An IoT and Blockchain Based System for Monitoring and Tracking Real-Time Occupancy for COVID-19 Public Safety †

Tiago M. Fernández-Caramés [1,2]*⦿, **Iván Froiz-Míguez** [1,2]*⦿ and **Paula Fraga-Lamas** [1,2]*⦿

1   Department of Computer Engineering, Faculty of Computer Science, Universidade da Coruña, 15071 A Coruña, Spain
2   Centro de investigación CITIC, Universidade da Coruña, 15071 A Coruña, Spain
*   Correspondence: tiago.fernandez@udc.es (T.M.F.-C.); paula.fraga@udc.es (P.F.-L.); Tel.: +34-981167000 (ext. 6051)
†   Presented at the 7th International Electronic Conference on Sensors and Applications, 15–30 November 2020; Available online: https://ecsa-7.sciforum.net/.

Abstract: The COVID-19 pandemic has brought several limitations regarding physical distancing in order to reduce the interactions among large groups that could have prolonged close contact. For health reasons, such physical distancing requirements should be guaranteed in private and public spaces. In Spain, occupancy is restricted by law but in practice, certain spaces may become overcrowded, existing law infringements in places that rely on occupancy estimations that are not accurate enough. For instance, although it is known the number of passengers that enter a public transportation service, it is difficult to determine the actual occupancy of such a vehicle, since it is commonly unknown when and where passengers descend. Despite existing a number of counting systems, they are either prone to counting errors in overcrowded scenarios or require the active involvement of the people to be counted (e.g., going through a lathe or tapping a card when entering or exiting a monitored area) or of a person that manages the entering/exit process. This paper presents a novel IoT occupancy system that allows for estimating in real time the people occupancy level of public spaces like buildings, classrooms, businesses or moving transportation vehicles. The proposed system is based on autonomous wireless devices that, after powering them on, do not need active actions from the passengers/users and require a minimum amount of infrastructure. The system does not collect any personal information to ensure user privacy and includes a decentralized traceability subsystem based on blockchain, which guarantees the availability, security and immutability of the collected information. Such data will be shared among smart city stakeholders to ensure public safety and then deliver transparent decision-making based on data-driven analysis and planning.

Keywords: IoT; tracking; traceability; blockchain; smart cities; smart campus; COVID-19; contact tracing; occupancy

1. Introduction

The COVID-19 pandemic poses unprecedented health care and socio-economical challenges for all the societies around the world. Mitigation measures have proven to be critical for containing the spread of the virus [1]. Restrictive measures like lockdowns can contain the epidemic and alleviate pressure on health care systems but they provoke dramatic economic consequences. There are other preventive measures that allow for performing economic and social activities while minimizing impact on people's health and the burden of health care systems. Such measures include hygiene, the use of

facemasks, physical distancing, social distancing, bans on large gatherings, mobility restrictions or the isolation of infected populations, among others.

Regarding physical distancing, in order to reduce the interactions among large groups that could have prolonged close contact, specific physical distancing requirements should be guaranteed in private and public spaces. In Spain, occupancy is restricted by law, but, in practice, certain spaces may become overcrowded. Thus, there are law infringements at some places that rely on occupancy estimations that may not be accurate enough. For instance, in public transportation (e.g., buses), although it is known the number of passengers that enter a vehicle, it is difficult to determine its actual occupancy, since it is commonly unknown when and where passengers descend. Current counting systems like Automated Passenger Counters (APCs) [2], video analysis tools or smart cards are useful but prone to counting errors in overcrowded spaces or when active involvement of the users is required (e.g., by tapping a public transport card when exiting a monitored area).

Regarding wireless identification technologies for tracking people occupancy, Radio Frequency IDentification (RFID), QR and Near-Field Communications (NFC) are arguably the most commonly used, although other technologies like ultrasounds, Ultra-Wide Band (UWB) or bluetooth can be used. For instance, Bluetooth/Bluetooth Low Energy (BLE) is playing a relevant role as an enabler technology for mobile contact tracing applications. The latest advances in identification technologies have allowed for increasing indoor reading distance and for providing more complex services, but such augmented capabilities may also add more vulnerabilities and security and privacy issues [3].

