computers

MDPI

Article

Smart Interconnected Infrastructures for Security and Protection: The DESMOS Project

Michail Feidakis [1,*], Christos Chatzigeorgiou [1], Christina Karamperi [2], Lazaros Giannakos [2], Vasileios-Rafail Xefteris [3], Dimos Ntioudis [3], Athina Tsanousa [3], Dimitrios G. Kogias [4], Charalampos Patrikakis [1], Georgios Meditskos [3,5], Georgios Gorgogetas [2], Stefanos Vrochidis [3] and Ioannis Kompatsiaris [3]

[1] Computer Networks & Services Research Laboratory, Ancient Olive Grove Campus, University of West Attica (UniWA), ZB 214, Thivon 250 & Petrou Ralli Street, 12241 Egaleo, Greece; chrihatz@uniwa.gr (C.C.); bpatr@uniwa.gr (C.P.)
[2] E-TRIKALA S.A., Kalampakas & Ampatis 28 Str., 42100 Trikala, Greece; xkaraberi@e-trikala.gr (C.K.); lgiannakos@e-trikala.gr (L.G.); ggorgogetas@e-trikala.gr (G.G.)
[3] Centre for Research and Technology Hellas, Information Technologies Institute, 6th Km Charilaou-Thermi, 57001 Thessaloniki, Greece; vxefteris@iti.gr (V.-R.X.); ntdimos@iti.gr (D.N.); atsan@iti.gr (A.T.); gmeditsk@iti.gr (G.M.); stefanos@iti.gr (S.V.); ikom@iti.gr (I.K.)
[4] iTrack Services Ltd., Kifissou 59, Ag. I. Rentis, 18233 Piraeus, Greece; dimikog@itrack.gr
[5] School of Informatics, Aristotle University of Thessaloniki, 54124 Thessaloniki, Greece
* Correspondence: m.feidakis@uniwa.gr

Citation: Feidakis, M.; Chatzigeorgiou, C.; Karamperi, C.; Giannakos, L.; Xefteris, V.-R.; Ntioudis, D.; Tsanousa, A.; Kogias, D.G.; Patrikakis, C.; Meditskos, G.; et al. Smart Interconnected Infrastructures for Security and Protection: The DESMOS Project. *Computers* **2021**, *10*, 116. https://doi.org/10.3390/computers10090116

Academic Editor: Grigorios E. Koulouras

Received: 19 August 2021
Accepted: 8 September 2021
Published: 16 September 2021

Abstract: This paper presents "DESMOS", a novel ecosystem for the interconnection of smart infrastructures, mobile and wearable devices, and applications, to provide a secure environment for visitors and tourists. The presented solution brings together state-of-the-art IoT technologies, crowdsourcing, localization through BLE, and semantic reasoning, following a privacy and security-by-design approach to ensure data anonymization and protection. Despite the COVID-19 pandemic, the solution was tested, validated, and evaluated via two pilots in almost real settings—involving a fewer density of people than planned—in Trikala, Thessaly, Greece. The results and findings support that the presented solutions can provide successful emergency reporting, crowdsourcing, and localization via BLE. However, these results also prompt for improvements in the user interface expressiveness, the application's effectiveness and accuracy, as well as evaluation in real, overcrowded conditions. The main contribution of this paper is to report on the progress made and to showcase how all these technological solutions can be integrated and applied in realistic and practical scenarios, for the safety and privacy of visitors and tourists.

Keywords: IoT; smartphone; bracelet; localization; crowdsourcing; privacy; security; computer intelligence

1. Introduction

Latest advancements in Internet-of-Things (IoT), wearable devices (sensors, smartphones), as well as data analytics, have attracted research interest in streaming real data analysis, with applications to various domains such as tourism and culture [1]. Semantic technologies and ontologies facilitate the interoperability between entities and platforms [2] for semantic sensor networks, while crowdsourcing and crowdsensing [3] have become a new paradigm for information exchange going beyond user-to-user communication. The latter, of course, entails new challenges in guaranteeing anonymity over data transmission. The provision of intelligence in sensor environments is an interactive process that requires monitoring changes, updating relevant services, and triggering system response [4], considering not only the interaction of objects but also the integration of software agents [5].

The integration of recent IoT and wearable technologies, together with the latest advancements in Computer Intelligence and Machine Learning, can provide the necessary

technological capacity to ensure security, safety, and privacy, especially in critical conditions (i.e., heart attacks, thieveries, fires, etc.) that often occur in overcrowded tourist destinations. From now onwards, the current paper describes the DESMOS solution, a robust ecosystem that interconnects smart infrastructures, applications, and humans, to provide citizens and tourists with security and protection, while also respecting their anonymity. The system promotes collaboration between people and devices and increases citizens' protection through:

- Fast, timely, and accurate notifications in case of emergencies (e.g., allergic shock situations, medical incidents, heart attacks, etc.), sending at the same time all the contextual information needed to help authorities coordinate and assist people, while protecting the privacy of citizens;
- Anonymous reporting of incidents using crowdsourcing, with a special focus on incidents involving tourists, e.g., thefts;
- The adaptability of services and devices, to respond to incidents and protect citizens/tourists;
- Localization of persons in cases where GPS is limited or is not provided at all.

