The Last Mile of M-Connected-Healthcare in the Covid Age: Data Sharing at Large Scale

Alberto Faro
Innovative Start-up
DeepSensing srl
Catania, Italy
albfaro@deepsensing.it

Daniela Giordano
Dept. of Electrical, Electronics and Computer Eng. Univ. of. Catania, Italy
IEEE Senior Member, ISAFOM Associate
daniela.giordano@dieei.unict.it

Mario Venticinque
Ist. per i Sistemi Agricoli e FOrestali del Mediterraneo (ISAFOM) CNR
Catania, Italy
mario.venticinque@cnr.it

2020 IEEE International Conference on Internet of Things and Intelligence System (IoTaIS) | 978-1-7281-9448-6/20/$31.00 ©2021 IEEE | DOI: 10.1109/IoTaIS50849.2021.9359706

Abstract— **Aim of the paper is to illustrate a platform for that supports the link between the patient and doctors, family members, clinical laboratories and hospitals, that is a platform that supports the last mile between patients and the entire healthcare network so that the personal data collected by edge devices don't remain confined locally at the patient side but are shared at large scale to aid the patients anywhere and anytime. In particular the paper illustrates from the engineering point of view how implementing the last mile for Covid monitoring and control in practice by means of available Cyber Physical Systems (CPSs), i.e., edge IoT devices provided with communication and computational functions, freeware home control systems and low cost relevant web services available on the market. The key element of our proposal is the one of using a portable BLE/MQTT gateway or to develop DIY MQTT sensors to allow health measurements taken by edge devices to be sent to a remote automated control system supervised by a doctor. A detailed analysis is carried out on the contact and contactless sensors that can be integrated in our platform from the more and more diffused smart bands and ibeacons until the IR thermal cameras. For each considered sensor, the paper discusses its integration it in the platform and the global scenario in which it may be used effectively**

Keywords - Cyber Physical Systems, M-Connected-Healthcare, Covid-19, Ubiquitous and Pervasive Systems.

I. Introduction

A layered platform to ubiquitous monitor and control people health status by means of edge devices was proposed by the authors in a previous paper to manage common needs for home automation and healthcare [1]. This platform, denoted as CSPc, was inspired by the communication and basic services of the Cyber Physical System (CPS) model [2]. Fig.1 shows the main functions of such platform where the first level consists of sensors and actuators controlled by automation systems at the second level which on its turn are coordinated by customer processes at the third level. The main feature of such platform is interoperability between elements at the same level by using the services offered by the elements at lower level.

In the healthcare, such interoperability aims at supporting the link between the patient and doctors, family members, clinical laboratories and hospitals, that is at supporting the *last mile* between patients and the entire healthcare network as defined in [3] so that the personal data collected by edge devices don't remain confined locally at the patient side but are shared at large scale to aid the patients anywhere and anytime.

This problem may be solved by a platform that satisfies three main requirements: 1) people should be monitored by edge devices able to send the sensed data through internet, 2) the sensed data and the commands issued by the automation systems should be formatted according to an agreed technical format, and 3) the data collected by sensors in a network may be used to activate actions of actuators located in a network with a different administrator.

As shown in fig.1, the CSPc model may be extended to deal with other aspects of the last mile in healthcare such as delivery of medicines from pharmacies to individual households or collection of test tubes for clinical analysis laboratory as described in [4], [5]. This aspect is not covered in this paper mainly dedicated to people monitoring and control from distance, however it is currently under study due to the increasing demand of such service from elderly people and from the ones living in rural areas.

