Array 9 (2021) 100051

Contents lists available at ScienceDirect

Array

journal homepage: www.elsevier.com/journals/array/2590-0056/open-access-journal

COVID-19 & privacy: Enhancing of indoor localization architectures towards effective social distancing

Paolo Barsocchi [a], Antonello Calabrò [a], Antonino Crivello [a], Said Daoudagh [a,b], Francesco Furfari [a], Michele Girolami [a,*], Eda Marchetti [a]

[a] ISTI-CNR, Institute of Information Science and Technologies, Pisa, Italy
[b] University of Pisa, Pisa, Italy

ARTICLE INFO

Keywords:
Social distancing
COVID-19
Indoor localization system
Privacy

ABSTRACT

The way people access services in indoor environments has dramatically changed in the last year. The countermeasures to the COVID-19 pandemic imposed a disruptive requirement, namely preserving social distance among people in indoor environments. We explore in this work the possibility of adopting the indoor localization technologies to measure the distance among users in indoor environments. We discuss how information about people's contacts collected can be exploited during three stages: before, during, and after people access a service. We present a reference architecture for an Indoor Localization System (ILS), and we illustrate three representative use-cases. We derive some architectural requirements, and we discuss some issues that concretely cope with the real installation of an ILS in real-world settings. In particular, we explore the privacy and trust reputation of an ILS, the discovery phase, and the deployment of the ILS in real-world settings. We finally present an evaluation framework for assessing the performance of the architecture proposed.

1. Introduction

The recent COVID-19 pandemic has been imposing profound changes in our daily life. Most of the affected countries adopted different countermeasures in order to reduce the contagious rate. Among them, an effective action is the so-called social distancing. The idea is simple as disruptive at the same time: citizens are invited to maintain at a certain physical distance from others. This recommendation applies when we interact with people out of our personal spaces, namely a restricted community of contacts.

Social distancing has become a new requirement in the way we access and provide services. In the context of the COVID-19 pandemic, policy-makers have to re-think the way we visit a supermarket, we catch a bus, or we interact with colleagues at work. We consider two possible ways of guaranteeing such a requirement: manually or automatically. The manual approach is commonly adopted in our cities, such as in a shopping mall. In this case, an operator observes the scene acting to limit and prevent close contacts among people; for example by managing the waiting queue, verbally distancing customers, or by optimizing the displacements of goods so that to reduce involuntary contacts. Although such approach is relatively easy to implement, we argue that a complementary solution needs to be adopted on the long period; we refer to it as automatic social distancing. In this work, we explore the possibility of automatically guarantying the social distance indoor with the adoption of a privacy-preserving Indoor Localization System (ILS). We focus on those services that are generally available indoor, such as a museum, airport facilities, or a supermarket. In these representative use cases, users roam through a sequence of points of interest such as galleries of a museum, check-in desks, or aisles of a supermarket. Our approach consists of estimating the current location of people with the ILS and to compute the personal distance among the subjects involved. Knowledge on the existence of crowds can be exploited by suggesting to the customers an alternative path able to minimize gatherings with others. In the last decade, ILSs have been widely adopted [1] in different scenarios; they are based on very different technologies, ranging from Wi-Fi fingerprinting [2] to solutions based on ultra-wide band radio waves [3]. We argue that the accuracy obtained from the most advanced systems is now sufficient for the purpose of the social distancing [4]. As a meaningful example, we refer to class of ultra-wide band systems able to constrain the localization error in the range of centimetres while tracking moving

* Corresponding author.
E-mail addresses: paolo.barsocchi@isti.cnr.it (P. Barsocchi), antonello.calabro@isti.cnr.it (A. Calabrò), antonino.crivello@isti.cnr.it (A. Crivello), said.daoudagh@isti.cnr.it (S. Daoudagh), francesco.furfari@isti.cnr.it (F. Furfari), michele.girolami@isti.cnr.it (M. Girolami), eda.marchetti@isti.cnr.it (E. Marchetti).

https://doi.org/10.1016/j.array.2020.100051
Received 24 July 2020; Received in revised form 9 November 2020; Accepted 15 December 2020
Available online 23 January 2021

objects [5]. We first propose a privacy-preserving ILS architecture able to guarantee real-time user's location and privacy of the data collected. The solution we propose in this work considers the General Data Protection Regulation (GDPR) as the grounding framework for preserving privacy through a compliant Access Control (AC) system [6–8]. The AC system ensures that only the intended users can access the protected (personal) data and get the permission levels required to accomplish their tasks. However, notwithstanding the important role of AC systems, their integration inside the localization system architecture is still an emerging challenge specifically considering the enforcement of the GDPR's requirements. Our solution relies on a privacy-by-design indoor positioning architecture, where purposes of data management are explicitly defined, consents collected and the rights related to privacy and data protection correctly enforced. We then discuss three use cases in which the architecture proposed can be adopted, namely visits to a museum, airport access, and shopping in a supermarket. For each of the use-cases, we present the requirements for guaranteeing social distancing indoor. We also introduce some barriers currently preventing a massive adoption of ILS-based tracing systems and we conclude our paper with an evaluation framework aimed at assessing the performance.

The innovation we propose with our work mainly consists of four aspects:

- we frame a reference architecture for social distancing based on an Indoor Localization System generalizing three common use-cases;
- we introduce a privacy-preserving access control system grounded on the European GDPR framework;
- we summarize three typical use cases in which the proposed architecture can be adopted, by highlighting the intrinsic challenges of the social distancing;
- finally, we discuss 4 main barriers to overcome for an effective adoption of such technologies in real-world settings.

As recently reported by M. Zissman (MIT Lincoln Laboratory) in a recent article from J. Hsu [9], "[…] In a perfect world, something like this would have taken a couple years to implement. There just isn't the time […]". We agree with such vision, and we consider that a great effort has to be spend for the integration of different technologies enabling the proximity detection of people both indoor and outdoor. Such effort will determine the success in fighting against the next pandemic.

The paper is organized as follows. Section 2 covers the background and related work in the field of Indoor Localization Technologies and GDPR-based Access Control. Section 3 describes our reference architecture for an ILS. Section 4 reports three reference use cases, namely visiting a museum, airport terminal access and shopping assistance. Section 5, we discuss some issues that we consider challenging for a real-world installation of an ILS and, finally, Section 6 describes our evaluation framework.

2. Background and related work

In the following, we focus on three main aspects that equally contributes to the proposed architecture: the related indoor localization technologies their specific characteristics 2.1; the Indoor Localization Apps 2.2 and the Access Control Systems 2.3. We discuss in particular the mobile application proposal able to deal with social distancing, exploring their main strengths and weaknesses in terms of authorization to access to the mobile resources requested to the user and their impact on user's privacy.

2.1. Indoor localization technologies

Several localization technologies have emerged in the last years to address the demanding of location-based services. We review two categories: Radio Frequency-Based (RF) and non-RF based. Among the RF technologies there exist systems based on the analysis of Wi-Fi [10], Bluetooth Low Energy (BLE) [11,12], LTE [13], and Ultra-Wide Band (UWB) [14,15] signals. Wi-Fi-based solutions have the advantage of exploiting the ubiquity of Wi-Fi Access Points. The most performing Wi-Fi solutions obtain high performance in terms of localization accuracy with reduced cost of maintenance and installation [16].

In the last few years, the Bluetooth Low Energy (BLE) standard has been adopted a cheap a viable technology for indoor navigation and localization. BLE tags are cheap and easy to deploy, moreover their battery life time spans from few months to years.[1] Indoor localization systems based on BLE often implements a range-based technique, according to which the moving target is localized in proximity of the BLE tags with the highest Received Signal Strength of the beacons emitted ([17] explores this technique for the purpose of tracing social interaction). However, more advanced solutions based on the beacon's angle or arrival and time of flight are also available with a very high accuracy level, as done with Quuppa[2] and the recent Bluetooth 5.1 stack.

Finally, the UWB network interface represents a recent and promising solution. Its accuracy can reach the centimeter-level with specific deployments. Its adoption has been increasing as Apple decided to provision the iPhone 11 with the U1 chip-set. As a result, we expect that in the near future other vendors will include such technology with Android-based smartphones. Some remarkable examples of UWB-based indoor solution are the Pozyx [18] and some recent works [19–21]. Non-RF based technologies for indoor localization rely on visual/camera [22], Visible Light Communication (VLC) [23], Inertial Measurement Unit (IMU) [24], and Magnetic Field Sensor (MEMS) [25]. The visual based systems exploits images captured by surveillance camera already deployed. The performance range in the centimetre scale but, in wide and public environments, the privacy regulations might limit their adoption on the large scale. Differently, if the user/target is equipped with a camera sensor, a visual-based system can reach accuracy performance around a meter of error. Furthermore, the end-user is required to keep the camera in a fixed position with the side-effect of influencing the its natural way of moving.

The Visible Light Communication is an emerging optical technology for high-speed data transfer which uses visible light modulated and emitted by Light Emitting Diodes (LEDs). Indoor positioning systems based on VLC use light sensors (e.g. camera sensor) to measure the position and direction of the LED emitters but they generally require line of sight between emitters and receivers [23].

Systems based on Micro Electro-Mechanical Systems (MEMS) exploit the distortion of the Earth's magnetic field mainly due to structural steel elements (e.g. steel fire doors) and furniture. As an example, these distortions can be a discriminating factor in environments comprised by corridors, rooms and small areas. The performances of these systems generally drops in wide and open space because the distortion are considered less meaningful [26].

