information

IMPACT FACTOR 3.1

CITESCORE 5.8

Article

An Internet of Things Approach to Contact Tracing—The BubbleBox System

Andrea Polenta, Pietro Rignanese, Paolo Sernani, Nicola Falcionelli, Dagmawi Neway Mekuria, Selene Tomassini and Aldo Franco Dragoni

Special Issue

Ubiquitous Sensing for Smart Health Monitoring

Edited by

Dr. Yusuf A. Bhagat

MDPI

https://doi.org/10.3390/info11070347

information

MDPI

Article

An Internet of Things Approach to Contact Tracing—The BubbleBox System

Andrea Polenta, Pietro Rignanese, Paolo Sernani *, Nicola Falcionelli, Dagmawi Neway Mekuria †, Selene Tomassini and Aldo Franco Dragoni *

Dipartimento di Ingegneria dell'Informazione, Università Politecnica delle Marche, Via Brecce Bianche 12, 60131 Ancona, Italy; S1088280@studenti.univpm.it (A.P.); S1088279@studenti.univpm.it (P.R.); n.falcionelli@pm.univpm.it (N.F.); d.n.mekuria@pm.univpm.it (D.N.M.); s.tomassini@pm.univpm.it (S.T.)

* Correspondence: p.sernani@univpm.it (P.S.); a.f.dragoni@univpm.it (A.F.D.)

† This author passed away on 30 May 2020.

Received: 8 June 2020; Accepted: 30 June 2020; Published: 3 July 2020

Abstract: The COVID-19 pandemic exploded at the beginning of 2020, with over four million cases in five months, overwhelming the healthcare sector. Several national governments decided to adopt containment measures, such as lockdowns, social distancing, and quarantine. Among these measures, contact tracing can contribute in bringing under control the outbreak, as quickly identifying contacts to isolate suspected cases can limit the number of infected people. In this paper we present BubbleBox, a system relying on a dedicated device to perform contact tracing. BubbleBox integrates Internet of Things and software technologies into different components to achieve its goal—providing a tool to quickly react to further outbreaks, by allowing health operators to rapidly reach and test possible infected people. This paper describes the BubbleBox architecture, presents its prototype implementation, and discusses its pros and cons, also dealing with privacy concerns.

Keywords: contact tracing; BubbleBox; E-health; privacy; COVID-19; IoT

1. Introduction

The COVID-19 is a pandemic disease that arose between the end of 2019 and the beginning of 2020 in China [1]. At the time of writing, it has infected over 4 million people and has caused over three hundred thousand deaths worldwide [2]. The outbreak of this novel disease forced governments to adopt containment measures for the pandemic, such as social distancing and quarantine [3]. Among these measures, isolation and identification of contacts, that is, contact tracing, are of paramount importance, as they could contribute to containing the outbreak or bring it under control over a longer time period [4]. In the early days of the outbreak, with few cases, contact tracing could be done manually, while the growth of cases made it more difficult [5]. For these reasons, several proposals to automate the contact tracing have been presented [6–12], using smartphones' Bluetooth connectivity or GPS location history to perform the tracing.

In this paper, we present BubbleBox, a system combining Internet of Things (IoT) and software technologies to detect and limit further outbreaks of the COVID-19 infection by performing contact tracing. The main novelty of BubbleBox is the adoption of a dedicated device—instead of using smartphones' Bluetooth or GPS as in the aforementioned proposals, BubbleBox relies on a dedicated Internet of Things (IoT) device, a wristband, to perform the contact tracing. In addition, a web-app serving as the system frontend and a server application as the data backend allow users to pair devices with their identities—this gives authorized medical personnel a means to quickly reach people who might need to be alerted or tested and monitor the spread of the disease. As already recognized by several studies [5,13,14], privacy is of utmost importance for a contact tracing application. In BubbleBox,

while the tracing might be based only on the device, being anonymous, we claim that giving away some personal privacy in favour of the health authorities is acceptable when providing a tool to quickly react to the challenges of the outbreak. In fact, one of the duties of e-health and telemedicine tools is to unburden healthcare providers, at least partially, from the workload pressure caused by the infection [15].

The rest of this paper is organized as follows. Section 2 briefly explains how technologies for e-health can help in facing the outbreak, highlighting the difference of our approach. Section 3 presents BubbleBox, describing in detail the architecture of each system component. Section 4 motivates the need for a dedicated device, discusses the privacy and security aspects in BubbleBox, and presents the BubbleBox prototype implementation. Finally, Section 5 summarizes our proposal and suggests future works.

2. Related Works

In recent years, several studies in the e-health field have been dedicated to devices and applications to monitor the activities of the users and their health status. In fact, wearable devices and apps have the potential to support users in training activities for sport and fitness [16,17]. Likewise, personal health systems applications take advantage of mobile apps and wearable devices [18,19] to implement self-monitoring protocols and/or telemedicine; for example, market-available smartwatches can be used to detect health conditions such as arrhythmia [20].