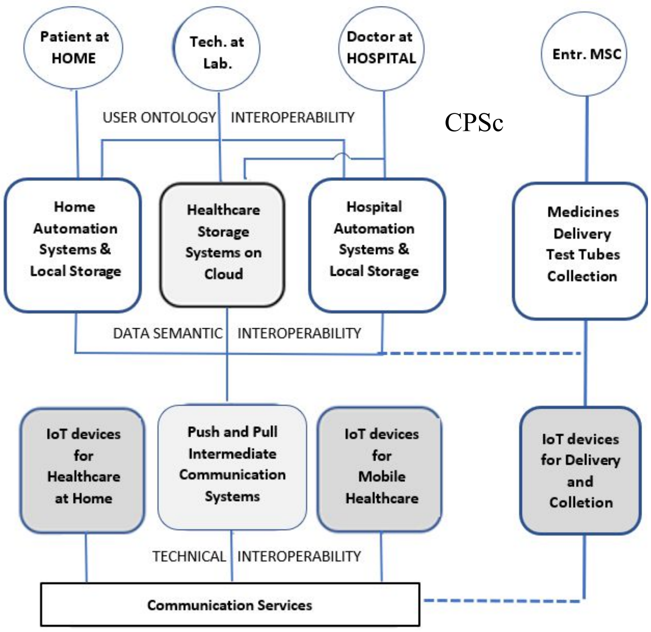

Fig. 1. Layered functional model to meet common healthcare needs. The user processes at third layer deal with: patients at home, technicians of clinical laboratories, doctors at hospital, entrepreneurs for the medical supply chain (MSC). The MSC part on the right is not covered on the paper.

Requirements 1 and 2 aiming at continuously monitoring and control people by sensors and actuators connected to internet have been discussed in [1], where we outlined also how to support edge device internetworking to meet requirement 3.

Aim of this paper is to illustrate from the engineering point of view how the mentioned requirements can be satisfied for Covid-19 monitoring and control by means of Cyber Physical Systems (CPSs) available on the market consisting of IoT devices provided with communication and computational functions. Sect.2 finalizes the general solutions proposed in the previous paper for managing the Covid-19 epidemy by proposing how linking in practice people to the healthcare network by means of CPSs. Sect.3 illustrates how implementing in practice the above functional architecture by using devices on the market or DIY (i.e., Do It Yourself) solutions to meet the *last mile* requirements in the main scenarios involving people and the healthcare network in the Covid-19 era.

II. DEVICES NETWORING/INTERNETWORKING TO COVER THE LAST MILE IN COVID-19 HEALTHCARE

The sensors and actuators available on the market are mainly provided with Bluetooth Low Energy (BLE), Radio frequency (RF), WiFi and 3G/4G/5G communication channels. However, they are generally not conceived to be supervised by a remote control service chosen by the user to allow family doctors or doctors at the hospital to make timely decisions. More frequently the edge devices send the data to a smart phone where it is implemented an APP for fitness or to a proprietary server to execute more complex control actions.

Instead. in our healthcare we require that hospitals make available on the global network the devices needed by remote patients, and vice-versa that patients make available to a remote hospital the home devices that are useful to monitor/control their pathology from distance. Also, patient health status should be monitored by family members or family doctors as well as some specific health parameters should be controlled when people enters into commercial, transportation and education services at urban scale.

Therefore, our use scenarios involve the networking of several devices belonging to different organizations that cannot be included in the same network for several reasons such as: security, maintenance flexibility, organization rules and property rights. For this reason, we propose a platform for the internetworking of several healthcare networks: the healthcare network at home or at work and the networks of the organizations providing sanitary assistance to the users and the ones that provide services to citizens.

Namely, each network is currently managed by a proper control system and does not share data to the others, whereas patients are more and more interested that devices of different networks exchange data to obtain sanitary services at global scale. In particular, it is not only demanded to alert doctors and family member at distance, but also to share data at global scale to allow the data collected at home may be used by devices at hospital.

Therefore, in each network of our platform the edge devices should be able to send/receive data to/from a control center indicated by the users and to cooperate with remote devices belonging to different networks. The first problem is that the healthcare edge devices have been conceived originally to exchange data

Thus in each network of our platform the edge devices should be able to send/receive data to/from a control center indicated by the users and to cooperate with remote devices belonging to different networks. The first problem is that the healthcare edge devices have been conceived originally to exchange data only with the smart phone or with the server of the manufacturers. For this reason, a portable micro gateway was proposed in [1] to transform the data sensed by the sensors contained in the BLE, RF, WiFi and 3G/4G/5G frames into JSON frames to be inserted into MQTT messages to be sent to an MQTT broker [6].

Also, we proposed that the MQTT broker should be linked directly to the automation system Domoticz [7] to meet time performance. The reasons to use Domoticz and the secure version of the MQTT protocol were explained in [1], where we clarified that this meets communication security and low energy consumption. To point out how privacy and service continuity are satisfied we consider the following frequent scenarios involving the last mile in healthcare: Sa) edge devices, MQTT broker and Domoticz are resident on the same LAN, and Sb) edge device is resident on a LAN different from the one in which there are the MQTT broker and Domoticz.