Public safety and an effective and data-based decision-making in a pandemic requires timely and trusted data sharing not only about infections, but also about human behavior and mobility. Regarding data sharing, most smart city stakeholders (e.g., public authorities, healthcare services, transportation companies, insurance companies, mobility service providers, infrastructure operators, payment system providers, research institutions) can collect specific data on users in relation to their interactions through smart cards and wearables, like their trip frequency, the route they follow and when they enter or leave a specific area. Such data can be collected in real-time or deferred, and further analyzed using Artificial Intelligence (AI) techniques for decision-making and predictions.

In the case of occupation information, it must be privacy-preserving, accurate, transparent and as trustworthy as possible. In the last years Distributed Ledger Technologies (DLTs) like blockchain have emerged as a novel decentralized solution for collecting, validating and storing the collected data or a proof of them (e.g., their hashes) in a way that can be transferred securely between stakeholders that do not necessarily trust each other. The DLT field is still in its infancy, but during the past years numerous prototype developments have been proposed in different fields [4,5].

This paper presents a novel IoT system that makes use of the previous technologies. Specifically, it allows for estimating in real time people occupancy level in public spaces like buildings, classrooms, businesses or moving transportation vehicles. In contrast to smartphone-based contract tracing applications, which require an active involvement from the users (e.g., to start a mobile app or to enable Bluetooth communications), the proposed system is based on autonomous wireless devices that do not need active user actions after powering them on and require a minimum amount of infrastructure. The proposed system does not collect any personal information to ensure user privacy and includes a decentralized traceability subsystem based on blockchain, which guarantees the availability, security and immutability of the collected information in order to share it among smart city stakeholders.

2. Design and Implementation of the System

2.1. Communications Architecture

Figure 1 shows the communications architecture of the proposed system. The architecture shows at the bottom an IoT device (e.g., a wearable) that is carried by the users to be identified. Each wearable is composed by different subsystems that control its operation, power it and allows for communicating with monitoring and identification devices that are placed in a monitored space. Specifically, the Monitoring

Point enables tracking the user while he/she remains in the monitored space and can send the collected information to a remote server, which gathers all the relevant information of the system, stores it in a database and process it to visualize it through a user-friendly interface. In addition, the Monitoring Point is also able to store information on a blockchain, where data or their hashes are stored. Furthermore, the blockchain can make use of smart contracts, which allow for executing certain pieces of code autonomously. Regarding the Identification Point, it is placed at the entrance of the monitored space in order to gather identification data from the wearable whenever a user enters the monitored space.
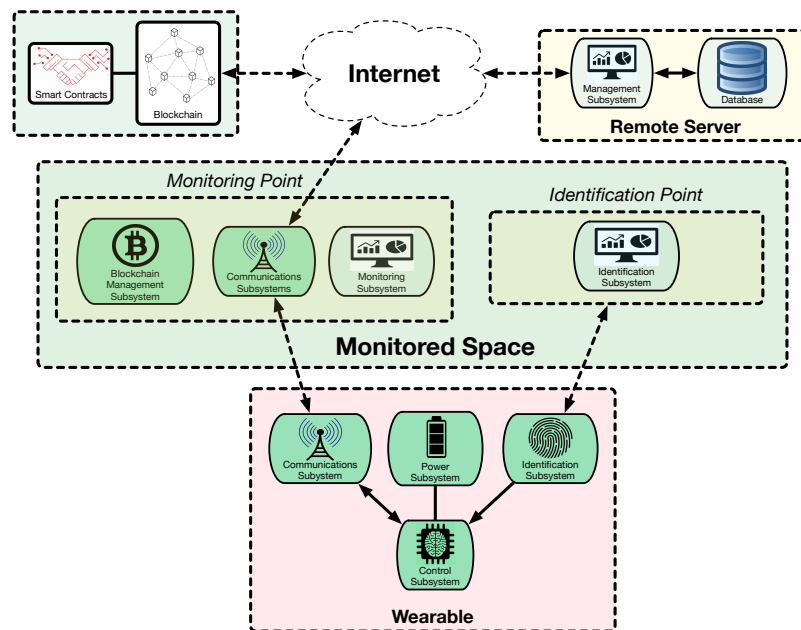

Figure 1. Communications architecture of the proposed system.