IMU based systems utilize tri-axial accelerometers and gyroscopes for sensing the motion. The combination of gyroscope and accelerometer is used to evaluate the heading direction [27]. Unfortunately, accelerometers are error prone due to random movements of human motion and, the gyroscope is susceptible of magnetic fields distortion. As a consequence, IMU-based systems generally reach low accuracy and requires a complex calibration process to detect, for example, user' step length and the motion speed [28]. We finally report on Table 1 a comparison of RF and non-RF based techniques, with a summary of their weaknesses and strengths.

We finally survey some architectures for indoor positioning. Such architectures provide features for a quick integration, such as an SDK or APIs for third-party developers. Authors of [29] introduced a middleware architecture for fusing multiple sources of information, showing how a

[1] BLE Tags can be configured in safe-mode with low power of emission and low advertisement rate.

[2] https://quuppa.com/.

Table 1
A comparison between indoor localization technologies.

Technology	Strengths	Weaknesses	Accuracy	Scalability
Camera	High accuracy, low maintenance	Requires dedicated hardware, difficult user identification	0.5–1 m	Medium
VLC	Potentially high accuracy, easy to install	Requires line of sight, requires additional hardware	0.5–1 m	High
IMU	No infrastructure required	Requires high customization, error prone to drift problems	1–5 m	N.A.
MEMS	Ubiquity of the signal, no infrastructure required	Error prone to interference, costly calibration process	2–5 m	N.A.
Wi-Fi	Easy to implement, cost efficient	Medium accuracy, generally require modifications to the APs	2–4 m	High
BLE	Low energy consumption, low cost	Error prone to noise, medium accuracy in wide environ- ment	2–4 m	High
UWB	High accuracy in small environment	Requires dedicated hardware, high costs	0.5–1 m	Low

data fusion approach leads to improved performances in the same indoor environment. In [30], authors describe an extensible framework for exploring location data's multifaceted representations and exposing a query layer. Lastly, Anyplace [31] shows a similar idea to the other architectures above mentioned by releasing an open-source architecture in order to easily deploy indoor localization functionalities in new environments.

2.2. Indoor Localization Apps

The most diffused technical solutions for guaranteeing social distance are based on mobile applications. Apps enable an easy-to-use user interface and, at the same time, a massive diffusion through the well-known app stores. Currently, there exist several applications whose features span from tracing contacts, e.g., Immuni [32] (the application build by Italian Health Minister), to the possibility of managing a waiting queue, e.g., ufirst [33].

Depending on their features, the apps require access to several entities and purposes. From a privacy-preserving point of view, unfortunately, not all the apps expose neither a clear claim about the usage of the collected personal information nor a clear description concerning the usage of such data. Consequently, we argue that the end-user might remain sceptic in daily using such apps. In order to provide a first outlook about the existing apps for social distancing or for detecting in social interactions [17], we report in Table 2 a selection of apps available on the Android Play Store and tested on a commercial smartphones. The table reports the analysis of some features and the authorizations required. In particular, the group of columns labelled Location, Others, Disk, Camera, report the name of the permissions' classification provided by the Android Play Store for grouping the different features. Finally, for each group, we report some details concerning the permissions of each app based on the description provided by the developers. In particular, we report the following information:

1. Approx location: if the app can localize the device within a wide area;
2. Precise location GPS & net: if the app can accurately localize the device;
3. Receive data from Internet: if the app can receive data form Internet;
4. View network conn.: if the app can check the networks to which the device has access;
5. Full network access: if the app can access to any of the networks the device is connected with;
6. Run at startup: if the app can automatic restart;
7. Prevent device sleeping: if the app can prevent the device from switching in sleeping mode;
8. Pair BT devices: if the app can pair with a Bluetooth device;
9. Access BT settings: if the app can initiate the device discovery or modify the Bluetooth settings;
10. Control vibration: if the app can control the device vibration;
11. CRUD contents: if the app can perform CRUD operations;
12. Take pictures or videos: if the app can take photos of record videos.

Taking a glimpse as a generic user to the installation and usage of the apps analysed in the Table 2, the consent forms are very generic and sometimes do not intuitively declare the purposes of data collection, the duration of the data retention or the possibility of future exploitation of the data collected.

For example, one application (the 2M Social distance checker) requests permission to access to the Call Log and Address Book without specifying how the data will be used, i.e., to enable the sharing of user experience with his/her contacts. From a technical point of view, in case of open-source applications [34] specific information about the real usage of sensors data or the procedures for managing them can be retrieved by accurate analysis of the source code. However, this operation is not feasible by common users without a computer science background and it is not allowed for proprietary application [35,36].

Additionally, rarely there is a clear claim on where and how the collected data will physically be stored or distributed. Indeed, depending on the country where the DB is, the rules for accessing its information could be compliant to a privacy standard different from that required by the application country. The situation could be even worse in case when the application is used by users belonging to different countries having not the same privacy rules. Consequently, there could be the risk of a personal data management not completely compliant with the consensus signed by the app users. For instance in Italian Immuni [32] (The application built by Italian Health Minister) developers clearly claims that the DB will be physically positioned in Italy and managed by the Italian Health Minister under the GDPR compliance.

Social distance can also be implemented with ad-hoc hardware components like people counter and smart bracelets [37,38]. These solutions have the benefit of guaranteeing reliability, since they do not dependent on the user's device. The features offered are limited to tracing the contacts with others or alerting when a user gets too close to another. More advanced features can also be implemented with data analysis techniques but, at the current stage, we were not able to find remarkable examples in the current literature.

2.3. GDPR and Access Control Systems

We now review some techniques adopted with Indoor Localization Systems that are commonly adopted to manage the privacy of the data collected. We first review the GDPR reference framework and then we survey some recent works. The GDPR [39] defines Personal Data as any information relating to an identified or identifiable natural person called Data Subject. As a result, a data subject is a Natural Person (a living human being), whose data are managed by a Controller. The GDPR is applied to the processing of personal data, whether it is automated (even partially) or not. The GDPR defines, among others, the following principles and demands: Purposes, i.e., data should only be collected for determined, explicit and legitimate purposes, and should not be processed later for other purposes; Accuracy, i.e., the processed data must be accurate and up-to-date regularly; Retention, i.e., data must be deleted after a limited period; Subject explicit consent, i.e., data may be collected

Table 2
Features of social distancing mobile apps.

App name	LOCATION		OTHERS								DISK	CAMERA
	Approx location	Precise location GPS & net	Receive data from Internet	View network conn	Full network access	Run at startup	Prevent device sleeping	Pair BT devices	Access BT settings	Control vibration	CRUD contents	Take pictures videos
Social Distancing Project (Su-Raksha)	✓							✓	✓	✓		
The Social Distancing App	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Social Distance	✓	✓	✓	✓	✓	✓	✓	✓	✓			
REXdistance					✓					✓	✓	✓
Social Distancing												
Social Distance Alarm		✓	✓	✓	✓	✓	✓	✓	✓			
Social Distancing					✓						✓	✓
1point5	✓	✓			✓		✓	✓	✓	✓		
Give Me Space		✓					✓	✓	✓	✓		
The Best Social […]												
Social distance		✓			✓		✓	✓	✓	✓		
Social Distancer				✓	✓		✓					✓
Distancing App	✓		✓	✓	✓	✓	✓	✓	✓	✓		
Social Distance							✓	✓	✓			
Social Distancing App	✓	✓						✓	✓	✓		
Pistis.io Social Distancing App	✓	✓		✓	✓		✓	✓	✓	✓		
Distancing alarm	✓	✓			✓							
2 M Social distance checker	✓	✓										
Social Distancing App - Wearable	✓	✓					✓	✓	✓	✓		
Keep Distance	✓	✓	✓	✓	✓	✓	✓	✓	✓			
Immuni				✓	✓	✓	✓	✓				

and processed only if the data subject has given his explicit consent.

Concerning the design of the Access Control (AC), it is usually implemented through an Access Control Mechanism (ACM), which is the system providing a decision to an authorization request, typically based on predefined Access Control Policy (ACP). The XACML [40] is one of the most widely used AC languages, and it provides the reference

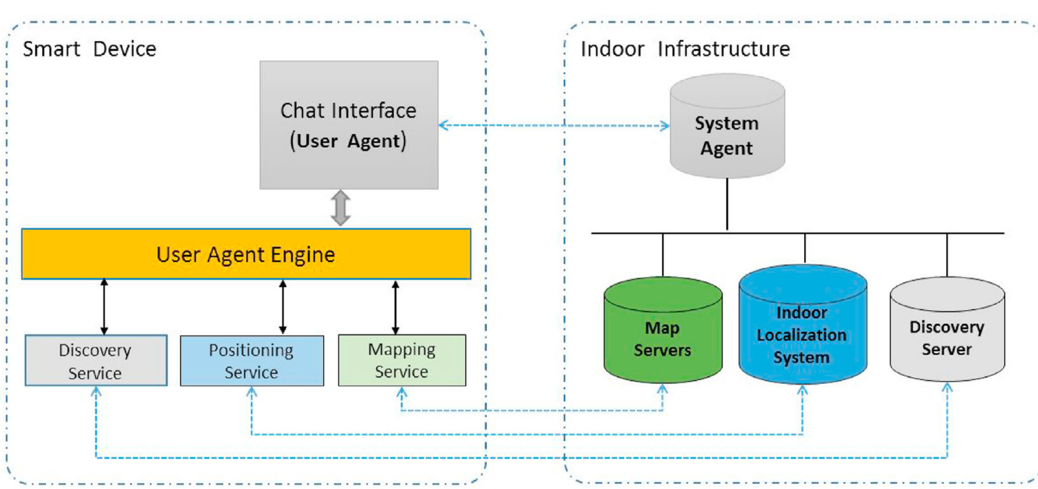

Fig. 1. Functional components of the integrated architecture.

architecture in the AC environment.