The former case deals with the monitoring of an user at the holiday home or walking. As a tentative solution we may satisfy his demand to be monitored by devices T1h/O1h and T1m/O1m by connecting them to the MQTT broker and Domoticz at the home network.

The latter case deals with the monitoring of the user by devices T1o and O1o when he is at his office. In this case, the user demand could be that T1o and O1o will be connected to the MQTT broker at office that on its turn is controlled by Domoticz at home. In both cases the last mile may be covered if the sensors at home or at the office are able to exchange data with MQTT broker and Domoticz in the same network, e.g., by using MQTT sensors.

However, the mentioned tentative solutions point out that in both cases the remote devices should send the MQTT messages to the MQTT broker resident at the home LAN by means of VPN connections and/or according to a suitable security policy to protect MQTT broker and Domoticz by means of password and SSL certificates.

To avoid to overload the home systems, in fig.2 we suggest to manage these two cases by a broker on Cloud, e.g., CloudMQTT (www.cloudmqtt.com). In this way all the remote devices and Domoticz will interact externally using the security policy of the broker on the Cloud.

Fig.3 points out a less frequent but important scenario Sc in which, the walking user as well as the user at the holiday home or at office cannot be coordinated from both Domoticz at home and Domoticz at hospital although they need that their edge devices should cooperate with the ones at hospital. This situation should be managed carefully to avoid conflicts about the data interpretation and system faults, and to preserve maintenance flexibility and property rights.

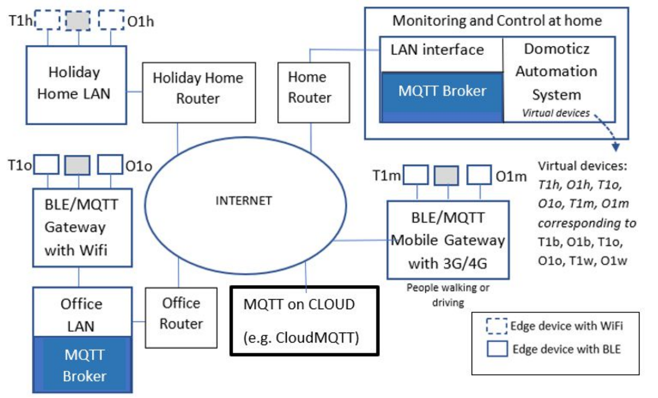

Fig. 2. Edge device networking in scenarios Sa and Sb, where T and O indicate respectively Thermometer and Oximeter. The MQTT brokers in the blue areas are not needed if Domoticz uses the Cloud MQTT broker.

.

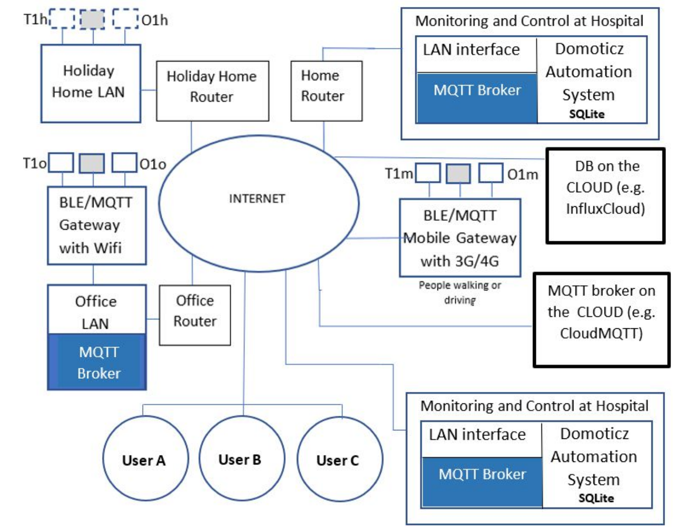

Fig. 3. Edge device networking in scenario Sc. MQTT brokers in the blue areas and local DBs to extend SQLite are not needed if Domoticz systems use MQTT broker and DB on the Cloud.

