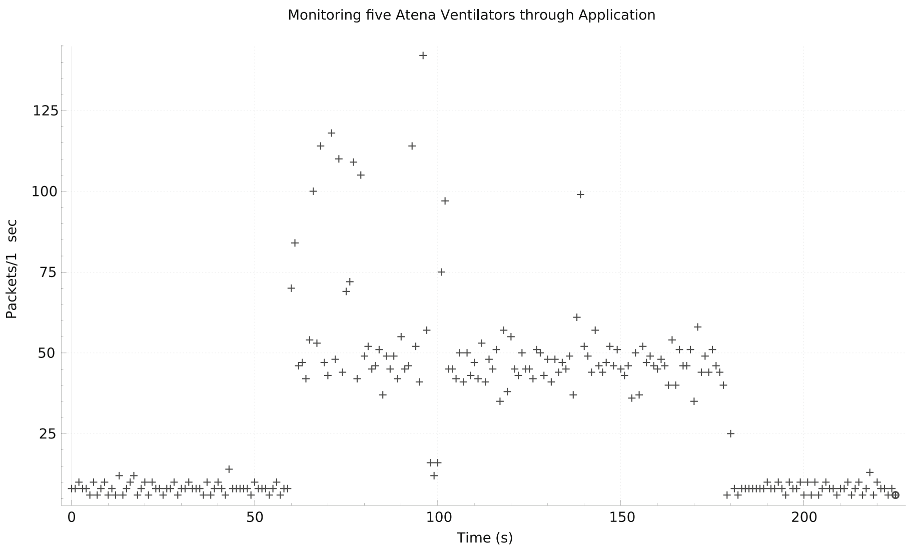

Fig. 7. Application with the Atena Respiratory Ventilator

The IoT mediator (another definition is “platform”) overcomes the challenges identified above. IoT platform makes the IoT architecture(s) understandable and easy to manage between IoT architectures. In addition to the respiratory ventilator application, this work also proposes an adaption to the IoT mediator.

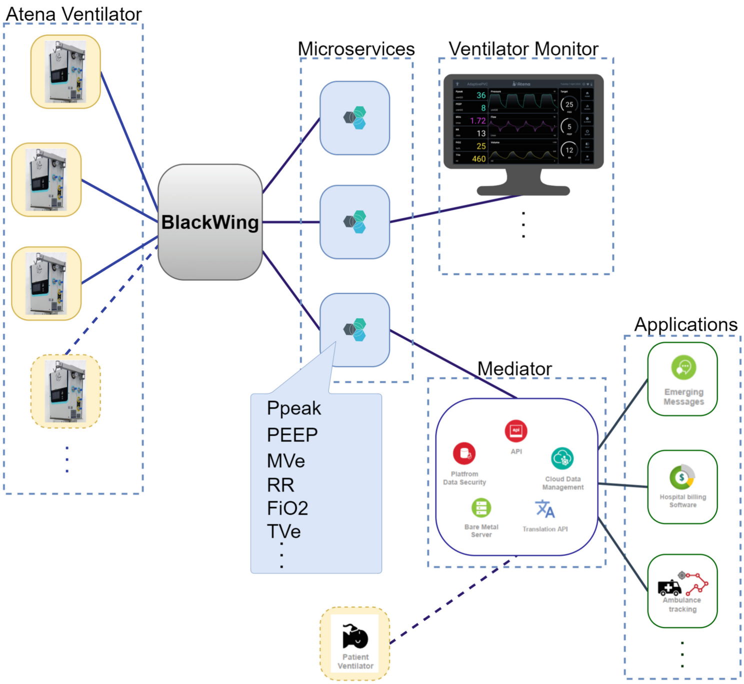

Fig. 8. Atena Respiratory Ventilator adaption the Mediator

Figure 8 illustrates the proposal of health IoT device adaption to the IoT Mediator, as also stated for future works. In this mediator adaption architecture, the Ventilator devices use the Blackwing security protocol to get managed micro-services (e.g., Ventilator parameters) and then use through the Mediator, which answers the applications and other ventilator brands.