In such a context, it is not a surprise that national governments are implementing measures based on mobile apps to help monitor and contain the outbreak of the COVID-19 infection, which surely is an e-health application. In Taiwan, the government decided to use smartphone data to track quarantined people and ensure they remained at home for the necessary time [6]. In Singapore, the government supported the development of the TraceTogether app [7]. The application uses the Bluetooth to exchange anonymous tokens between the two smartphones involved in a contact. Such tokens are uploaded to a server as well, so that the contact is traced. When a user tests positive for COVID-19, she/he is asked to use the app to upload all the tokens generated by her/his smartphone—the people owning the smartphones involved in contacts with those tokens can be called by phone and tested, if necessary, but uniquely by the government or health authorities; contacts are anonymous and users do not know which other users they met. In Italy, a very similar approach is followed with the Immuni app, which works with anonymous tokens exchanged via Bluetooth [8], exactly as the TraceTogether app, without using any GPS-related information. In parallel to applications and developments supported by the governments, universities, research centers, and volunteers started publishing their own proposals about apps for tracing contacts. For example, CoEpi [9], Covid Watch [10], and the Decentralized Privacy-Preserving Proximity Tracing [11] (DP-3T) are all proposing solutions to implement anonymous contact tracing using smartphones' Bluetooth. The application proposed in Reference [12], instead, is based on GPS location history, relying on transformation of data and encryption to preserve privacy.

BubbleBox differs from the cited related works for one key aspect—the contact tracing is based on the usage of a dedicated device, instead of relying completely on the smartphone. A mobile app and a server application are used to complement the BubbleBox services, providing a tool to monitor the outbreak and find who might need to be alerted and tested. However, the contact tracing is performed uniquely with the Wi-Fi and Bluetooth connections of the dedicated device, which can work without any app. In this way, the battery of smartphones and similar portable devices can be saved; moreover, even people who do not want or cannot regularly bring the smartphones can participate in contact tracing.

The cited related works have different degrees of privacy preservation—in Taiwan, the government took the right to perform a complete tracking; in Singapore, users are asked to share their data only if infected; in the DP-3T proposal the privacy is completely decentralized, so that each smartphone manages its own data, and no personal data is collected. In BubbleBox, part of the

personal data are given to the authorized medical personnel to allow a quick reaction to the need of testing or contact people to be alerted. However, the BubbleBox dedicated device can be used without sharing any personal data—in that case it can be used as a device to immediately alert its user when she/he meets other people without respecting the safe social distance.

3. The BubbleBox System

BubbleBox is a set of IoT and software technologies integrated to detect and limit further outbreaks of the COVID-19 infection by performing contact tracing. As such, the BubbleBox system is intended to support:

- the citizens, by tracing and notifying potentially contagious contacts when two or more people break the safe social distance;
- health authorities, in managing patients and their status to rapidly check and get in touch with infected, possibly infected, and quarantined patients;
- researchers and experts, by collecting anonymized data if needed, and offering a data source to precisely monitor the trends in the spread of the infection or the impact of external factors on it [21,22].

To achieve such goals, the BubbleBox system is composed of a wearable device, that is, a wristband, to anonymously trace all the contacts under the safe social distance between the person who wears it and other people; an optional web app which allows users to pair their device with their identity, using a smartphone, tablet or PC; a data backend, which stores such data to make it available to the authorized health personnel and, anonymized, monitor the spread of the infection.

The wristband is in charge of tracing the contacts—it generates a unique id and, thanks to its Wi-Fi module, is able to detect other BubbleBox wristbands within 20 m. In that case, the wristband recovers its BLE module from the deep sleep mode (for battery saving reasons) to detect when another BubbleBox wristband is nearer than the safe social distance (2 m). Through its display, the device shows when the contact occurs as well as the total number of contacts occurred while wearing it. When a known Wi-Fi network is available, the device can automatically upload the contact data to the BubbleBox server—the contact data is composed of the timestamp of the contact, the id of the wristband sending data, and the id of the detected wristband.

The wristband can work as a stand-alone device, without the other components of the BubbleBox system. As such, it informs its user of the contacts occurred under the safe social distance; and, uploading data to the server, it allows to understand how many of such contacts took place at a regional or national level. Therefore, the data collected by the wristbands are completely anonymous and the tracing is decentralized on the devices. However, such data can be paired with the identity of the person wearing the wristband, only if she/he wants to do so. In this regard, the BubbleBox app allows the user to pair a wristband with her/his identity and create an account, pairing wristband and app. The user can use the BubbleBox app as another means to upload the data about contacts with other wristbands, as well as send information about her/his health status to health authorities. For example, the user can use the app to alert that she/he is feeling the symptoms of the infection.

The BubbleBox server infrastructure serves as a data backend. The authorized health personnel can access such data—if the BubbleBox users registered to the platform using the app, the authorized staff can check who informed about symptoms, contacting them immediately; they can update the health status of positive tested patients and check their contacts, in order to decide whether other people should be tested. Thus, through a web frontend, the health authorities can use the data on the server to actively supervise patients, update their status (healthy, with symptoms, positive, in quarantine), and monitor the spreading of the infection outbreak. A schematic representation of the components of the BubbleBox system and their interactions is depicted in Figure 1.