To clarify how to manage such critical use case, in fig.4 we show how an MQTT Sonoff switch should be configured to measure Temperature and Humidity at home. Its configuration is obtained by a web browser using its local address (e.g., 192.168.1.x, where x ranges from 2 to 255). The configuration mainly consists of three sections: WiFi, MQTT and Domoticz.

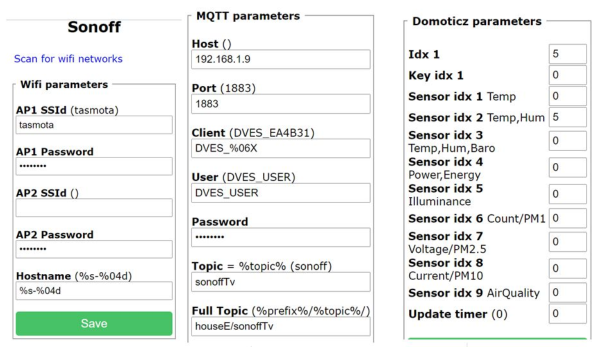

Fig. 4. Parameters for Sonoff switch configuration

Therefore, to configure any MQTT devices we should know address and password of the router of its WiFi LAN, the local address and port of the MQTT broker, the MQTT topic associated to the device and its Domoticz identifier. Of course, all these data cannot be shared between Domoticz at home and the one at hospital since the administrator at hospital could change the home network configuration.

A partial way to overcome such problem is using the MQTT topics associated to the edge devices. In fact this allows an MQTT APP on a smart phone of a doctor at hospital (see fig.5) to visualize from distance the values of the edge devices by knowing only the global address of the home router or the public address of the CloudMQTT (and related passwords) and the relevant topics.

Also, the knowledge of the global address of the home router allows distant doctors to visualize through the APP Domoticz the status of the edge devices of their interest and the historical data collected by such device (fig.6).

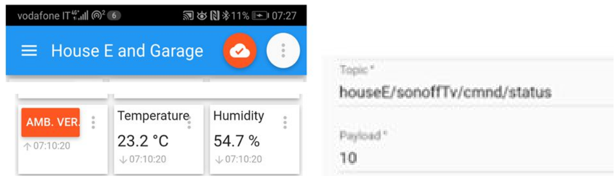

Fig. 5. MQTT APP to visualize the data collected by an edge device using the JSON formula on the right

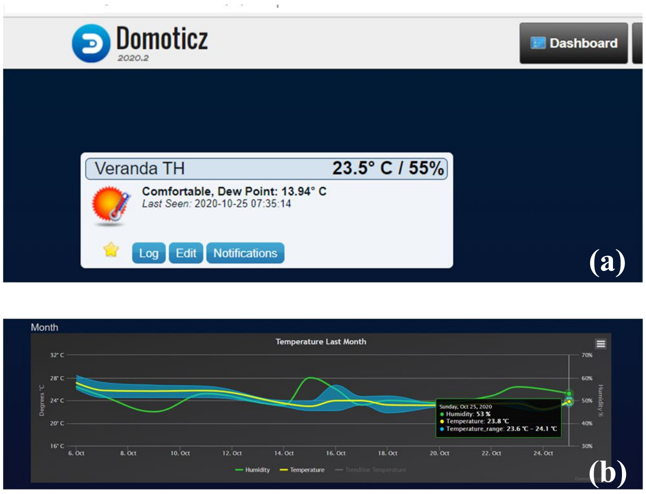

Fig. 6. Domoticz APP to visualize the data collected by edge devices and to visualize how they evolve in time.

In both cases, the administrators can authorize the users, i.e., the doctors, to carry out only subscribe/publish (read/write) operations related to specific topics (devices). But this does not allow the devices to be managed by both local and remote Domoticz systems. In fact, a modification of the topics or device identifiers has to be notified by an administrator to the other one. This involves a certain rigidity since device reconfiguration cannot be done freely by the legitimated administrator.

A better way to overcome the problem is using an intermediate web service to allow any device to cooperate at a large scale with another one without providing the name of its topic or the Domoticz identifier. To this aim we can use

Beebotte [8] and IFTTT [9] to allow the device internetworking by means of a global naming scheme.