All the heterogeneous data and information are fused and interpreted through semantic reasoning and decision-making for supporting real-time alerts and notification of responsible entities.

The DESMOS solution brings together state-of-the-art technologies to cope with real issues and use cases specified by end-users in crowded places. Of course, such a solution can showcase some impact only when evaluated repeatedly and in real settings. Despite the COVID-19 pandemic, the DESMOS integrated system has been tested, validated, and evaluated in almost real settings through two pilots (A-Pilot, B-Pilot) involving 99 and 331 participants, respectively, which took place during July 2020–May 2021, in the Mill of Elves–Mylos Matsopoulou, and the City Centre, in Trikala, Thessaly, Greece. Out of these, three different use cases have been encountered: (1) Emergency medical event treatment; (2) real-time incident reporting; and (3) finding lost children in crowded areas. From the results, it appears that there was a substantial improvement of the solution from the A-Pilot to the B-Pilot, validating the final implementation and application of the DESMOS solution. However, full testing under large crowd conditions with high density of people (>1000 participants) has been postponed for the future, when health-related risks due to COVID-19 will be extinct.

In this work, we briefly present some background and state-of-the-art technologies regarding IoT sensors, devices, and localization. Then, we present our DESMOS design and implementation, followed by its testing, and validation in the two pilots. Finally, we present our results, followed by conclusions, limitations, and future steps, contributing to the realistic and practical adoption of these technologies, for the safety and privacy of visitors and tourists.

2. Background

Modern mobile phones (smartphones) come with a variety of built-in sensors with the capacity to detect environmental changes (temperature, humidity, lighting), the user's activity and location, health, and personal status through biometrics, etc. More specifically, modern mobile phones feature, as a standard:

- Ambient sensors (thermometer, barometer, photometer, camera, microphone) that measure environmental parameters such as *temperature*, *air pressure*, *brightness*, and *humidity*;
- Positioning systems (Global Navigation Satellite System—GNSS) that measure the physical position of the device in space;
- Motion sensors (accelerometer, gyroscope) that measure forces applied to the axis such as acceleration and rotation;
- Biometric sensors (heart rate, fingerprint) including sensors that measure a person's physiological characteristics.

Apart from smartphones, other wearable devices include smart bands or bracelets that act as external sensors—for instance, Xiaomi Mi Band smart bracelets are popular due to their small size and price [6]. These bracelets have built-in sensors (accelerometer, heart rate monitor, and vibration/alert mechanism), and are equipped with a Bluetooth Low Energy (BLE) protocol. In addition, they feature extended power autonomy, thus being able to operate for several days without the need for charging.

Usually, data collected from smart bands are pushed to smartphones using Bluetooth and then forwarded to the cloud. EveryGate [7] constitutes a flexible platform used to collect all the relevant data from interconnected devices (mobile, smart bands), providing high processing and storage capabilities. It is a patented technology [8] that allows the automatic retrieval and forwarding to the cloud of several parameters related to the operation and status (e.g., moving or not) of a node on which this technology is installed. Specifically, depending on the node to be used, the platform allows the collection of 160 parameters in real-time [7]. In addition, EveryGate scans the area for iBeacon tags and other on-screen sensors using Bluetooth 4.0. All the data are transmitted to the cloud, providing information on proximity, temperature, humidity, pressure, etc. or other important features such as the automatic monitoring of packets and their switching conditions. In addition, the platform offers protection by restricting access only to selected mobile applications, thus saving bandwidth and battery life.

2.1. Localization

In cases where localization through GPS is limited (i.e., indoor) or is not provided from the device (i.e., low-cost, expendable bracelets), it can also be applied according to transmitted wearable devices' signals such as Received Signal Strength Indicator (RSSI). In these cases, localization is accomplished through trilateration and filtering techniques that have been investigated thoroughly over the last years. Various research studies have proposed solutions to improve trilateration performance. Yang et al. [9] proposed a novel trilateration algorithm for indoor localization based on RSSI. The system they proposed utilizes Gaussian filtering to remove measurement noise from RSSI, and then, a least-square curve fitting method to estimate the transmit power and path loss exponent. The final position prediction is based on a novel trilateration method, using an error function that needs to be minimized. This method can deal with the different cases where the circles do not intersect at exactly one point. Finally, they apply a Bayesian filter to boost the accuracy of the final target's position. Experiments revealed that the method they proposed improves the final position prediction, reducing the error by less than 1 m, even in cases with no line of sight. Sasiwat et al. [10] developed a method to deal with RSSI variations due to human presence, applying adaptive filters to the final estimation of the distances between the target and the anchor nodes, followed by a simple trilateration method. The system achieved the reduction of the position estimation error by up to 46%. A weighted trilateration method is proposed in [11] along with a Kalman filter to improve the performance of the localization system. The weighted trilateration method considers multiple cases, in which the three circles do not intersect exactly on one point, improving the final localization, especially in small room scenarios.