We refer to [41] for a systematic review of privacy in indoor positioning systems. As emerged by this survey, recent proposals show how location and topology-aware are becoming feature for the security [42]. However, most of the research has been focused either on:

- using technology Wi-Fi and the fingerprinting methods combined with cryptography solutions [43–45];
- using access control mechanisms for (physical) protection within virtual perimeters [46];
- using location information to automatically authenticate customer [47];
- specific security attributes that do not fully cover the GDPR's requirements [48–50].

3. Overview of the integrated architecture

In the following, we detail the reference architecture based on an Indoor Localization System (ILS) for guaranteeing social distancing. The architecture relies on two layers: the smart device and the localization infrastructure. As detailed in Fig. 1 these layers include components such as: a User Agent for managing the interactions on behalf of the end-user, the Indoor localization system including GDPR-based Access Control subsystem and the Map server. The reference architecture extends the solution presented in [4], and it integrates the GDPR-based access control described in [51,52].

3.1. Aim and scope

The approach we followed with this work is to firstly framing a reference architecture to be adopted in very different scenarios. To this purpose, our effort has been mainly focused on generalizing a common architectural design of a remote ILS, based on 3 main building blocks: a map server, the ILS engine, and a discovery agent to broadcast its existence. We then focus on the client side in the form of a smart device, as the primary interface to interact with the end-users. The architecture we propose has been deliberately designed without constraining to any of the common scenarios we daily experience. Differently, we tried to provide the community with a modular architecture to be customized. Furthermore, the current literature concerning the ILS does not identify a standard de-facto for indoor localization, rather multiple and heterogeneous solutions are available. To the best of our knowledge, this work introduces a privacy-by-design solution, mainly inspired by the European GDPR framework, as one of the most advanced regulations about privacy in force since the last decade.

3.2. Architecture requirements

Indoor localization systems are based on very different technologies. A standardization process of these systems is therefore the first objective that should be pursued in order to increase the spread and the usability of location-based services. We argue that standardized programming interfaces for the design of an ILS have a twofold benefit:

- to provide inter-operable location-based services to the end-users:
- to integrate in a seamless way outdoor and indoor localization systems.

Concerning the first benefit, its adoption can be used not only to locate and track people, but also to measure their physical distance. Its adoption can be considered an effective counter-measure to track, prevent and analyse how close people are in indoor environments. We refer to Section 4 for a in-depth description of three use-cases in which we describe the adoption of an ILS in real-world scenarios. Moreover, the standardization will increase the possibility for a user-agent to discover and to bind to any of the ILS available indoor. Such aspect is crucial for an open market, since it breaks the silos of custom and vertical solutions available so far.

Concerning the second benefit, we consider that the current user experience for outdoor localization systems (e.g. GPS) must be preserved also indoor. Under this context, the standardization could improve the design of systems enabling the hand-off between outdoor and indoor areas. We imagine a smooth transition from an outdoor map (e.g. provided by OpenStreepMap or Google Maps) to detailed indoor maps provided by an ILS.

As first step towards such standardization process is the definition of architectural requirements to be considered. In the following, we report a list of 4 requirements that we consider mandatory:

1. To discover the available Indoor Localization System dynamically (**R1**)

A discovery process should be defined to enable a person to look up for services available in a specific environment [53]. The process can be triggered through the Web or based on short-range network infrastructures. We refer to the first approach as global search, since the user queries the Web looking for an ILS available e.g. in a supermarket. In this case, the user fetches the meta-information of an ILS via the HTTP or similar protocols. Differently, the second approach is referred to as local search since the user looks up for nearby ILSs, by exploiting network interfaces such as Wi-Fi Direct, Bluetooth or LTE- Direct and the upcoming 5G. Such interfaces allow to look up for surrounding services in the range of few meters.

2. Indoor localization systems must self-describe their features to ensure interoperability with heterogeneous systems (**R2**).

We expect the definition of a common language for describing the features provided by an ILS. More specifically, ILS has to advertise some core information, such as: the localization technology adopted, the privacy requirements, the location of the indoor map and any other resource required for a device to discover, connect and access to the ILS. The benefit of such language is the possibility of replicating the user-experience for outdoor navigation (e.g. through Google Maps or similar) also indoor.

3. Privacy must be guaranteed and the service policies must be well defined and verifiable(**R3**).

One of the most critical aspects for the location-based services is the possible loss of control of the personal data collected. As a meaningful example, we recall the contact tracing apps also exploiting the device localization and designed for the purpose of mitigating the COVID-19 pandemic. In these cases, end-users are worried about non-expect usage of the data collected for commercial purposes. Some example of data that we consider critical are: the timestamp of the contacts, the IDs of the contacts, any information about the device used and, in some cases, the GPS location of the users.

Localization systems suffer intrinsically from this problem, therefore independently from the contingency period, explicit mechanisms for accepting policies, together with the ability to verify and manage the data collected, must be designed and implemented in accordance with the various national laws.

4. Indoor localization systems must be easy to use, intuitive and interactive (**R4**).

The interaction between the ILS and the end-user needs to specifically tackled. We argue that their success also depends on the way a user interacts with it. Most of the people already interacts fluently with GPS navigation systems (e.g. Google Maps, Garmin or TomTom charts). In particular, users search, discover and navigate toward a specific location that can always be represented as a pair of coordinates in the space (e.g. lat, long as WGS84 coordinates). The same user-experience should be replicated also for indoor environment, even if a higher number of challenges are present. To this purpose, we consider mandatory to design intuitive work-flows. As for example, the end-user should be able not only to search for a location, but also to navigate toward person, to pick up a list of products in a specific order or to meet a moving target indoor. A further level of interaction is also represented by the possibility of asking to an ILS context information describing the environment, such as the existence of a crowd or the waiting time before accessing a service. Such level of interactivity can be obtained by designing multi-modal interfaces, such as the Instant Messaging (IM) paradigm. Indeed, the IM paradigm implements the best metaphor for managing the exchange of information between the end-users and a system in a intuitive way. The user can chat with the ILS in order to get the position of its target, to receive suggestions, to be notified proactively and or to be guided step-by-step toward its final destination.

3.3. Architectural components

The requirements R1 to R4 are grounding for our architectural design. We describe in this section, several functional components to be deployed in two distinct layers: those present on the user device and those made available by the indoor infrastructure. This distinction easily recalls the two methods through which the position of a user is estimated: self-positioning processed by the smartphone and remote positioning processed at the local infrastructure. We also consider the possibility of having hybrid solutions. We report in Fig. 1 an overview of the components described. For the sake of brevity, we do not consider here the possibility of other solutions that could make use of the Cloud. For example, internal maps could be downloaded from any server on the Cloud (e.g. Google Maps), as well as a route to a target calculated by a navigation service available on the cloud. We mainly focus on abstract functionalities common to all the architectures and how they are to be described. Therefore, many concrete architectures can be derived by combining the abstract components we report in Section 4.4. We report in Fig. 2 an overview of the main components.

In the first group of components, the most important is the **User-Agent**. It can be described as an intelligent software component that operates on behalf of the end-user. The main functions it provides are: global and local discovery (**R1**), to manage the privacy for the end-users (**R3**), to interact with the local infrastructure to estimate position of the end-user (**R2**), to interact with the end-user (**R4**). Other functional components that could be installed on the device are the **Navigator** and a **Translator**, the first of course to manage navigation, determination of the shortest routes etc, the second is increasingly adopted to facilitate vocal interaction, as done with commercial vocal assistants (Amazon Alexa, Apple Siri, Google Home) (**R4**).

The second group of components concern the infrastructure. In particular, the **Indoor Location System** and the **Map Server** (**R2**, **R3**). The first consists of hardware and software artifacts deployed in the environment that are functional to the estimation of the user's position and the data protection, as detailed in Section 3.4. The second one provides the indoor maps and features of the indoor environment useful for navigating. Other components we foresee are the **Discovery Server** which provides the description of the resources available by the infrastructure (**R1**, **R2**) and the **System Agent** which is the counter-part with which the User Agent can communicate. In particular, the System Agent can be seen as a regular chat user to which send requests for assistance or information (**R4**), it can be implemented by an Instant Messaging bot. Components deployed in the infrastructure are interfaced by respective services orchestrated by the User-Agent. A person trough the User-Agent interface can interact with the System-Agent of the indoor infrastructure.

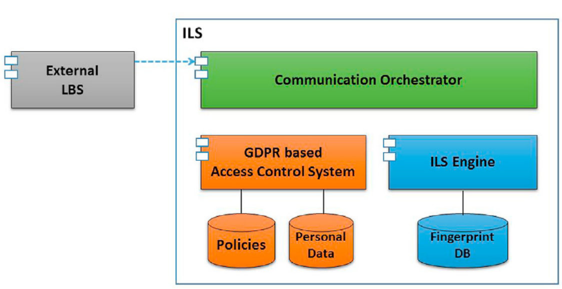

Fig. 2. ILS and Data protection components.