Beebotte (Bb) is a *platform as service* available on the web that behaves as a broker on which the devices can publish messages to be received by other devices by means of subscribe operations. In this case the edge devices exchange data through an intermediate virtual Beebotte device so that a data sensed by an edge device will published on this virtual Beebotte device that on its turn will be received by the remote edge device by a subscribing operation.

IFTTT is a web service that allow an edge device to execute commands in the format: *IF This* (event) *Then That* (action), where the event is detected by a device of a network A, whereas the action should be carried out by a device resident on the same network A or on a network B identified by its IFTTT global name.

Both IFTTT and Beebotte can be integrated with Domoticz so that an event detected by an edge device controlled by a Domoticz may activate actions on devices belonging to a network managed by a Domoticz with a different administrator. Only devices made available on the global network by the administrators will cooperate at large.

Also, reconfiguration or restarting of the edge devices could be solicited by this intermediate service in case of malfunctioning thus increasing the service continuity. In principle, IFTTT is suitable to send alert messages from a device to remote ones, whereas Beebotte is more useful to send data sensed by a device to a remote device for further processing at the distant site.

To complete the implementation of the CPS model of fig.1 we should clarify how the users at the third level may interact with the automation systems. If the users behave as administrators, they can enter into the MQTT brokers and Domoticz using certified passwords clarified above.

If they are interested in processing the collected data, we suggest, as shown in fig.3, that the users don't use the data stored on the SQLite files internal to Domoticz, but the ones stored on external databases suitable to manage time-series data coming from IoT devices, such as Influx Cloud (influxdata. com) [10]. How specific tools, such as Grafana (grafana.com), to graphically represent the Influx data or Decision Support Systems carried out by intensive computing processes is for further works.

III. Last Mile to Covid-19 monitor/control: practical solutions for the main scenarios

As above said, the healthcare edge devices that meet our requirements are devices able to send/receive MQTT messages to/from an MQTT broker residing on the server defined by the user. Although edge devices are mainly provided with BLE interface, often they are not able to send MQTT messages to the server chosen by the user where there are the MQTT broker and the Domoticz automation system.

In this section we discuss how to integrate in practice in our platform the edge devices relevant for Covid-19, i.e., the ones related to body temperature, oxygen in the blood and respiration rate. Other parameters to evaluate the severity level of the disease, e.g., the blood pressure and heart beats per minute, may be measured by many BLE smart bands available on the market. The sensed data may be sent to the MQTT broker using the outlined BLE/MQTT gateway.

A. Contact and contactless Thermometers

IR thermometers are widely used to check the forehead temperature of the people entering into the public services. Both stand alone gun laser thermometers not provided with BLE and BLE laser guns, e.g., the one produced by Kinsa, may be used for this aim.

The former devices cannot be included in our platform and are relevant only for a local control, on the contrary the latter devices may be included in our global platform at condition that they are used having nearby a BLE/MQTT gateway such as the gateway based on ESP32 [11] illustrated in the same fig.7-up.

Two ESP32 gateways were proposed by he authors in a previous paper [1]. Both gateways consists of ESPP32 chips widely diffused also for healthcare measurement. They are provided with a BLE antenna to detect and decodify the BLE frame: the first is provided with an interface to 3G/4G/5G, and the second with a LAN module to send data to the local WiFi network.

Let us note that to this aim it is necessary that the MQTT gateway decodifies the BLE frames sent by the thermometer to the smart phone so that it is possible for it to send the bytes representing the body temperature to the MQTT broker. The BLE frame may be decodified easily if the manufacturers provide the frame format otherwise this should be obtained by BLE sniffers. This is not a general solution, but we tested that this is possible for many BLE thermometers.