4 Conclusions and Future Works

This work presented a remote secured monitoring application for a real respiratory device called Atena. Preliminary findings with traffic analyzing tools for a remote monitoring application edge side. Additionally, a security protocol was adapted to keep the application and device integrity for the edge consumers and server.

Lastly, to maintain services availability and integrity of the monitoring application, an IoT mediator integration is modeled, and this work is stated as a future work.

Acknowledgements. Project "(Link4S)ustainability - A new generation connectivity system for creation and integration of networks of objects for new sustainability paradigms [POCI-01-0247-FEDER-046122 | LISBOA-01-0247-FEDER-046122]" is financed by the Operational Competitiveness and Internationalization Programmes COMPETE 2020 and LISBOA 2020, under the PORTUGAL 2020 Partnership Agreement, and through the European Structural and Investment Funds in the FEDER component.

References

1. Afrizal, S.H., Hidayanto, A.N., Hakiem, N., Sartono, A., Priyambodo, S., Eryando, T.: Design of mHealth application for integrating antenatal care service in primary health care: a user-centered approach. In: Proceedings of 2019 4th International Conference on Informatics and Computing, ICIC 2019 2, 0–5 (2019). https://doi.org/10.1109/ICIC47613.2019.8985911
2. Almotiri, S.H., Khan, M.A., Alghamdi, M.A.: Mobile health (m-Health) system in the context of IoT. In: Proceedings - 2016 4th International Conference on Future Internet of Things and Cloud Workshops, W-FiCloud 2016, pp. 39–42 (2016). https://doi.org/10.1109/W-FiCloud.2016.24
3. Bhuiyan, M.N., Rahman, M.M., Billah, M.M., Saha, D.: Internet of Things (IoT): a review of its enabling technologies in healthcare applications, standards protocols, security, and market opportunities. IEEE Internet Things J. **8**(13), 10474–10498 (2021). https://doi.org/10.1109/JIOT.2021.3062630
4. Branco, S.: Blackwing Specifications (2018). https://blackwing.readthedocs.io
5. Liu, J., Miao, F., Yin, L., Pang, Z., Li, Y.: A noncontact ballistocardiography-based IoMT system for cardiopulmonary health monitoring of discharged COVID-19 patients. IEEE Internet Things J. **8**(21), 15807–15817 (2021). https://doi.org/10.1109/JIOT.2021.3063549
6. Pathinarupothi, R.K., Durga, P., Rangan, E.S.: IoT-based smart edge for global health: remote monitoring with severity detection and alerts transmission. IEEE Internet Things J. **6**(2), 2449–2462 (2019). https://doi.org/10.1109/JIOT.2018.2870068, https://ieeexplore.ieee.org/document/8464257/
7. Pinto, A., Correia, A., Alves, R., Matos, P., Ascensão, J., Camelo, D.: eHealthCare - A Medication Monitoring Approach for the Elderly People. In: Gao, X., Jamalipour, A., Guo, L. (eds.) MobiHealth 2021. LNICST, vol. 440, pp. 221–234. Springer, Cham (2022). https://doi.org/10.1007/978-3-031-06368-8_15, https://link.springer.com/10.1007/978-3-031-06368-815
8. Stoyanova, M., Nikoloudakis, Y., Panagiotakis, S., Pallis, E., Markakis, E.K.: A survey on the internet of things (IoT) forensics: challenges, approaches, and open issues. IEEE Commun. Surv. Tutorials **22**(2), 1191–1221 (2020). https://doi.org/10.1109/COMST.2019.2962586
9. Yang, G., et al.: A fealth-IoT platform based on the integration of intelligent packaging, unobtrusive bio-sensor, and intelligent medicine box. IEEE Trans. Industr. Inf. **10**(4), 2180–2191 (2014). https://doi.org/10.1109/TII.2014.2307795