3.4. Indoor localization system and data protection

We now detail the internal structure of a generic ILS. We consider it provides three main sub-components, as detailed in Fig. 2: the **ILS Engine**, the **GDPR-Based Access Control System** (G-ACS) and the **Communication and Interaction Orchestrator**. Such components implement the main features of an ILS. Moreover, we expect that they rely two distinct database for collecting the information.

The ILS Engine implements the core functionality of the localization algorithm: it returns back to the User Agent the timestamped coordinates according to the map reference system (e.g. latitude and longitude as WGS84 reference system) [10,54].

Data provided by an ILS can be simultaneously accessed by multiple actors. More specifically, the end-user, the system administrator or a generic supervisor might require access to specific data. In order to manage the different grants for the actor, we consider that the ILS and the GDRP Access Control System (G-ACS) components have to cooperate (see Fig. 2). In particular, the latter is in charge of evaluating each single data access request and to allow or deny the access according to several factors. They are: the consents collected, the data validity period, the specific users/service rights and the access control policies established inside the overall Localization Infrastructure.

Finally the Communication and Interaction Orchestrator is the component in charge of man-aging the communication to and from the ILS. This component is exploiting publish-subscribe design pattern through extensible events. It is in charge to instantiate communication channels and manage flows of notifications and events data. Those events can be structured adopting several asynchronous messaging technologies like Java Messaging Service (JMS), Advanced Message Queueing Protocol (AMQP), Message Queueing Telemetry Transport (MQTT) in order to decoupling not only the locations of the publishers and subscribers, but also decouple them temporally.

3.5. Components in action

The interaction among the components described in reported in Fig. 3. The indoor infrastructure periodically advertises its presence broadcasting an URI. The URI points to the meta-information of the ILS. When the end-user enables the indoor positioning on its device, the User Agent starts listening for such announces (Listen for URI activity). The Discovery phase ends when the User-agent accesses the URI in order to obtain the description of all the resources that are part of the infrastructure. The structure of the information obtained during the discovery phase represents a key-point. We report a schematic example of such information in Fig. 4. The information reported can be represented following different formats, such as JSON or XML text-based format.

The Access stage can now start. During this stage, the end-user grants or denies some consents required by the ILS to work properly (Consent evaluation). This process can also in-volve a more fine-grained assessment of the consents (specialized consent acceptance activity), depending on the kind of services to be used. If consents are accepted, the subscription data as well as the collected consents are used by the G-ACS System for example:

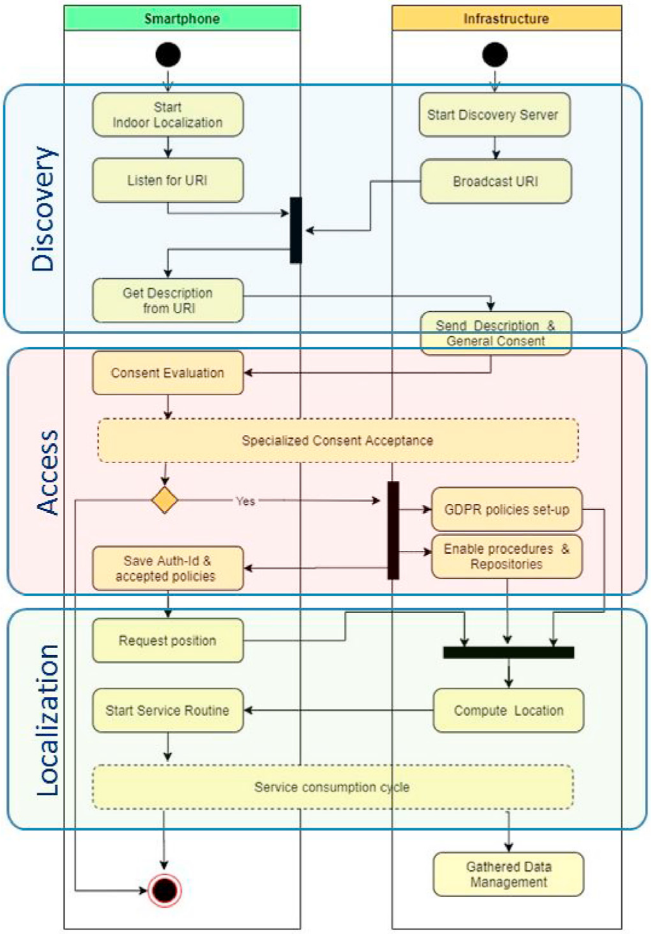

Fig. 3. Activity diagram for the system components.

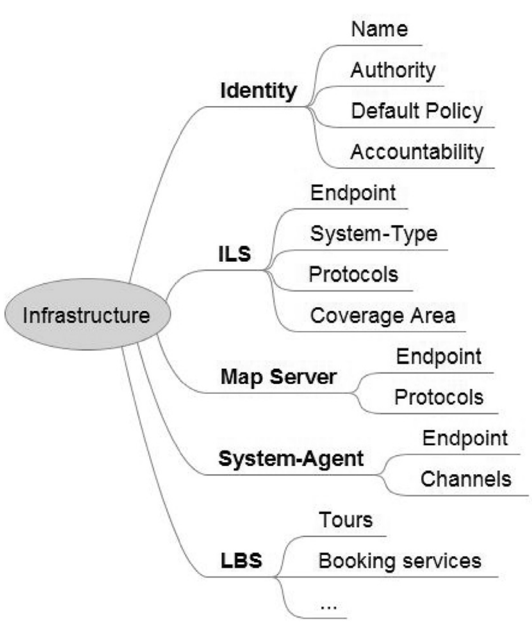

Fig. 4. Information describing an ILS through a Discovery Process.

- setting up the user specific GDPR-access control polices in order to guarantee that all the information collected and exchanged between the services are managed according the GDPR's demands (GDPR policies set-up activity);
- preparing the required database infrastructure and security procedures so as to guarantee for instance: the isolation of the data from the point of view of storage; the data anonymization; the data deletion according in agreement with the consensus collected (Enabling procedures and repositories activity).

On the other side, even the User Agent needs to save the policy accepted by the person and identification code that will be used to communicate with the infrastructure resources. Once the access phase has been finalized, the Service consumption cycle starts, that is the Localization phase. At this point. the user interaction and (privacy) data flow is realized taking in account the GDPR provisions such as: assure data treatment in line with purposes and scopes specified in the collected consents (as per Art. 5.1(a) of the GDPR), assure only authorized data transfer to third parties in accordance with the general principle demanded in Art. 44, and the enforcement of the Right to erasure ('right to be forgotten') defined in Art. 17, (Gathered Data Management phase) Right-to-be-Forgotten, (Gathered Data Management phase), in line with Art. 17. The process ends in case of consent revocation (in this case we are considering the right to withdraw as stated in Art. 7.3) or when the user requires to terminate a specific service.

4. Designing indoor social distancing

We now discuss how to guarantee social distancing of users in three representative use-cases, namely visiting a museum, accessing an airport and shopping assistant. We describe for each of them the overall user-experience, the requirements to be guaranteed and some enabling technologies that can be used for adopting an indoor localization system.

As a general observation, information about the physical distance among people can be exploited in three different stages: before, during and after the end-user visits a location. More specifically, knowing how people dispose indoor during the such stages, can increase the user-experience and improve the effectiveness of countermeasures to the diffusion of diseases (see Section 2). We report in Fig. 5 an example of how the information concerning the social distance can be used during while visiting a generic indoor environment. More specifically:

- *before* visiting an environment, the end-user can plan her/hist visit so that to avoid crowded time slots. Planning the visit allows to minimize the probability of involuntary contacts and it can reduce queue to access to specific services;
- *during* a visit, the end-user can optimize the way she/he moves indoor, so that to reduce the contact probability with others. As a representative example, we refer to the possibility of planning the order of products to pick while shopping. The path selection can be achieved by prioritizing those areas of a shopping mall scarcely visited by customers;
- information about the social distance can also be used *after* the visit. More specifically, knowledge about how many people visited a specific location, can be used to plan an efficient cleaning schedule, to better dispose products and, more generally, to allow the service provider to re-think the way services is accessed. Data collected after the visits can be used for statistical purpose as well, in order to measure if the actions taken prevent the existence of crowds.