2.2. Implementation

In order to implement the proposed communications architecture, the following technologies were selected:

- Wearable. It is based on a ESP32 board, which uses a low-cost System-on-Chip (SoC) that embeds WiFi and Bluetooth transceivers. The wearable also includes an NFC module (PN532 from NXP) that is able to communicate with the Identification Point.
- Identification Point. It is an NFC reader placed at the entrance of the monitored space. Users tap their wearable into this NFC reader to power it up and to exchange the required initial identification information through NFC Data Exchange Format (NDEF) messages, which enable the Identification Point and the wearable to recognize each other in a secure way.
- Monitoring Point. It makes use of two ESP32 boards: one is used as Bluetooth scanner (i.e., it collects beacons from the deployed wearables), while the other one is dedicated to emit Bluetooth beacons. Therefore, beacons are used to track users and, at the same time, users track a Monitoring Point through its beacons. As a consequence, no connections are actually established between the Monitoring Point and the wearables. Moreover, beaconing increases user counting speed and avoids the use of complex authentication mechanisms. Furthermore, beaconing is a low-power communication technique, thus being ideal for extending wearable battery life. However, it must be noted that in some countries sniffing information like MAC addresses can be considered illegal, so future developers should check their country laws before deploying a system like the one proposed in this paper.

- Remote server. It is a cloud server that runs the backend software, which is based on a Message Queue Telemetry Transport (MQTT) broker and Node-RED. The backend software is also responsible for managing the interactions with the decentralized storage and the blockchain.
- Decentralized storage system and blockchain. The system allows for using InterPlanetary File System (IPFS) to store the collected information in a distributed way. Moreover, Ethereum's blockchain and smart contracts can be integrated to preserve traceability on the occupancy level and on the users that remain in a monitored space during certain time intervals.

Figure 2 represents through a sequence diagram the most relevant interactions among the previously described components. As it can be observed in Figure 2, the system works as follows:

- Initially, the wearable, after being switched on, goes into an ultra-low power mode (deep sleep mode) in order to increase battery life.
- When the user taps the wearable into the NFC reader (when he/she enters the monitored space), the internal circuitry of the wearable rectifies the current from the electromagnetic field created by the NFC reader and wakes up the rest of the components of the wearable.
- Then, the wearable and the NFC reader exchange their identification data. To preserve user privacy, the wearable sends a random Bluetooth MAC address to the NFC reader, which will be used only while the user remains on the monitored space. Additional information can be exchanged to improve the security of the system, like the 128-bit rolling proximity identifiers defined by Google's and Apple's contact tracing Bluetooth specification [6].
- If the identification information is exchanged successfully, the wearable emits a confirmation beep. With such an information, the wearable and the Monitoring Point (i.e., its Bluetooth Monitor) of the monitored space can track each other through the beacons that they emit periodically.
- The Bluetooth Monitor collects through its Bluetooth scanning interface the beacons from the wearables of the monitored space whose Received Signal Strength Indicator (RSSI) is under a prefixed threshold (i.e., whose signal strength can be considered to be close enough to the Bluetooth Monitor). In the system tested in this paper, the threshold was calibrated manually, but more advanced techniques can be used to improve the detection algorithm accuracy [7].
- The beacon information collected from the wearables and their RSSIs are sent to the backend server through MQTT to determine the occupancy level of the monitored space. Moreover, the backend can store traceability information on the decentralized storage and/or on the blockchain.
- If the wearable does not capture beacons from a Bluetooth Monitor during a specific amount of time (e.g., two minutes during the tests performed for this paper), it goes into deep sleep mode to reduce power consumption, since it assumes that the user exited the monitored space.
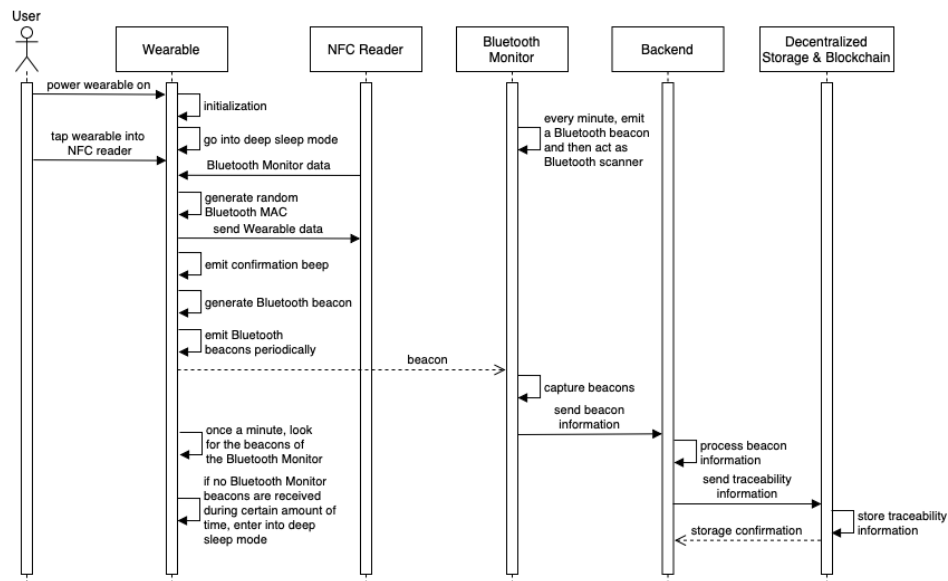
Figure 2. Sequence diagram of the most relevant interactions of the main system components.