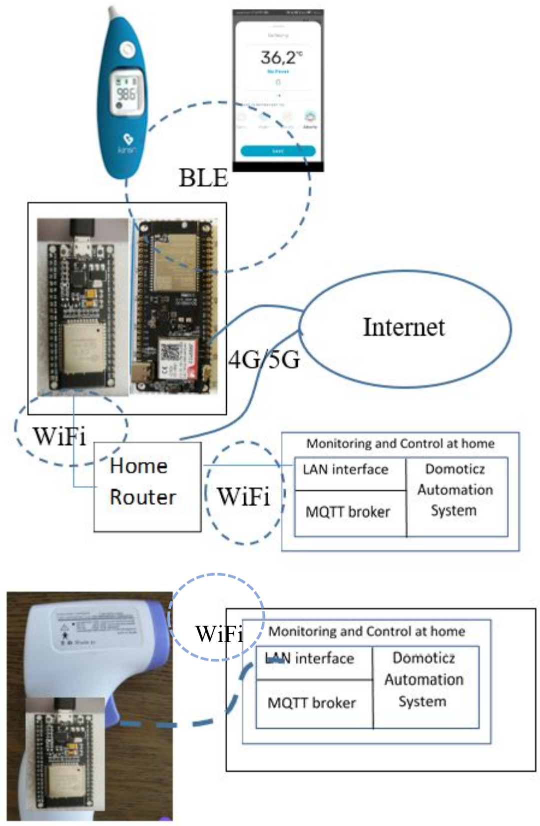

Fig.7 . How Integrating BLE thermometers and MQTT IR laser guns in the platform

A further step to meet our requirements may be the one of using the MQTT IR thermometer, e.g., the one shown in fig.7-down. It is an IR laser gun in which the internal PBX that links sensor, display and command buttons is substituted by an ESP32 chip provided with WiFi antenna able to send the sensed data to the display and to the MQTT broker residing in the server defined by the user.

Two IR sensors are available on this laser gun, i.e., the MLXBAAB and MLXDCI to detect the forehead temperature of a subject from about 10 to 30 cm of distance with an accuracy of ±0,3ºC.

Also, BLE thermometers consisting of small plates conceived to check the body temperature of children may be used with satisfactory accuracy. In all these cases, we should use a gateway to extract from the BLE frames the body temperatures to be sent to the MQTT broker.

Accuracy of about ±0,1 ºC may be obtained by DIY projects that use sensors such as the MLX30205 linked to an ESP32 board by the I2C interface (fig.8). The MQTT gateway may be implemented in the same ESP32 board.

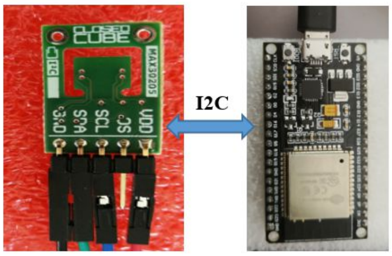

Fig. 8.MQTT thermometer using MLX30205 sensor

Recently, IP thermal cameras are more and more diffused to measure facial temperature for two main reasons: the first is that they may be used at a medium distance (of about 2-3 meters) while the user is walking.

The second reason is that the IR cameras are able to provide both facial temperature and face recognition when they are used at a relatively low distance (of about 0.3-0,5 meters), thus allowing us to check the entrance of people to public services if they are in good health conditions and are authorized to enter.

These IP thermal camera partially meet our requirements. Indeed they may be installed everywhere by means of a mobile router or by linking them to the RJ45 sockets of a LAN, but only personnel connected to the same LAN or to the same mobile router can receive and control the images taken by the camera as shown in fig.10.

Remote personnel connected to another network are not able to check the images of the people at the entrance, even if they may be informed when some people is not allowed to enter, e.g., since he is without mask, or with high temperature or he is not authorized.

This can be obtained (see fig.9) connecting the signal provided by the cameras in suspected cases to a Sonoff switch for not opening the entrance and sending an alarm to a remote device through the IFTTT or Beebotte service.

Moreover, if the body temperature is close to the upper limit, the entering people may ask for a double check by an online laser gun, e.g., the MQTT laser gun in fig.10, to decide if his body temperature meets the requirement by using a more accurate thermometer.

Just in case the measurement is below the prefixed threshold (usually of 37.5 °C) , the IR thermometer will send the authorization message to the Sonoff switch controlling the entrance door to allow the people to enter into the service.