4.1. Use case 1: visiting a museum

Visiting a museum is a challenging scenario in which to guarantee a proper social distance among the visitors. A museum is generally organized with a visiting path designed to guide visitors through the artworks. Users can decide to follow the path and to move across the rooms in a specific order. Small museums do not recommend any specific path

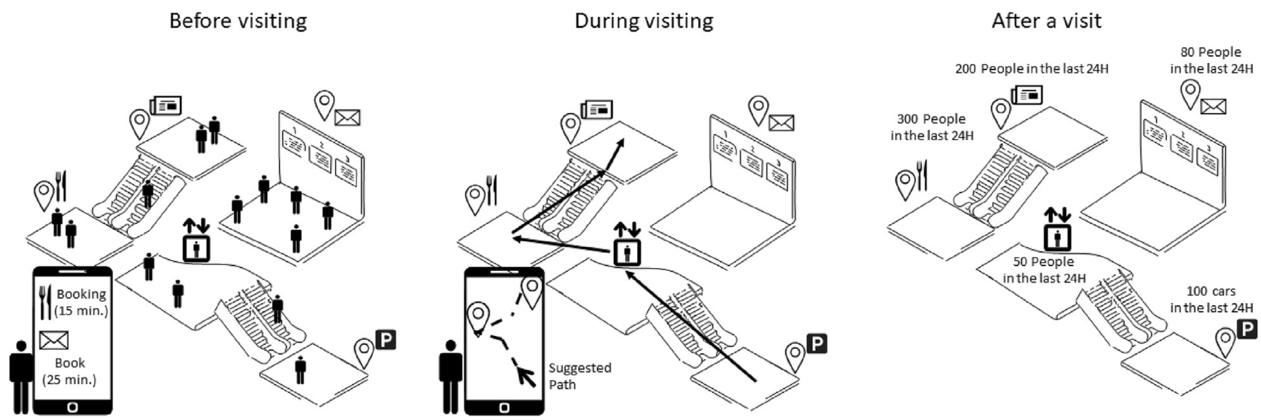

Fig. 5. How information about social distance can be used before, during and after visiting a generic indoor environment.

to follow, while others have multiple paths. Users following a path do not have any time restriction during their visits, they are free to move across the rooms and to rest. Moreover, the number of visits in a museum changes dramatically according to several factors, such as the day of the week, the hour, the scheduled holidays as well as the whether conditions. The combination of such factors determines the existence of burst of visits, as discussed in Ref. [55] that are challenging to predict.

The requirements that need to be preserved during a visit are:

- users have to be able to respect easily the distance from other visitors;
- the total number of visitors has to be managed;
- design multiple visiting paths so that to reduce the encounter probability among visitors;
- the user-experience needs to be guaranteed during a visit;
- users can wear a wristband or install a specific app before their visit;

We consider that the adoption of an indoor localization system in a museum can support the adoption of effective countermeasures for limiting crowded areas. More specifically, the knowledge of the position of the visitors can be used for 1) observing the way visitors access the museum and 2) to manage in real-time the flow of visits. Concerning the first goal, we argue that it is highly important to measure quantitatively the way visitors access a museum. More specifically, it is possible to measure the total amount of visits, the visits during a specific time interval, the visiting time for each room and artwork, the existence of preferential paths during a visit and other metrics useful to describe the social attitude of the users. Such information, can be in turn used to meet the second goal, namely to plan the visits according to the requirements previously reported.

Users can be localized by adopting proximity-based technologies such as Bluetooth Low Energy (BLE) or the UltraWide frequencies. Such technologies are becoming more and more popular. In particular, BLE is already available in most of the commercial smart devices, while the UltraWide technology is expect to diffuse in the near future. It is worth to notice that the iPhone 11 already provides the U1 chip-set. Bluetooth and UltraWide band allow to detect proximity not only between users but also between users and points of interests such as artworks or furniture. Moreover, such technologies can be easily integrated with personal devices such as smartphones or an audio guides without the need of a complex network infrastructure. Some remarkable works already addressed the problem of localizing people in a museum, we refer to Refs. [56–58] for further details.

4.2. Use case 2: airport access

The layout of an airport is generally a combination of indoor/outdoor multi-floor environments with restricted areas. Except for shops, generally the airports offer multi-storey buildings within wide and open spaces in which users freely roam. An airport terminal provides several services for the end-users. Some of them are mandatory to all the passengers, others are optional and provided only for the entertainment purpose. The number of users accessing to such services changes dramatically according to the seasons and according to external factors, such as weather conditions, strikes and delays of the flights.

The requirements that need to be preserved for travellers in order to guarantee appropriate social distance are:

- the airport facilities have to be accessed with a pre-determined order. More specifically, users have to check-in, to pass through the security clearances and, finally, to step toward the destination gate. The order and the time to complete the previous steps should be orchestrated so that to consider: the amount of users, the existence of crowds and any situation leading to involuntary contacts;
- users have to be able to respect easily the distance from other users;
- the user-experience must be preserved as much as possible;

Also for this use-case, we consider beneficial the adoption of a modular indoor localization system tracking the distance among users. In particular, the indoor localization system can be used for detecting the existence of crowds in a specific location e.g. check-in desks and to prevent other passengers to stack in queue. Furthermore, such localization system can be also exploited for security tasks, such as identification and tracking of target subjects. The majority of the terminals are already equipped with Wi-Fi networks available also for traveller. Some works already address the problem of localizing users in an airport. Authors of [59] proposes a multi-modal solutions based on Wi-Fi and BLE tags. Through the availability of a precise map of the environment and an accurate survey of the environment. The end-user can benefit of services based on positioning information on their own commercial smartphone. In [60] authors propose an interesting approach, based on BLE technology in an airport scenario, using a combination of Received Signal Strength Indication (RSSI) and Time-of-flight.

4.3. Use case 3: shopping assistant

A shopping mall is generally organized with product-specific aisles. Customers are free to decide the order of the products to pick. Malls also have some locations for specific fresh products, such as bakery or fresh-fish. In these locations, the self-service is generally not allowed, and customers interact with an operator. Some small/mid-size malls guide customers through a suggested walking path, while in large-scale malls, customers can freely move within the areas.

Similarly, to the other use-cases, the number of users can changes along the time. The burst of visits can be roughly predicted since the working schedule forces many people to shop during the evening or week-ends. In this context, the requirements for respecting the social distance between customers are:

- specific products need to be booked in advance so that to reduce the number customers waiting in the same location;
- users should be able to easily respect the distance from other users;
- the user-experience must be preserved as much as possible.

A shopping mall equipped with an indoor localization system can provide several services for customers. We foresee the possibility of optimizing the path to follow in order to completing the shopping list. Moreover, the supermarket can provide a queue management service that notifies the customers when to approach to a specific desk. Finally, a supermarket can provide services for personalized advertising to the end-users. In fact, indoor positioning systems shall make available a set of personal data which can be exploit to promote sales products or to promote temporary offers.

In the last decade, supermarkets have been equipped with internet access, throughout Wi-Fi Access Points deployed in the environment. These APs can be exploited also to provide an indoor localization services. The more promising technique in this environment is the fingerprinting technique, where the RSSI previously collected together with the position of the user is leveraged to infer the current user position [61]. In fact, the accuracy of this technique ranges in the order of few meters and, exploiting also inertial sensors of the smartphone, ILSs are generally able to localize users accurately. A distributed ILS can provide meaningful information before, during and after shopping. For example, before shopping, users can use the aggregated information about the number of current buyers to plan the purchases or not. During shopping, the user is reassured about the use of the ILS which can provide a "safe route" as described before. After shopping, information related to all the routes followed by customers can be used to thoroughly sanitize the most frequented spaces.

4.4. A reference architecture for different use cases

Although our goal is not to define a reference implementation of the architecture described in Section 3, we consider that some of the components in Fig. 2 can be implemented with existing software artifacts available in the current literature. We report in this section some meaningful examples both for the Indoor Infrastructure and for the Smart Device.

Concerning the Indoor Infrastructure, the Map Server is responsible for managing the indoor map. In particular, it provides the base maps or a tile set covering a specific area. The Map Server couples with the client side, in charge or downloading (possibly, with parallel connections) and rendering the map on a e.g. 5-inch screen. Both modules are available in literature and can be re-used as third-party black boxes. As for example, the open source map-view solutions, open layers and leaflet are available. According to the specific needs, it is also possible to adopt different Map Server such as mapbox, Google Maps and AcrGis.[3]

Concerning the ILS engine the literature also offers some interesting and open source solutions that can be deployed as off-the-shelf products, among them we refer to Anyplace as a complete framework for indoor localization comprising API, Viewer, Navigator and Logger components.[4] We finally mention some existing discovery protocols that can be embedded with the Indoor Infrastructure to discover the server in a seamless way. In particular, the SLP, UPnP, ZeroConf and WS-Discovery are old-but-robust valuables candidates for discovering networked resources [62]. Moreover, if the goal is to implement a local discovery then the Bluetooth beaconing and the Wi-Fi probing also represent two interesting protocols that can be used to broadcast small chunk of information.

Finally, in relation to the Smart Device we found several client interfaces that can be customized. Among them, we consider that Telegram app[5] is a valuable alternative since it offers the possibility of customizing the popular chat-based application by reusing most of features available. Such choice allows to include specific features enabling the localization, the discovery and the map rendering in a chat box. We finally remark that guidelines for choosing the proper technical solution are out of the scope for this paper but, it is worth to remark that these design decisions strongly depend on the considered use cases.

5. Towards social distancing through ILS

We now discuss some issues related to the concrete possibility of adopting an indoor localization system for the purpose of measuring the distance among users. This section covers different aspects of its adoption. In particular, in subsection 5.1 we discuss the impact on the privacy and trust reputation of the ILS. Subsection 5.2 focuses on the discovery phase of ILS. Subsection 5.3 presents two alternatives for the social distancing, namely a manual and automatic approach and, lastly, subsection 5.4 concludes with a description of some challenges of the deployment phase of an ILS in real-world settings.

5.1. Privacy and trust reputation

Our first consideration faces with the problem of how to guarantee privacy of data collected by an ILS. We refer to [63] for complete survey also covering the following issues.