3. Experiments

Several tests were carried out to determine the response time and the accuracy of the proposed system when estimating the occupancy level of two facilities: an 82 m^2 research lab and a 22 m^2 meeting room. In both scenarios, a monitoring device and 10 wearables were used. For the sake of simplicity, seven wearables remained static inside the monitored rooms, while the other three were carried by users when entering and exiting the monitored space.

During the tests, the real occupancy level and the enter and exit timestamps were written down and then compared with the values estimated by the system. The RSSI thresholds were selected empirically for each room to minimize false positives and negatives when estimating occupancy levels. Specifically, an RSSI threshold of -90 dBm was selected for the meeting room, while the Monitoring Point of the research lab used a -91 dBm threshold.

As an example, Figure 3 shows the evolution of the real and estimated occupancy levels through time for the two monitored rooms. The blue line indicates the real occupancy of the rooms, the orange line represents the occupancy level estimated by the system and the green line quantifies the number of errors during the occupancy estimation (i.e., the number of wearables that were not positioned correctly). In addition, the vertical red lines indicate the time instants when people either entered or exited the rooms. As it can be observed in Figure 3, under the described circumstances, the system estimates correctly the occupancy level most of the time. Nonetheless, when wearables enter/exit a room, there is some lag when updating the occupancy level. Such a lag is quantified in Tables 1 and 2, which show that, for all cases, the occupancy level update time is less than a minute, which is fast enough for most monitored spaces.
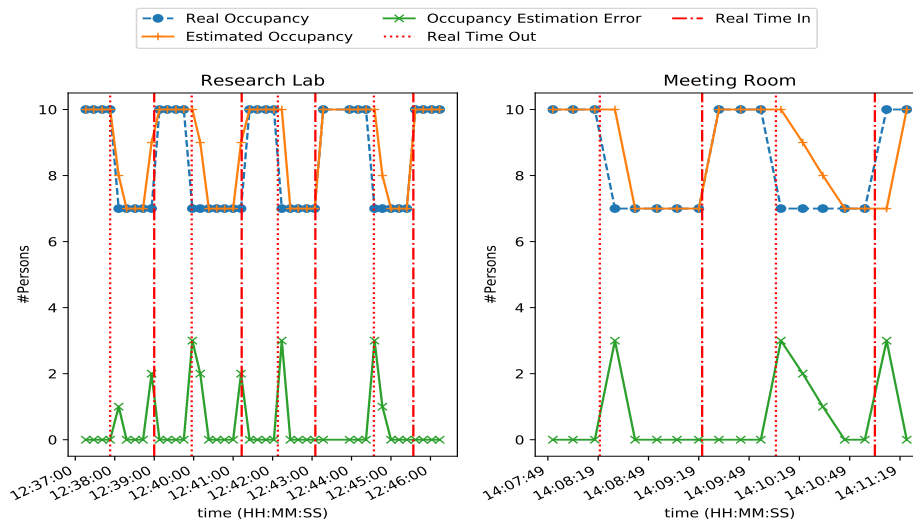
Figure 3. Occupancy level estimation over time.