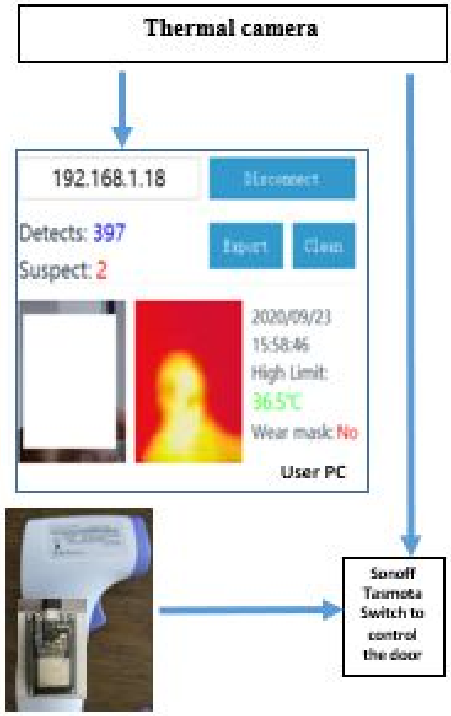

Fig. 9. Entrance controlled by: thermal camera, Sonoff switch and IR MQTT laser gun.

B. Blood oxygen level and Respiration rate

Blood oxygen level (or SpO2 level) and respiration rate are more specific to discover Covid-19 disease with respect to the body temperature since this disease is a severe lung disease highly involving the respiration activity.

The available sensors to measure the blood oxygen are mainly contact sensors although there are some studies about the possibility to detect SpO2 level using IR cameras, e.g., [12]. However, such studies are still at research level, and consequently the current less invasive way to measure SpO2 level by a contact device is the one of using a finger optical pulse oximeter.

Analogously, the respiration rate may be measured using contact devices, e.g., by chest straps, small plates measuring the neck micro movements during respiration, and recently by means of a finger device named Mightysat[TM] by Masimo able to measure both SpO2 level and respiration rate. The use of thermal cameras is also in this case at research level [13].

Due to the difficulties of using straps and small plates, the most suitable devices to integrate in our platform are the BLE oximeters, e.g., the ones by Happy Electronics and

Mightysat™ in fig.10.center, to measure SpO2 and the respiration rate from the modifications of the user plethysmograph waveform [14]. Fig.10 includes also:

- wrist watches such as TICWRIS tested successfully to measure body temperature and SpO2, and the wrist band Polar H9 currently under study to measure respiration rate from ECG.
- a DIY MQTT band based on MLX30205 and MAX86150 supervised by ESP32 is under development to obtain all the need measurements by a single device, i.e., body temperature, SpO2, and respiration rate.

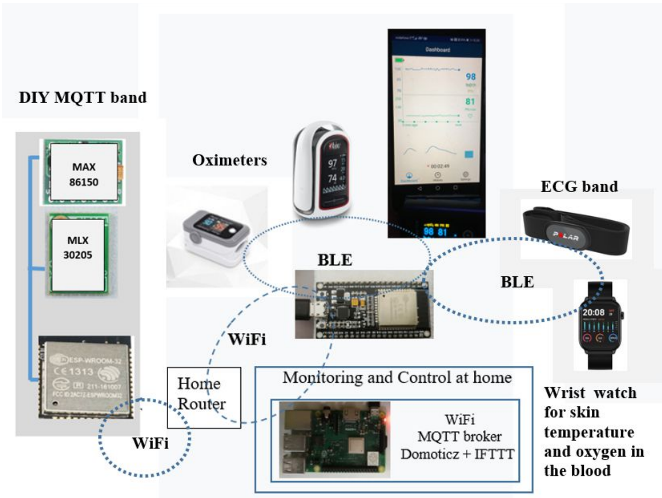

Fig.10. Integrating DIY bands, BLE oximeters, ECG bands, wrist watches into the platform.

IV. Concluding Remarks

The paper illustrated how to implement a monitoring and control system to manage global events such the Covid-19 pandemy involving the cooperation of many health devices belonging to different administrative systems. How MQTT broker and metrological DB on Cloud may improve scalability, security, and flexibility of the platform was discussed.

The paper proposed also how implementing the platform by using common IoT devices, freeware home control systems and relevant web services available on the market.

The platform is under test in the projects IHOSP and SELCA supported by EC regional funds aiming at remote monitoring a hundred of patients affected by complex pathology. In this case, the use of Domoticz at both patient and hospital sides is feasible since each Domoticz system is able to manage until 255 devices. In SELCA we are also testing the medical supply chain and the management of the clinical analysis of people with limited mobility.