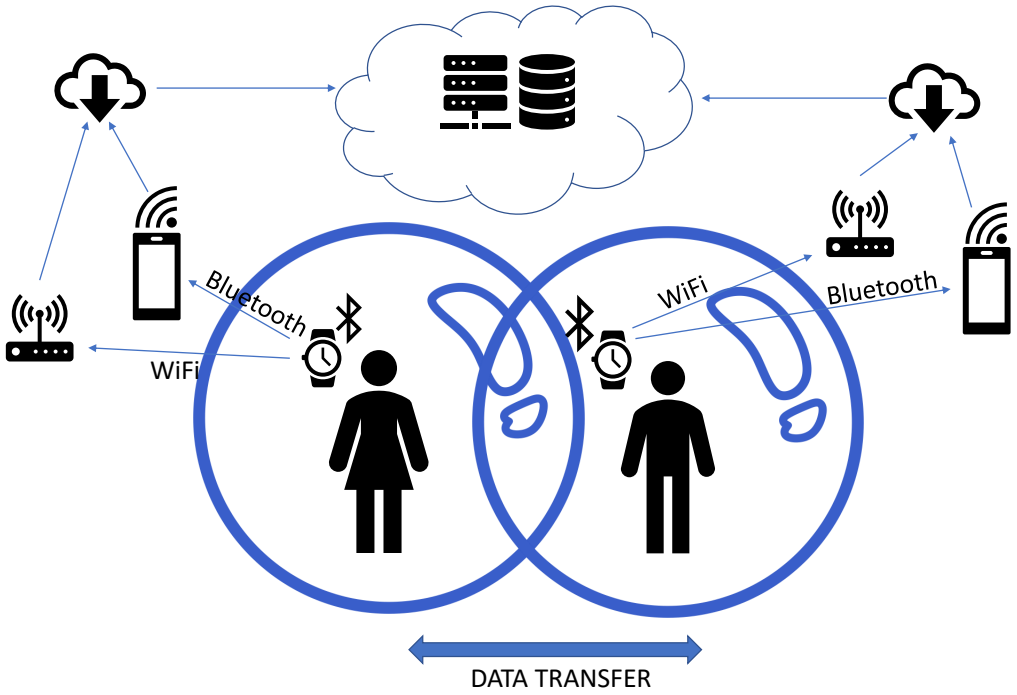

Figure 1. The BubbleBox system is composed of a device, i.e., a wristband to log unsafe contacts, an app, to pair devices and the identities of people wearing them, and a server infrastructure to store data and make it available of the authorized medical personnel.

We understand that using the app to pair the wristband with an identity implies privacy concerns. While the wristband itself is enough to anonymously trace unsafe contacts, we want to offer to health authorities a means to tackle some of the challenges posed by the COVID-19 outbreak—the need to understand who needs to be tested and to rapidly reach them; the management of the infection related data; a quick and precise mapping of the outbreak spreading. We claim that having an infrastructure which allows the pairing of an identity with a device ID helps with facing such challenges, even if it means giving away some privacy in favour of the authorized medical staff.

In the following, we provide a detailed description of each component of the BubbleBox system, namely the BubbleBox Device, that is, the wristband, the BubbleBox App, that is, the front-end of the system to register personal data and pair it with the device, and the Server Infrastructure.

3.1. The BubbleBox Device

The BubbleBox device is a wristband which provides the core functionality of the system—tracing contacts under the safe social distance. In addition, it shows to its user when a contact occurs as well as a counter of the contacts (total or in a time window). These functionalities work without registering the device with the app, and make the device capable of tracing contacts anonymously. The operating components of the device are:

- an Arduino Micro (https://store.arduino.cc/arduino-micro) with the NFR24L01 (https://www.sparkfun.com/datasheets/Components/nRF24L01_prelim_prod_spec_1_2.pdf) module to give it Wi-Fi capabilities. The Arduino Micro is the processing core of the device, managing the other components and logging the contacts. The NFR24L01 module allows it to detect other BubbleBox devices in a range of 20 m, in order to wake up the Bluetooth module and detect when the distance with another device is under the safe social distance. In this way, we save the battery life of the device—the consumption of the Arduino Micro with the NFR24L01 is lower than 15 mAh, whilst the Bluetooth module consumes 50 mAh when it is turned on and only 0.05 mAh when it is in deep sleep mode.

- An ESP32 (https://www.espressif.com/en/products/modules) module to give the device Bluetooth Low Energy (BLE) connectivity. The Received Signal Strength Indicator (RSSI) of the detected devices allows to estimate the relative distance and, thus, trace unsafe contacts.
- A RTC DS3231 (https://datasheets.maximintegrated.com/en/ds/DS3231.pdf) module. It is a real time clock which allows us to get the time and date on the device and, thus, the timestamps of the contacts.
- A OLED display (0.96″) used to shows contacts, time, and date to the user. With the display, two buttons allow the user to connect to Wi-Fi networks via WPS or with the smartphone, via BLE.
- A MicroSD card reader, to log the contact data, sent to the system server when a Wi-Fi network is available.
- A Lithium battery (and its charger), to power the device.

These components are small enough to be assembled as a wristband or a watch, but still usable to execute the tracing task of the BubbleBox device.

As showed in Figure 2, the operation of the BubbleBox device can be summarized in six phases:

1. **Scan of the area.** The Android Micro module, with its NRF24L01, scans a range of 20 m to understand if there are other BubbleBox devices. This preliminary scan is executed with a period of 4 s and allows to save the battery of the device, as this module consumes less power than the ESP32, which stays in deep sleep mode until one or more devices are found.
2. **BubbleBox device found.** When one or more BubbleBox devices are detected, the Arduino Micro wakes the Bluetooth module, that is, the ESP32, from its deep sleep mode.
3. **Bluetooth turned on.** The device information (MAC address, Device name, UUID) becomes available for the Bluetooth scans of the other BubbleBox devices.
4. **Bluetooth scan and distance detection.** The ESP32 module is in charge of scanning the area for other BubbleBox devices and check the distance through RSSI.
5. **Contact detected.** If another device is under the safe social distance (2 m), this has to be considered an unsafe contact.
6. **Contact logged.** The Arduino Micro logs each unsafe contact into its MicroSD card. Using its DS3231 real time clock, the device saves the log <*Date, Time, MyId, OtherId*> where "MyId" and "OtherId", in our tests, were the mac address of the ESP32 modules of user's device and the detected device. In case the ESP32 and the NRF24L01 modules do not detect any other device, the ESP32 module is set back to deep sleep mode.