Privacy by design encompasses seven principles that should be followed [64]: proactive privacy protection instead of remedial action after privacy violations have happened; privacy as the default setting; privacy embedded into the design; full functionality with full privacy protection; privacy protection through the entire life-cycle of the data; visibility and transparency; and respect for user privacy. Solutions for incorporating these principles in the design of an ILS are necessary. In parallel, data minimization approaches should be considered as a best practice for privacy by design adoption.

Furthermore, we argue that information sharing, active defence and automation methods should be integrated with an ILS. Thus, we consider mandatory to develop efficient methods to create, disseminate, and consume threat intelligence in a standardized and admissible way. It is also necessary to adopt defence mechanisms able to increasing the cyber adversary's cost by decreasing their overall efficiency of the active cyber operation. In parallel, in order to make the solutions effective, automation should be considered and solutions integrated into business workflow, governance, and structure control.

We also consider an orthogonal aspect of the privacy, namely the trust reputation of the ILS. Since the architecture described in Fig. 1 involves a variety of components, it is required to implement different protections policies and to ensure that there are no privacy leaks at any of the stages we modelled in Fig. 3. Additionally, the architecture should be deployable across different systems and environments maintaining the required level of trust. Another aspect linked with the management of the trust of the system, is how to guarantee trust for third-party components that an ILS can integrate. As for example: multiples Map servers and different implementations of ILSs can coexist with the design presented in Section 3. To this purpose, we foresee some possible solutions: to provide interoperability recommendations and specifications; to define specific governance; to provide on-line verification and validation tools in order to identify the security risks. In parallel, data should be encrypted both at rest and in transit.

[3] http://openlayers.org, https://leafletjs.com/.
[4] www.indoorlocation.io/.
[5] http://github.com/DrKLO/Telegram.

5.2. Discovering an ILS with local and global interfaces

The capability of discovering an ILS automatically is a central aspect. We consider two possible approaches for the discovery phase: local and global. The local discovery is based on the analysis of local signals when entering a new environment. In this case, the user exploits short-range network interfaces looking up for nearby signals. However, we consider that a global search is required as well. In this last case, a standard search through a web-browser allows to query and to connect with the ILS. We recall the well-known user experience though which users look for services on a search engine. The search engine summarizes to the user a box with key information about the service, such as the street address, the opening hours, the popularity of the service (e.g. Google Popular Times). We expect to extend such list, by also reporting the information of the Indoor Localization System, e.g. showing an URL with the meta-information reported in Fig. 4.

Mobility in multiple indoor environments increases privacy issues. Continuing on the example of the outdoor navigation services offered by Google, we know that the people who activate the history of their positions are tracked by Google, which, through the user account, allows you to view your movements and possibly eliminate them entirely. In the case of indoor navigation, this information will be collected by multiple subjects who must make it accessible to the owners of the data both for consultation and for modification. The task of the User Agent in this case becomes essential, because it must be capable of maintaining a history of the indoor sites visited. In particular, it must keep track of the policies and consents signed by the user, as well as links to the various interfaces to access the consultation and modification services of personal data. Nevertheless, much of this information must be conveyed during the Discovery process (Figure JSON file) Privacy management in general is more complex than the use case presented here, de-pending on whether the localization techniques used are Self-positioning or Remote positioning based. Systems that intrinsically guarantee privacy should be favoured, in which the position is estimated by the user agent (self-positioning) and is not known by other subjects, such systems are also more scalable. However, with respect to social distancing, you must in any case give up your rights and reveal your position even if used only anonymously, therefore defining an access control based on GDPR is always an indispensable step.

5.3. A dichotomy of manual and automatic social distancing

Another crucial aspect is the safety distance among people (usually fixed in the range of 1–2 m) which is normally perceivable on sight. People in favour of using automatic tools to support social distancing are already well prepared to keep the right distance from others. We observe two conflicting requirements: firstly, service providers e.g. a shopping centre, aim to increase the number of customers while, secondly, customers are interested to access a service scarcely populated. Therefore, a service obeying to the current prescriptions will grant the access to the maximum number of admitted customers. Such situation is generally perceived by the final users as potentially unhealthy, even if customers stay 1–2 m away from others. Such consideration is predominantly of psychological nature. However, we argue that also the adoption of apps for preserving the social distance do not resolve the dichotomy between number of customers and distance among them. In fact, the false positive/negative alerts of such app, combined with the privacy issues previously mentioned, discourage their use in the daily basis.

Under this respect, the technology adopted by the apps is determinant for their successful adoption on the large scale. More specifically, range-based applications (i.e. based on Wi-Fi/Bluetooth signal strength) often fail in crowded scenarios or in those environments characterized by barriers and obstacles. Differently, the adoption of indoor localization system based on the data-fusion techniques are more reliable in such circumstances. Data-fusion allows to gather and to combine heterogeneous sensing and context information. Although more complexity with respect to a range-based approach, fusing data together allows to overcome issues such as body attenuation, indoor reflections and multi-path fading. The side-effect of an Indoor Localization System is the mostly represented by its installation costs.

The current trend is to adopt solutions for preserving the social distance that are based on apps for smartphones. We consider that such approach might fail on the large-scale and on the long-term. We consider necessary to understand those practicable alternatives and how to gradually move from the use of apps to the use of infrastructures, such as an Indoor Localization System.

If we consider that people are well predisposed for social distancing through the use of sight, a first discriminating factor is the type of environment. In open spaces, such as a supermarket, people will have greater ease of self-determination if a situation is risky or not. Differently, in indoor and constrained environments people need to be supported with automatic tools.

The transition from manual to automatic systems for social distancing requires bridging technologies able to reduce the deployment costs. As a remarkable example, we mention those systems designed to count the number of people in each room. Once a certain density has been reached, the system warns incoming people, in order to limit the access to such places. In any case, even if a precise localization system is not used, common interfaces must be studied through which to communicate to all end-users. Other aspect to consider is that the turnout of people could be estimated from the reservations that are made to visit a certain environment. This practice is currently used by the most visited museums, where you can buy tickets online and avoid long queues to buy tickets. In other environments such as airports, by integrating the various information systems of the airline companies, the number of people at a certain time can be determined on the basis of the scheduling of flights departing and arriving. Obviously, this is an alternative to preparing new infrastructures for localization, but it is an estimate that can be affected by various random factors, lost reservations, flight delays, random congestion. But even in this case, an interface to people who access the environment/system is necessary to allow it to check the crowding status and possibly receive notifications.

5.4. Deploying an ILS in real-world environments

We now discuss some deployment issues of an ILS that at realistic conditions.

Deploying an ILS requires to accomplish at least the following two steps: survey of the environment and hardware installation and system calibration. Such steps are required for all the use-cases we detailed in Section 4. The first step requires to visit the environment where the ILS is supposed to be deployed, with the goal of considering features of potential impact to the performance of the system. Some examples are: the building-material of the environment, the dimension of the area to be covered and the existence of outdoor/indoor areas. The building material of the environment has a great impact to the propagation of radio signals. As for example, concrete-based walls heavily attenuate 802.11 signals modulating at 2.4 GHz, with respect to wooden or drywall. Moreover, the shape of the environment is another feature that influences the signal propagation. Wireless signals, generally, propagate more easily in open spaces due to the limited presence of obstacles. Finally, the existence of outdoor areas to be covered also influences the overall performance.

The previous step leads to the installation of the hardware required by an ILS. This step, usually, requires to find places where to deploy anchor nodes enabling the localization of the users, such as Wi-Fi Access Points, Bluetooth tags or UltraWide band boards. The hardware to be deployed often requires a power supply source in the nearby, the absence of surrounding obstacles and a safety distance from the end-users. The combination of such requirements makes the deployment a challenging task in places not designed for such purpose.

The last step copes with the configuration of the ILS. With the term configuration, we refer to all the settings depending on environmental

Table 3
Evaluation framework of the reference architecture.

	KPI	Objective	Measuring tool	Unit	Issues
End-user	Personalized feedbacks	To measure the overall impression of the final users (feel of protection, motivation is using the app)	questionnaire, survey	Statistics with the reported answers	1. Share the questionnaire 2. Bias of the answers caused by frustration and anxiety emotional states
Smart-Device	User acceptance	The success of ILS depends on the way the user interacts with it	users feedback: average number of scores received	Statistics with the reported answers	none
	Energy consumption	To measure the impact of the app to the battery life-cycle	Reporting APIs provided by iOS and Android SDKs	(Milli) Watts consumed by the app	none
	App usage	To estimate the usage of the app and the voluntary/involuntary stops of thew app	Reporting APIs provided by iOS and Android SDKs	1. Average usage time 2. Number of crash 3. Number of stops of the app	To manage appropriately any sensitive information collected
	Discovery and Access latency	To measure the time required by the app to discovery and access to the Indoor infrastructure	Profiling APIs available for iOS and Android SDK	Milliseconds	none
	Initial localization	To measure the time required by the app to compute the initial localization of the device	Custom reporting APIs profiling.	Milliseconds	none
	Maps Data transferred	To measure the amount of data transferred for rendering indoor maps	Profiling APIs available for iOS and Android SDK or Custom reporting APIs profiling	#byte	none
Indoor infrastructure	location latency	To measure the time required by the infrastructure to localize the smart device.	Custom profiling API server-side	Milliseconds	none
	ILS load	To measure the computational load of the ILS to estimate the position of all the devices connected	Performance profiling tools (e.g. Java JMX, Python DataDog client, Visual Studio profiler)	1. CPU load 2. RAM allocated 3. Data structure inspection	Overhead of the profiling tool
	Map Server load	To measure the computational load of the Map Server to provide maps to the clients	Performance profiling tools (e.g. Java JMX interface, Python DataDog client, Visual Studio)	1. CPU load 2. RAM allocated 3. Data structure inspection 4. Data transfer rate	Overhead of the profiling tool
	performance of the proximity detection	To measure the correct detection of devices in proximity	Custom reporting API	Confusion matrix from which extract: Accuracy, Precision, F1, k-Statistics etc. metrics	To compare the results obtained with a reliable ground-truth to build the confusion matrix
	update location frequency	To measures the system's capacity to re-compute the user's locations seamlessly	Custom reporting API	Ratio between the number of received samples and the number of expected samples (for instance one every second).	none
Service-provider	Installation complexity	To measure the technical issues behind a correct deployment the indoor infrastructure	Custom reporting tool maintenance effort	Time of installation and of configuration,	none