Table 1. Detection delay for the research lab.

Action	Real Occupancy Level Change Time (hh:mm:ss)	Estimated Occupancy Level Change Time (hh:mm:ss)	Detection Delay (s)
Exit 1	12:37:53	12:38:18	35
Entrance 1	12:39:00	12:39:08	8
Exit 2	12:39:57	12:40:23	34
Entrance 2	12:41:13	12:41:25	12
Exit 3	12:42:08	12:42:27	19
Entrance 3	12:43:05	12:43:17	12
Exit 4	12:44:34	12:45:00	26
Entrance 4	12:45:34	12:45:37	3

Table 2. Detection delay for the meeting Room.

Action	Real Occupancy Level Change Time (hh:mm:ss)	Estimated Occupancy Level Change Time (hh:mm:ss)	Detection Delay (s)
Exit 1	14:08:20	14:08:41	21
Entrance 1	14:09:21	14:09:31	10
Exit 2	14:10:05	14:10:46	41
Entrance 2	14:11:04	14:11:23	19

4. Conclusions

This paper presented a novel IoT system aimed at estimating occupancy levels in public spaces during the current COVID-19 pandemic. The proposed system is based on the use of IoT devices that interact with identification and monitoring devices deployed in the monitored areas. The collected information can be either stored in remote servers or in a decentralized storage system like a blockchain. The initial experiments performed with the system show good accuracy when estimating occupancy level and a less-than-a-minute update lag. Future work will be focused on improving current threshold-based occupancy detection algorithm.

References

1.　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.

2.　Cheng, S.; Liu, B.; Zhai, B. Bus arrival time prediction model based on APC data. In Proceedings of the 6th Advanced Forum on Transportation of China, Beijing, China, October 2010.

3.　Fernández-Caramés, T.M.; Fraga-Lamas, P.; Suárez-Albela, M.; Castedo, L. A Methodology for Evaluating Security in Commercial RFID Systems, Radio Frequency Identification. In *Radio Frequency Identification*, 1st ed.; Crepaldi, P.C., Pimenta, T.C., Eds.; INTECH: Rijeka, Croatia, 2016.

4.　Fernández-Caramés, T.M.; Blanco-Novoa, O.; Froiz-Míguez, I.; Fraga-Lamas, P. Towards an Autonomous Industry 4.0 Warehouse: A UAV and Blockchain-Based System for Inventory and Traceability Applications in Big Data-Driven Supply Chain Management. *Sensors* **2019**, *19*, 2394.

5.　Fernández-Caramés, T.M.; Froiz-Míguez, I.; Blanco-Novoa, O.; Fraga-Lamas, P. Enabling the Internet of Mobile Crowdsourcing Health Things: A Mobile Fog Computing, Blockchain and IoT Based Continuous Glucose Monitoring System for Diabetes Mellitus Research and Care. *Sensors* **2019**, *19*, 3319.

6.　Google & Apple. Contact Tracing Bluetooth Specification Preliminary—Subject to Modification and Extension. April 2020 v1.1. Available online: https://bit.ly/2Tp8Mtp (accessed on 23 October 2020).

7.　Fraga-Lamas, P.; Fernández-Caramés, T.M.; Noceda-Davila, D.; Vilar-Montesinos, M. RSS Stabilization Techniques for a Real-Time Passive UHF RFID Pipe Monitoring System for Smart Shipyards. In Proceedings of the 2017 IEEE International Conference on RFID (RFID), Phoenix, AZ, USA, 9–11 May 2017; pp. 161–166.