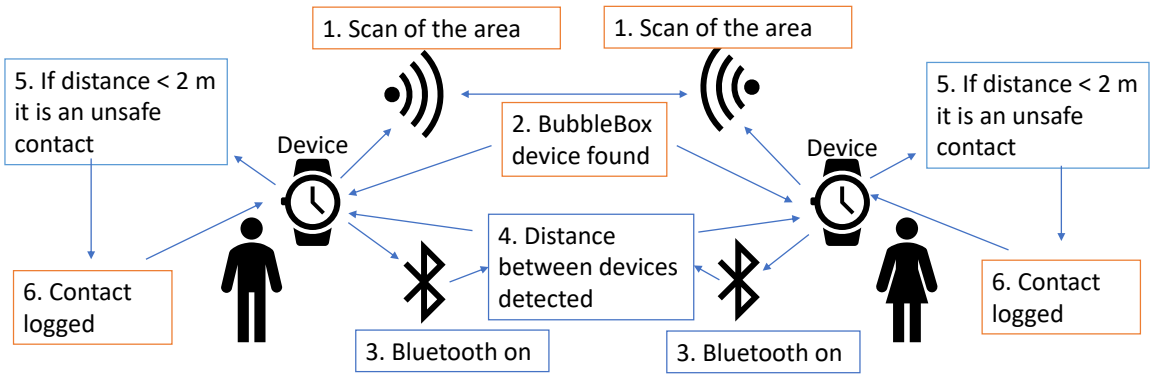

Figure 2. When the Wi-Fi module of a device detects other BubbleBox devices, the Bluetooth module is turned on and, if two devices are nearer than 2 m, a contact is logged.

3.2. The BubbleBox App

The BubbleBox system includes a web app, usable with a PC, a smartphone or a tablet—the user can register the BubbleBox device with her/his identity as well as manage her/his own data.

While such feature might cause some privacy concerns, it would be an advantage for the authorized health personnel able to access to data on the BubbleBox servers—users can report that they have symptoms, and the health staff can check contacts and precisely understand who else needs to be tested. In addition, the users can be contacted immediately, in case they need to be tested or updated about their status.

Figure 3 shows the app when used with a smartphone. When the user starts the app she/he is asked for her/his username and password (Figure 3a). If the user does not have such credentials, she/he can create an account (Figure 3b), filling a form with her/his personal data, such as name, surname, the birth date, and tax code. Once registered, the user can pair her/his device with the app (Figure 3c). This step can be done immediately or anytime from the app main menu. The user is guided step by step during the pairing: she/he is asked to frame a QR code which can be shown in the device display (or available in the device package) to pair the device and the app (Figure 3d,e). As an alternative, the user can register her/his device using a code available on the device or its package.

Figure 3f shows the app main page. Here, the user can check the total number of daily unsafe contacts or the total number in the last 14 days (without any information, of course, on the identity of the other people involved in those contacts). From the main page, the user can rapidly report symptoms. The main page also shows some general rules to stay safe during the outbreak. Finally, in the top-right corner, the user gets a recap of her/his health status in relation to the outbreak. The health status can be:

- sound, if she/he did not report any symptom or has been involved in any unsafe contact with positive people;
- with symptoms, if she/he reported symptoms and need to be tested by the authorized health staff;
- positive, if she/he has been found positive after medical tests;
- in quarantine, if the medical staff decided that the user should stay in quarantine for being in contact with other positive people.

3.3. The BubbleBox Data Backend

A server-side application, that is, the data backend of the BubbleBox system, manages a database to securely store the data collected by the other two components, that is, the device and the app. Therefore, the data backend stores:

- user data of those users who registered with the app;
- the relation which pairs user data and devices, for the registered users;
- the contacts under the safe social distance detected by the device;
- the symptoms report uploaded by the users, and their status related to the outbreak (sound, positive, in quarantine, with symptoms).

This kind of data can help the medical operators, especially those in charge of managing tests and monitor patients, to tackle some of the challenges of the outbreak. In fact, the medical staff with the authorization for the BubbleBox data has additional features in the web-app, with dedicated areas. Specifically, medical operators will use an area to check symptoms reported by users. In addition, they have an area to monitor the status of their patients, modify it, and also send notifications to specific users, for example, in case they need to be tested. Finally, the data can be exported, anonymized, to help monitoring the spreading of the outbreak. With enough people using BubbleBox in a certain area, such data can be used to precisely trace the infection in that specific area.