settings. As a meaningful example, we refer to the fingerprint-based techniques (see subsection 2.1). In this case, the localization system requires a database mapping the quality of the radio signals (e.g. Received Signal Strength Indicator) with a number of locations. Such database is generally built only after the hardware installation and it can be obtained with a data collection campaign often achieved manually by an expert. Another representative example of configuration is represented by all the algorithm settings of the ILS it-self. Such settings, very often, model features of the environment and they can be tuned only after the installation of the system in the target environment. Nevertheless, the configuration of a ILS is not one-shot task. Rather, real-world localization systems configured and re-configured multiple times during their life-cycle. Some factors that require a new round of configuration are: environmental changes such as new obstacles or a new layout of the environment, new areas to be covered or modifications due to hardware replacement.

6. Measuring the performance of the integrated architecture

We finally focus on the assessment of the performance of the integrated architecture as a crucial part of applicability of the solution we propose in this work. Our goal is to frame a reference architecture based on localization techniques for the purpose of measuring quantitatively the distance among people roaming in an indoor environment. In this picture, both the user experience and the hardware/software components can be measured to understand the effectiveness and its real applicability in real-world scenarios. To this purpose, we consider a set of measurable KPIs addressed to the 4 main players: the End-Users, the Smart Device, the Indoor Infrastructure and the Service Providers. We detail the motivation behind the such choices, how to measure the KPIs, the unit of measurement and any critical issue arising from the KPI. Table 3 summarizes the KPIs we propose.

7. Conclusions

Computing the inter-personal distance among people in real-time represents a challenging task. However, the recent COVID-19 pandemic imposes such requirement to the way people interacts and to the way people access services in indoor environments. Countries affected by such pandemic reacted to the emergency in different ways by adopting counter-measures that, in some circumstances, might be not effective after the lock-down phase. In particular, we focus on exploitable technologies for guaranteeing social distance among people that are generally employed in the field of indoor localization. In this work, we describe the adoption of an Indoor Localization System (ILS) with a twofold goal. On one hand, the ILS can be adopted to localize people and, on the other hand, for measuring the in-between physical distance. We first present some functional requirements for an ILS and a reference architecture. Then, we present three significant use-cases where an ILS can be adopted for measuring distance among users. We discuss how information describing the distance among people can be used during three stages: before, during and after accessing a service. We also discuss some issues and new possible new lines of investigation concerning the design of an ILS for the purpose of the social distance. In particular, our attention moves towards the design of discovery protocol able to identify available ILSs indoor and to the adoption of privacy mechanisms for the treatment of sensitive information collected about end-users. The letter point is, in our opinion, one of the most important barrier to the adoption and diffusion location-based services. We argue that a more transparent approach for the data treatment would benefit the adoption of such location-based services offered by ILSs.

Credit author statement

Paolo Barsocchi: Conceptualization, Methodology, Investigation, Supervision, Visualization, Writing – review & editing. Antonello Calabrò: Conceptualization, Methodology, Investigation, Supervision, Visualization, Writing – review & editing. Antonino Crivello: Conceptualization, Methodology, Investigation, Supervision, Visualization, Writing – review & editing. Said Daoudagh: Conceptualization, Methodology, Investigation, Supervision, Visualization, Writing – review & editing. Francesco Furfari: Conceptualization, Methodology, Investigation, Supervision, Visualization, Writing – review & editing. Michele Girolami: Conceptualization, Methodology, Investigation, Supervision, Visualization, Writing – review & editing. Eda Marchetti: Conceptualization, Methodology, Investigation, Supervision, Visualization, Writing – review & editing.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgment

This work is partially supported by CyberSec4Europe project grant agreement n. 830929.

References

[1] Zafari F, Gkelias A, Leung KK. A survey of indoor localization systems and technologies. IEEE Commun Surv Tutor 2019;21(3):2568–99.
[2] Shao W, Luo H, Zhao F, Ma Y, Zhao Z, Crivello A. Indoor positioning based on fingerprint-image and deep learning. IEEE Access 2018;6:74699–712.
[3] Vinicchayakul W, Promwong S, Supanakoon P. Study of uwb indoor localization using fingerprinting technique with different number of antennas. In: 2016 international computer science and engineering conference (ICSEC). IEEE; 2016. p. 1–4.
[4] F. Furfari, A. Crivello, P. Barsocchi, F. Palumbo, F. Potortì, What is next for indoor localisation? taxonomy, pro- tocols, and patterns for advanced location based services, in: 2019 international conference on indoor positioning and indoor navigation (IPIN), IEEE, pp. 1–8.
[5] Minoli D, Occhiogrosso B. Ultrawideband (uwb) technology for smart cities iot applications. In: 2018 IEEE international smart cities conference (ISC2). IEEE; 2018. p. 1–8.
[6] Basin D, Debois S, Hildebrandt T. On purpose and by necessity. In: Proceedings of the twenty-second interna- tional conference on financial cryptography and data security (FC); 2018.
[7] Ramadan Q, Salnitriy M, Strüber D, Jürjens J, Giorgini P. From secure business process modeling to design- level security verification. In: Proceedings of the ACM/IEEE 20th international conference on model driven engineering languages and systems (MODELS). IEEE; 2017. p. 123–33.
[8] Ranise S, Siswantoro H. Automated legal compliance checking by security policy analysis. In: Computer safety, reliability, and security - SAFECOMP 2017 workshops, ASSURE, DECSoS, SASSUR, TELERISE, and TIPS, Trento, Italy, september 12, 2017, proceedings, vol. 10489. Springer; 2017. p. 361–72. of Lecture Notes in Computer Science.
[9] Hsu J. The dilemma of contact-tracing apps: can this crucial technology be both effective and private? IEEE Spectrum 2020;57(10):56–9. https://doi.org/10.1109/MSPEC.2020.9205550.
[10] Potortì F, Crivello A, Girolami M, Barsocchi P, Traficante E. Localising crowds through wi-fi probes. Ad Hoc Netw 2018;75:87–97.
[11] Pelant J, Tlamsa Z, Benes V, Polak L, Kaller O, Bolecek L, Kufa J, Sebesta J, Kratochvil T. Ble device indoor localization based on rss fingerprinting mapped by propagation modes. In: 2017 27th international conference radioelektronika (RADIOELEKTRONIKA). IEEE; 2017. p. 1–5.
[12] T. Martin, G. Karopoulos, J. L. H. Ramos, G. Kambourakis, I. N. Fovino, Demystifying COVID-19 digital contact tracing: A survey on frameworks and mobile apps, CoRR abs/2007.11687. arXiv:2007.11687. URL https://arxiv.org/abs/2007.11687.
[13] Lee JH, Shin B, Shin D, Kim J, Park J, Lee T. Precise indoor localization: rapidly-converging 2d surface correlation-based fingerprinting technology using LTE signal. IEEE Access 2020;8:172829–38. https://doi.org/10.1109/ACCESS.2020.3024933.
[14] Ridolfi M, Van de Velde S, Steendam H, De Poorter E. Analysis of the scalability of uwb indoor localization solutions for high user densities. Sensors 2018;18(6):1875.
[15] Li P, Yang X, Yin Y, Gao S, Niu Q. Smartphone-based indoor localization with integrated fingerprint signal. IEEE Access 2020;8:33178–87. https://doi.org/10.1109/ACCESS.2020.2974038.
[16] He S, Chan S-HG. Wi-fi fingerprint-based indoor positioning: recent advances and comparisons. IEEE Commun Surv Tutor 2015;18(1):466–90.
[17] Girolami M, Mavilia F, Delmastro F, Distefano E. Detecting social interactions through commercial mobile de- vices. In: 2018 IEEE international conference on