It is for further study how available plugins and a set of cooperating Domoticz systems allow us to implement an automation system to control a larger number of devices. Alternative solutions based on the Influx DB are also under study. Since the use of thermal images for healthcare is more and more demanded, two MQTT IR cameras based on Heimann and Melexis thermal sensors are under development. Filters for denoising [15] , [16] and techniques to improve accuracy [17] of the thermal images are under test.

Further studies are planned to forecast the Covid-19 diffusion using the data collected by the proposed platform and a machine leaning algorithm based on the one described in [18]. By this system we aim at improving the available Covid-19 forecast systems such as the one proposed by Kinsa based on how the body temperature of people residing in certain areas increases in time, e.g., https: //health weather. us, and the one based on the Covid-19 tracking, e.g., https://coronavirus. jhu.edu/.

References

[1] A. Faro, D. Giordano, M.Venticinque, Deploying WiFi, RF and BLE sensors for pervasive monitoring and control, IEEE Conf. on Metrology for Industry 4.0, Rome, Italy, 2020

[2] H. Gill, NSF perspective and status on cyber–physical systems, NSF Workshop on Cyber–physical Systems, National Science Foundation, Austin, USA, 2006

[3] W.H. Bradford, Role of the Internet in Solving the Last Mile Problem in Medicine" J Med Internet Res 2019 (Oct 28); 21(10), 2008

[4] J. Babaian, The last mile in healthcare, Nov. 2018 https:// hcldr.wordpress.com/2018/11/06/the-last-mile-in-healthcare/

[5] S.S.S. Abbabathula, N. Kuntagod, R.E. Rote and S. Podder, Last Mile Healthcare Through Micro-entrepreneurs, 2020 IEEE International Conference on Software Architecture Companion (ICSA-C), Salvador, Brazil, 2020, pp. 181-184, 2020.

[6] A. Stanford-Clark, H.L. Truong, MQTT For Sensor Networks, https://mqtt.org/new/wp-content/uploads/200906/MQTT-SN_nspec_ nv1.2.npdf, 2013

[7] Domoticz, Open Source Home Automation System, https://www.domoticz.com/DomoticzManual.pdf, 2015

[8] Beebotte, https://beebotte.com 2017

[9] M. Xianghang, et al., An empirical characterization of IFTTT: ecosystem, usage, and performance, IMC, London, UK, 2017

[10] A. Struckov et al., Evaluation of modern tools and techniques for storing time-series data. Procedia Computer Science 156 (2019) 19–28

[11] N. Qunoot, et al., Design Healthcare system using Raspberry PI and ESP32, International Journal of Computer Applications, NY, USA, Vol. 177 – N.36, 2020

[12] M. Tepper, Thermal imaging method for estimating oxygen saturation Journal of Biomedical Optics Sept./Oct. 2009

[13] J. Ruminski, A. Kwasniewska Evaluation of Respiration Rate Using Thermal Imaging in Mobile Conditions. In: Ng E., Etehadtavakol M. (eds) Appl. of Infrared to Biomedical Sciences. Series in BioEngineering. Springer, 2017

[14] P.H. Charlton et al., Breathing Rate Estimation From the Electrocardiogram and Photoplethysmogram: A Review, in IEEE Reviews in Biomedical Engineering, vol. 11, pp. 2-20, 2018

[15] F. Cannavò, G. Nunnari, D. Giordano, C. Spampinato, Variational Method for Image Denoising by Distributed Genetic Algorithms on GRID Environment. WETICE'06 : 15th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, Manchester, UK. June 2006

[16] S. Budzan, Wyżgolik, Noise Reduction in Thermal Images. In: Chmielewski L.J., Kozera R., Shin BS., Wojciechowski K. (eds) Computer Vision and Graphics.,ICCVG 2014. Lecture Notes in Computer Science,vol 8671 Springer,2014

[17] Y. Zhanga et al., An experimental method for improving temperature measurement accuracy of infrared thermal imager, Infrared Physics & Technology Volume 102, November 2019

[18] A. Faro, D. Giordano, F. Maiorana, Spampinato C., Discovering Genes-Diseases Associations From Specialized Literature Using the Grid, 2009, IEEE Transactions on Information Technology in Biomedicine, vol. 13, no. 4, 2009