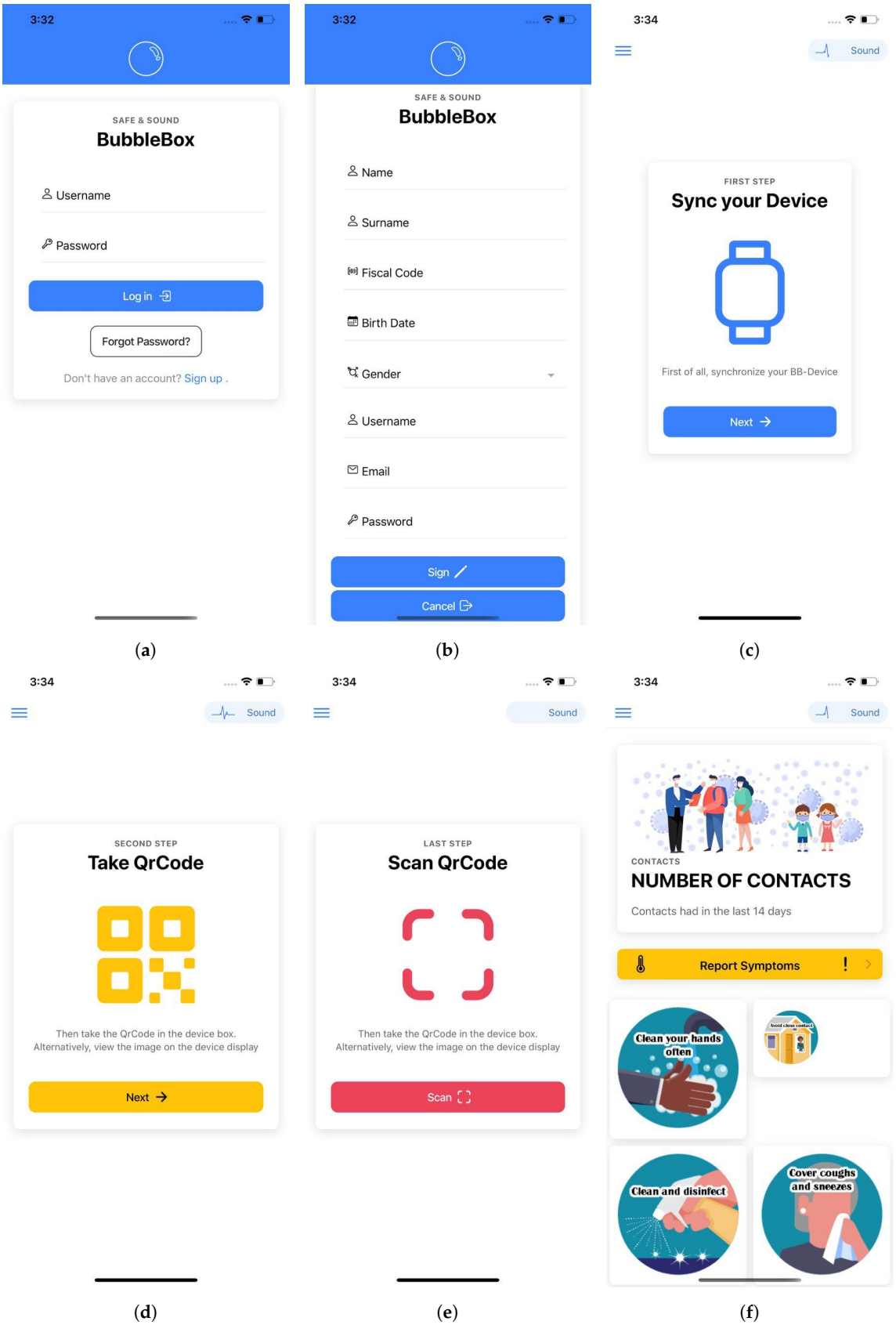

Figure 3. The BubbleBox App, with its home page (**a**); the user registration page (**b**); the pairing with the device with the scan of a QR code (**c**–**e**); and the home page once registration process is completed (**f**).

4. Discussion

The main goal of the BubbleBox system is to use IoT and software technologies to support the management of the COVID-19 outbreak (as well as of other outbreaks in the future). In this regard, in Section 3, we proposed an architecture based on a dedicated device, that is, the wristband, an app for the user, as the system frontend, and a data backend. In this Section, we motivate this choice explaining why BubbleBox, a solution based on the use of dedicated device, might be better than a solution based on the smartphone only. In addition, we discuss about privacy in our proposal; we briefly introduce the details of the prototype implementation used for some preliminary tests, and, finally, we provide an analysis about costs and limitations of our approach.

4.1. Dedicated Device vs. Smartphone

One might argue that BubbleBox could use only the smartphone to perform its tracing task, using smartphones' Bluetooth to estimate the distance with other devices. Relying on the smartphone only for the tracing task would boost the initial adoption of the system thanks to the proliferation of smartphones available in the market—starting using BubbleBox would be as easy as just downloading the dedicated app. However, we advocate the use of a dedicated device instead of relying on the smartphone only:

- using the app on the smartphone for the distance estimation and, therefore, to perform the entire tracing would require to have the Bluetooth always turned on. However, this would cause an energy overhead on commodity smartphones, draining the battery [23]. The dedicated device, instead, has its own battery, so the smartphone battery is consumed as per its normal usage.
- A dedicated device can be used also in places were the user normally does not use or does not want to use the smartphone.
- A dedicated device can be used also by children or older adults, and other people or the medical staff can register for them the device using a PC, a smartphone, or a tablet.

Hence, these reasons support the use of a dedicated device, giving away the chance of using smartphone pervasiveness to boost the initial adoption of the BubbleBox system.