Pervasive computing and communications workshops (PerCom workshops); 2018. p. 125–30.
[18] Barral V, Sua′rez-Casal P, Escudero CJ, Garc′ıa-Naya JA. Multi-sensor accurate forklift location and tracking simulation in industrial indoor environments. Electronics 2019;8(10):1152. https://doi.org/10.3390/electronics8101152.
[19] Xu Y, Shmaliy YS, Li Y, Chen X. Uwb-based indoor human localization with time-delayed data using filtering. IEEE Access 2017;5:16676–83.
[20] Bregar K, Mohorcic M. Improving indoor localization using convolutional neural networks on computationally restricted devices. IEEE Access 2018;6:17429–41.
[21] You W, Li F, Liao L, Huang M. Data fusion of uwb and imu based on unscented kalman filter for indoor localization of quadrotor uav. IEEE Access 2020;8: 64971–81.
[22] Van Opdenbosch D, Schroth G, Huitl R, Hilsenbeck S, Garcea A, Steinbach E. Camera-based indoor position- ing using scalable streaming of compressed binary image signatures. In: 2014 IEEE international conference on image processing (ICIP). IEEE; 2014. p. 2804–8.
[23] Zhang W, Kavehrad M. Comparison of vlc-based indoor positioning techniques. In: Broadband access communi- cation technologies VII, vol. 8645. International Society for Optics and Photonics; 2013. 86450M.
[24] Shao W, Luo H, Zhao F, Wang C, Crivello A, Tunio MZ. Depedo: anti periodic negative-step movement pedometer with deep convolutional neural networks. In: 2018 IEEE international conference on communications (ICC). IEEE; 2018. p. 1–6.
[25] Kim S-E, Kim Y, Yoon J, Kim ES. Indoor positioning system using geomagnetic anomalies for smartphones. In: 2012 International conference on indoor positioning and indoor navigation (IPIN). IEEE; 2012. p. 1–5.
[26] Shao W, Luo H, Zhao F, Crivello A. Toward improving indoor magnetic field–based positioning system using pedestrian motion models. Int J Distributed Sens Netw 2018;14(9). 1550147718803072.
[27] Lu C, Uchiyama H, Thomas D, Shimada A, Taniguchi R-i. Indoor positioning system based on chest-mounted imu. Sensors 2019;19(2):420.
[28] Shao W, Luo H, Zhao F, Wang C, Crivello A, Tunio MZ. Mass-centered weight update scheme for particle filter based indoor pedestrian positioning. In: 2018 IEEE wireless communications and networking conference (WCNC). IEEE; 2018. p. 1–6.
[29] Lemic F, Handziski V, Mor N, Rabaey J, Wawrzynek J, Wolisz A. Toward standardized localization service. In: 2016 international conference on indoor positioning and indoor navigation (IPIN). IEEE; 2016. p. 1–8.
[30] Stevenson G, Ye J, Dobson S, Nixon P. Loc8: a location model and extensible framework for programming with location. IEEE Pervasive Comput 2009;9(1): 28–37.
[31] Zeinalipour-Yazti D, Laoudias C. The anatomy of the anyplace indoor navigation service. SIGSPATIAL Spec 2017;9(2):3. https://doi.org/10.1145/3151123.3151125.
[32] Immuni, uno strumento in piu' contro l'epidemia. https://www.immuni.italia.it/.
[33] ufirst, risparmia tempo con ufirst. URL https://www.ufirst.com/.
[34] Kunai. URL https://github.com/kunai-consulting/OpenTrace.
[35] Skyook https://syook.com/the-social-distancing-app/.
[36] Who has access to your smartphone data? https://cacm.acm.org/magazines/2020/10/247585-who-has-access-to-your-smartphone-data/fulltext.
[37] ifeel-you bracelet. https://www.iit.it/iit-vs-covid-19/ifeel-you-bracelet.
[38] Nguyen QH, Johnson P, Nguyen TT, Randles M. A novel architecture using ibeacons for localization and tracking of people within healthcare environment. In: 2019 global IoT summit (GIoTS). IEEE; 2019. p. 1–6.
[39] Regulation (EU). 2016/679 of the European parliament and of the council of 27 april 2016 (general data protection regulation). Off J Eur Union 2016;L119:1–88.
[40] eXtensible Access Control Markup Language (XACML) Version 3.0 (2013). http:\docs.oasis-open.org\xacml\3.0\xacml-3.0-core-spec-os-en.html.
[41] Holcer S, Torres-Sospedra J, Gould M, Remolar I. Privacy in indoor positioning systems: a systematic review. In: 2020 international conference on localization and GNSS (ICL-GNSS); 2020. p. 1–6.
[42] Greaves B, Coetzee M, Leung WS. A comparison of indoor positioning systems for access control using vir- tual perimeters. In: Fourth international congress on information and communication technology - ICICT 2019, London, UK, february 25-26, 2019, vol. 1; 2019. p. 293–302.
[43] Järvinen K, Leppäkoski H, Lohan E, Richter P, Schneider T, Tkachenko O, Yang Z. PILOT: practical privacy- preserving indoor localization using outsourcing. In: 2019 IEEE European symposium on security and privacy (EuroS P); 2019. p. 448–63.
[44] R. Nieminen, K. Jarvinen, Practical privacy-preserving indoor localization based on secure two-party computation, IEEE Trans Mobile Comput (01) (5555) 1–1. doi: 10.1109/TMC.2020.2990871.
[45] Yang Z, Järvinen K. The death and rebirth of privacy-preserving wifi fingerprint localization with paillier encryption. In: IEEE INFOCOM 2018 - IEEE conference on computer communications; 2018. p. 1223–31.
[46] Greaves B, Coetzee M, Leung WS. Access control requirements for physical spaces protected by virtual perime- ters. In: Furnell S, Mouratidis H, Pernul G, editors. Trust, privacy and security in digital business. Cham: Springer International Publishing; 2018. p. 182–97.
[47] Haofeng J, Xiaorui G. Wi-fi secure access control system based on geo-fence. In: Proceedings of ISCC 2019; 2019. p. 1–6.
[48] Jensen CD, Geneser K, Willemoes-Wissing IC. Sensor enhanced access control: extending traditional access control models with context-awareness. In: Ferna′ndez-Gago C, Martinelli F, Pearson S, Agudo I, editors. Trust management VII. Berlin, Heidelberg: Springer Berlin Heidelberg; 2013. p. 177–92.
[49] Barsocchi P, Calabrò A, Ferro E, Gennaro C, Marchetti E, Vairo C. Boosting a low-cost smart home environment with usage and access control rules. Sensors 2018; 18(6):1886.
[50] Calabrò A, Marchetti E, Moroni D, Pieri G. A dynamic and scalable solution for improving daily life safety. In: Proceedings of APPIS 2019; 2019. p. 1–6.
[51] Daoudagh S, Marchetti E. A life cycle for authorization systems development in the gdpr perspective. In: Proceedings of the fourth Italian conference on cyber security, Ancona, Italy, February 4-7, 2020; 2020.
[52] Bartolini C, Daoudagh S, Lenzini G, Marchetti E. Towards a lawful authorized access: a preliminary gdpr- based authorized access. In: Proceedings of ICSOFT 2019, Prague, Czech Republic, july 26-28, 2019; 2019. p. 331–8.
[53] Girolami M, Barsocchi P, Chessa S, Furfari F. A social-based service discovery protocol for mobile ad hoc networks. In: 2013 12th annual mediterranean ad hoc networking workshop (MED-HOC-NET); 2013. p. 103–10.
[54] Crivello F Potortì A, Girolami M, Traficante E, Barsocchi P. Wi-fi probes as digital crumbs for crowd localisation. In: 2016 international conference on indoor positioning and indoor navigation (IPIN); 2016. p. 1–8. https://doi.org/10.1109/IPIN.2016.7743599.
[55] Isella L, Stehle′ J, Barrat A, Cattuto C, Pinton J-F, den Broeck] WV. What's in a crowd? analysis of face-to-face behavioral networks. J Theor Biol 2011;271(1): 166–80. https://doi.org/10.1016/j.jtbi.2010.11.033.
[56] Alletto S, Cucchiara R, Del Fiore G, Mainetti L, Mighali V, Patrono L, Serra G. An indoor location-aware system for an iot-based smart museum. IEEE Internet Things J 2016;3(2):244–53.
[57] Xia H, Zuo J, Liu S, Qiao Y. Indoor localization on smartphones using built-in sensors and map constraints. IEEE Trans Instrum Meas 2019;68(4):1189–98.
[58] Wu X, Shen R, Fu L, Tian X, Liu P, Wang X. ibill: using ibeacon and inertial sensors for accurate indoor localization in large open areas. IEEE Access 2017;5:14589–99.
[59] Molina B, Olivares E, Palau CE, Esteve M. A multimodal fingerprint-based indoor positioning system for airports. IEEE Access 2018;6:10092–106.
[60] Giovanelli D, Farella E. Rssi or time-of-flight for bluetooth low energy based localization? an experimental evaluation. In: 2018 11th IFIP wireless and mobile networking conference (WMNC). IEEE; 2018. p. 1–8.
[61] Renaudin V, Ortiz M, Perul J, Torres-Sospedra J, ì Jime′nez AR, Pe′rez-Navarro A, Mendoza-Silva GM, Seco F, Landau Y, Marbel R, et al. Evaluating indoor positioning systems in a shopping mall: the lessons learned from the ipin 2018 competition. IEEE Access 2019;7:148594–628.
[62] Meshkova E, Riihijarvi J, Petrova M, Mahonen P. A survey on resource discovery mechanisms, peer-to-peer and service discovery frameworks. Comput Network 2008;52(11):2097–128. https://doi.org/10.1016/j.comnet.2008.03.006.
[63] Deliverable D4.3: Research and Development Roadmap. Research-and-Development-Roadmap-1-Submitted.pdf. 2020.
[64] Cavoukian A. Privacy by design: leadership, methods, and results. Dordrecht: Springer Netherlands; 2013. p. 175–202. https://doi.org/10.1007/978-94-007-5170-5_8.