4.2. Privacy and Security

One of the biggest concerns about tracing system to manage the COVID-19 outbreak is about personal privacy—at the moment of writing this paper, specific research is being devoted to this topic [5,14]. In our proposal, the BubbleBox device is able to trace anonymously contacts under the safe social distance. In our tests, the mac address of the device is used as a unique id to log the contacts. While such an id is anonymous, it might suffer from linkage attacks [5], that is, once discovered the identity, such identity will be forever linked with that id. However, the device can be programmed to generate "ephimeral" ids [5,11] which change after a time window, instead of using the mac address as an id. Moreover, the device can work without being paired with an identity, therefore staying anonymous—it can be used just as an indicator of unsafe contacts. However, our claim is that giving away some privacy to government and health authorities can let the medical personnel quickly react to the spread of the infection. In this regard, in the prototype implementation, we used a centralized DBMS on a server application, using regular authentication over HTTPS to access the database. However, in future, BubbleBox, and more in general this kind of applications, might take advantage of a permissioned blockchain, using a distributed ledger such as Hyperledger Fabric [24] to add an additional layer of security.

4.3. Prototype Implementation

To demonstrate the feasibility of BubbleBox, we implemented a prototype version of the system. As shown in Figure 4, we used a breadboard to connect the component described in Subsection 3.1. The goal was to test the distance estimation done by the BubbleBox device. In such a prototype

device, which simulates the wristband, we used the ESP 32 DevKitC (https://www.espressif.com/en/products/devkits/esp32-devkitc/overview) instead of the ESP32 module—the functionalities are the same, but the DevKit perfectly fits into the breadboard. In addition, instead of the Arduino Micro with the NFR24L01 module, we used an Arduino Nano (https://store.arduino.cc/arduino-nano), which embeds the functionalities of both modules. Repeating such configuration with more breadboards, we tested the detection of unsafe contacts with the Bluetooth module, using RSSI. The tests were performed in laboratory settings only to validate the distance estimation—the breadboards were placed at different distances and moved, checking the awakening of the ESP32 module and the distance calculation with RSSI.

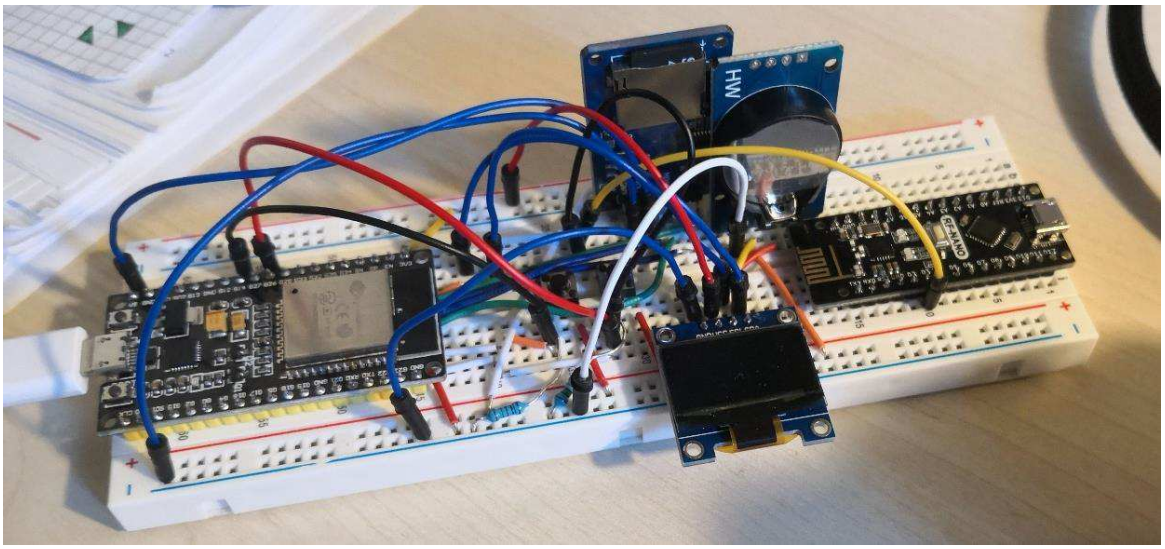

Figure 4. A breadboard with the device components, used to simulate the wristband and, thus, test the distance estimation performed by such device.

Concerning the software components of the system, we developed the prototype of the BubbleBox App (showed in Figure 3) with the Ionic Framework (https://ionicframework.com/). We implemented the prototype of the server app to build the BubbleBox Data Backend with Express JS (https://expressjs.com), using MySQL (https://www.mysql.com) as the Database Management System (DBMS). The interactions between an authenticated BubbleBox App and the backend are based on the HTTP methods GET, POST, PUT, and DELETE.

The source code of each component of the prototype, as well as the implementation of the device are publicly available on a GitHub repository (https://github.com/BubbleB0x).

4.4. Cost Analysis

The device architecture described in Section 3.1 costs around 45–50€ (∼18€ for the Arduino Micro, ∼5€ for the NFR24L01 module, ∼10€ for the ESP32 module, ∼1€ for the real time clock module, ∼5€ for the display, and ∼5€ for the MicroSD card reader). One might argue that the price is too expensive for an IoT device that needs to be distributed to the highest possible portion of the population. However, such costs are those available in the electronics market when buying each item individually. A mass production of the device in its final design would significantly reduce the components' price. In addition to the device costs, development costs for the final mobile application and the data backend need to be taken into account, as well as hosting, maintenance and memory space costs.

4.5. Limitations

The proposed system inevitably suffers from some limitations. Concerning the dedicated device design, this paper suggested a wristband. We used a prototype to test the distance estimation. However, to fully validate the BubbleBox device, usability tests with the proper design are needed to assess the user experience with the wristband and the system, for example, using state-of-the-art scales such as the System Usability Scale (SUS) [25] or the Usability Metrics for User Experience (UMUX) [26]. In fact, assessing the acceptability of the wristband among the users is essential as well as their general satisfaction in interacting with BubbleBox. For example, the users who regularly wear a watch might not like to wear a second wristband, or they might find it uncomfortable. In such cases, possible countermeasures are evaluating different portable designs (e.g., a wallet) and/or adding services to the device, such as fitness tracking and smartwatch functionalities.

In addition, BubbleBox as a digital contact tracing system needs to cover a high portion of the population to be effective [27], being efficient when used by 60–75% of the population [28]. However, this limitation affects contact tracing in general, and possible countermeasures involve the action of national governments which can propose incentives for the usage of digital systems.

5. Conclusions

In this paper we presented BubbleBox, a system integrating an IoT device and a software platform to detect and limit further outbreaks of the COVID-19 infection. As such, BubbleBox aims at supporting both people and health authorities. The BubbleBox device, a wristband, traces contacts under the safe social distance. With a web-app, the users can pair their identity with their device, as well as report their symptoms. In this way, they offer to the authorized medical personnel a quick way to understand the spreading of the infection, monitor who needs to be tested, and easily contact patients. Finally, the collected data, anonymized, can help researchers in understanding trends about the spreading of the infection.

Differently from other proposals in this field, BubbleBox relies on a dedicated device, instead of using the smartphone as the only source for tracing contacts. While this approach does not take advantage of the wide smartphone diffusion in the market for the initial adoption of the system, it certainly saves smartphone battery lives; in addition, it can be effective in monitoring contacts of people who do not own a smartphone such as children or older adults.

Privacy is an important aspect for tracing apps. While the contact tracing is anonymous, in our proposal the users give away part of their privacy to the government and health authorities to help them face the emergency. However, as reported in the Discussion Section, countermeasures to limit the revealed data and enhance security are possible.

As future works, the final BubbleBox device as a wristband has to be designed. With that, proximity tests to estimate the social distance and usability tests are needed to understand the real effectiveness of the system. Usability is crucial to increase the number of people who will use the system and, thus, maximize the coverage of the contact tracing. Moreover, as explained in the Discussion Section, the software infrastructure can be made even more secure and protected implementing a distributed database with blockchains. Finally, as apps and systems to contain the outbreak will surely pop up, there is the need to establish a standard for the collected data, as such systems will be really effective only if interoperable.

Author Contributions: Conceptualization, methodology, software, A.P. and P.R.; validation, P.S., N.F., D.N.M., S.T. and A.F.D.; writing—original draft P.S.; writing—review and editing N.F., D.N.M. and S.T.; supervision A.F.D. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Rothan, H.A.; Byrareddy, S.N. The epidemiology and pathogenesis of coronavirus disease (COVID-19) outbreak. *J. Autoimmun.* **2020**, *109*, 102433. [CrossRef] [PubMed]
2. World Health Organization. WHO Coronavirus Disease (COVID-19) Dashboard. Available online: https://covid19.who.int/ (accessed on 16 May 2020).
3. Anderson, R.M.; Heesterbeek, H.; Klinkenberg, D.; Hollingsworth, T.D. How will country-based mitigation measures influence the course of the COVID-19 epidemic? *Lancet* **2020**, *395*, 931–934. [CrossRef]
4. Hellewell, J.; Abbott, S.; Gimma, A.; Bosse, N.I.; Jarvis, C.I.; Russell, T.W.; Munday, J.D.; Kucharski, A.J.; Edmunds, W.J.; Sun, F.; et al. Feasibility of controlling COVID-19 outbreaks by isolation of cases and contacts. *Lancet Glob. Health* **2020**, *8*, e488–e496. [CrossRef]
5. Cho, H.; Ippolito, D.; Yu, Y.W. Contact Tracing Mobile Apps for COVID-19: Privacy Considerations and Related Trade-offs. *arXiv* **2003**, arXiv:2003.11511.
6. Wang, C.J.; Ng, C.Y.; Brook, R.H. Response to COVID-19 in Taiwan: Big Data Analytics, New Technology, and Proactive Testing. *JAMA* **2020**, *323*, 1341–1342. [CrossRef] [PubMed]
7. Singapore Government Agency. Help Speed Up Contact Tracing with TraceTogether. Available online: https://www.gov.sg/article/help-speed-up-contact-tracing-with-tracetogether (accessed on 15 May 2020).
8. Italian Ministry for Technological Innovation and Digitalization. Immuni: Tutto Quello Che c'è da Sapere e le Risposte del Dipartimento. Available online: https://innovazione.gov.it/Immuni-tutto-quello-che-ce-da-sapere/ (accessed on 15 May 2020).
9. Lewis, D.M.; Leibrand, S. CoEpi: Community Epidemiology in Action. Available online: https://www.coepi.org/ (accessed on 15 May 2020).
10. Von Arx, S; Becker-Mayer, I; Blank, D.; Colligan, J.; Fenwick, R.; Hittle, M.; Ingle, M.; Nash, O.; Nguyen, V.; Petrie, J.; et al. Covid Watch. Slowing the Spread of Infectious Diseases Using Crowdsourced Data. Available online: https://www.covid-watch.org/covid_watch_whitepaper.pdf (accessed on 15 May 2020).
11. Troncoso, C.; Payer, M.; Hubaux, J.-P.; Salathé, M.; Larus, J.; Bugnion, E.; Lueks, W.; Stadler, T.; Pyrgelis, A.; Antonioli, D.; et al. Decentralized Privacy-Preserving Proximity Tracing. Available online: https://github.com/DP-3T/documents (accessed on 2 May 2020).
12. Berke, A.; Bakker, M.; Vepakomma, P.; Larson, K.; Pentland, A.S. Assessing Disease Exposure Risk with Location Data: A Proposal for Cryptographic Preservation of Privacy. *arXiv* **2003**, arXiv:2003.14412.
13. Bell, J.; Butler, D.; Hicks, C.; Crowcroft, J. TraceSecure: Towards Privacy Preserving Contact Tracing. *arXiv* **2004**, arXiv:2004.04059.
14. Kuhn, C.; Beck, M.; Strufe, T. Covid Notions: Towards Formal Definitions–and Documented Understanding–of Privacy Goals and Claimed Protection in Proximity-Tracing Services. *arXiv* **2004**, arXiv:2004.07723.
15. Moazzami, B.; Razavi-Khorasani, N.; Dooghaie Moghadam, A.; Farokhi, E.; Rezaei, N. COVID-19 and telemedicine: Immediate action required for maintaining healthcare providers well-being. *J. Clin. Virol.* **2020**, *126*. [CrossRef] [PubMed]
16. Chambers, R.; Gabbett, T.J.; Cole, M.H.; Beard, A. The use of wearable microsensors to quantify sport-specific movements. *Sport. Med.* **2015**, *45*, 1065–1081. [CrossRef] [PubMed]
17. Kos, M.; Kramberger, I. A Wearable Device and System for Movement and Biometric Data Acquisition for Sports Applications. *IEEE Access* **2017**, *5*, 6411–6420. [CrossRef]
18. Bayo-Monton, J.L.; Martinez-Millana, A.; Han, W.; Fernandez-Llatas, C.; Sun, Y.; Traver, V. Wearable sensors integrated with Internet of Things for advancing eHealth care. *Sensors* **2018**, *18*, 1851. [CrossRef] [PubMed]
19. Falcionelli, N.; Sernani, P.; Brugués, A.; Mekuria, D.N.; Calvaresi, D.; Schumacher, M.; Dragoni, A.F.; Bromuri, S. Indexing the Event Calculus: Towards practical human-readable Personal Health Systems. *Artif. Intell. Med.* **2019**, *96*, 154–166. [CrossRef] [PubMed]
20. Bumgarner, J.M.; Lambert, C.T.; Hussein, A.A.; Cantillon, D.J.; Baranowski, B.; Wolski, K.; Lindsay, B.D.; Wazni, O.M.; Tarakji, K.G. Smartwatch Algorithm for Automated Detection of Atrial Fibrillation. *J. Am. Coll. Cardiol.* **2018**, *71*, 2381–2388. [CrossRef] [PubMed]

21. Pirouz, B.; Shaffiee Haghshenas, S.; Shaffiee Haghshenas, S.; Piro, P. Investigating a serious challenge in the sustainable development process: analysis of confirmed cases of COVID-19 (new type of coronavirus) through a binary classification using artificial intelligence and regression analysis. *Sustainability* **2020**, *12*, 2427. [CrossRef]
22. Shaffiee Haghshenas, S.; Pirouz, B.; Shaffiee Haghshenas, S.; Pirouz, B.; Piro, P.; Na, K.S.; Cho, S.E.; Geem, Z.W. Prioritizing and Analyzing the Role of Climate and Urban Parameters in the Confirmed Cases of COVID-19 Based on Artificial Intelligence Applications. *Int. J. Environ. Res. Public Health* **2020**, *17*, 3730. [CrossRef]
23. Radhakrishnan, M.; Misra, A.; Balan, R.K.; Lee, Y. Smartphones and BLE Services: Empirical Insights. In Proceedings of the 2015 IEEE 12th International Conference on Mobile Ad Hoc and Sensor Systems, Dallas, TX, USA, 19–22 October 2015; pp. 226–234. [CrossRef]
24. Androulaki, E.; Barger, A.; Bortnikov, V.; Cachin, C.; Christidis, K.; De Caro, A.; Enyeart, D.; Ferris, C.; Laventman, G.; Manevich, Y.; et al. Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains. In *Proceedings of the Thirteenth EuroSys Conference*; Association for Computing Machinery: New York, NY, USA, 2018. [CrossRef]
25. Brooke, J. SUS-A quick and dirty usability scale. *Usability Eval. Ind.* **1996**, *189*, 4–7.
26. Finstad, K. The Usability Metric for User Experience. *Interact. Comput.* **2010**, *22*, 323–327. [CrossRef]
27. Ferretti, L.; Wymant, C.; Kendall, M.; Zhao, L.; Nurtay, A.; Abeler-Dörner, L.; Parker, M.; Bonsall, D.; Fraser, C. Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing. *Science* **2020**, *368*, 6936. [CrossRef] [PubMed]
28. eHealth Network. Mobile Applications to Support Contact Tracing in the EU's Fight against COVID-19 Common EU Toolbox for Member States. Available online: https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf (accessed on 25 June 2020).