The number of nodes has a crucial role in the localization's accuracy, since the more nodes utilized, the more information retrieved for the position estimation. Ismail et al. [12] provided a comparison of trilateration and multilateration, revealing that the number of nodes used for the position estimation, improves the localization accuracy. Moreover, Rahman et al. [13] proposed the utilization of more than three nodes for the final position estimation. They compared classic trilateration with iterative multilateration methods in various scenarios concluding that multiple nodes offer more robust localization.

2.2. Privacy and Security

The increasing deployment of IoT devices in almost every possible environment, revealed vulnerabilities regarding data privacy and security, since many of the data col-

lected are sensitive, allowing an attacker to tamper with them for various purposes. For example, data collected by smart grid meters can expose the users' habits, working hours, and way of living [14]. Moreover, data gathered by smartphones, allow the inference of users' location and their moving patterns [15]. Additionally, IoT devices have limited processing power, resulting in inefficiencies in the existing security protocols and privacy mechanisms. From now onwards, various solutions have been explored. For instance, the authors in [16] proposed a mechanism to protect privacy in medical healthcare systems using a lightweight homomorphism algorithm and an improved encryption algorithm based on DES. Additionally, the authors in [17] proposed an architecture based on onion networks for reporting crimes and incidents without exposing the user's identity. Finally, the authors in [18] proposed a protocol for anonymous authentication between IoT devices and operation centres to tackle the trustworthiness evaluation problem in IoT devices.

2.3. Crowdsourcing

The recent extensive use of smart mobile devices has attracted research focus in crowdsourcing. The concept of crowdsourcing deploys the mobile devices of people participating in an event or activity, to collect data. For example, authors in [19] have developed a smartphone application to monitor the noise levels within a city. Using these data, they construct a map that shows the level of noise pollution in the city. The authors in [20] built a framework to sense congestion inroads, using the sensors and onboard computer of a car.

2.4. The DESMOS Challenge

In the current paper, we present our attempt to integrate all these technologies to the DESMOS platform and validate and evaluate this integration in real critical situations (i.e., heart attacks, thieveries, fires, etc.) that often occur in overcrowded tourist destinations. This challenge entails progressing the state-of-the-art as follows:

1. By suggesting an innovative, knowledge-based solution for the diffusion of related information at different levels of the framework, promoting an agent-based computational model;
2. By deploying new techniques to ensure the anonymity of the information that users send with particular emphasis on tourism-related events;
3. By providing a solution on localization when GPS is limited (i.e., indoor) or is not provided at all, which is validated in real conditions.

3. Design and Implementation

The DESMOS solution is a smart infrastructure interconnecting (i) IoT nodes (smartphones and their built-in sensors, smart bands/bracelets, beacons), and applications (mobile apps, Everygate), over a cloud-based platform (open stack). This infrastructure is composed of several nodes that operate on the lower layer of the IoT architecture (Sensor Layer). The solution was implemented according to the Use Case-based, Incremental Development Model [21], following two iterations regarding testing and evaluation, and comprising the following steps (Figure 1):

1. Requirements: Tentative scenarios and use cases, user requirements analysis, and user satisfaction indicators;
2. Design and Modeling: Architecture, system requirements, and business processes (designed in Unified Modeling Language (UML), Business Process Notation (BPN), and Key Performance Indicators (KPIs));
3. Implementation (mobile applications, privacy and security, inference mechanisms and rules);
4. Integration, testing, and validation.

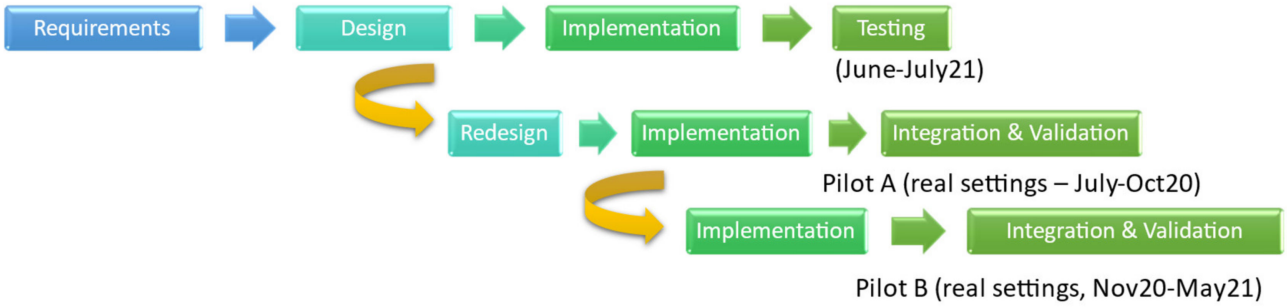

Figure 1. DESMOS development cycle.

3.1. Use Cases

The DESMOS solution was originally developed for two points of touristic interest in Trikala, Greece: (a) Mylos Matsopoulou (~25,000 m^2) that operates the whole year, but gets quite crowded during Christmas, due to the Theme Park "Mill of the Elves" (~40,000 visitors per day in 25,000 m^2, ~1,000,000 visitors in 40 days) (Figure 2), and (b) Trikala city center, which also gets overcrowded during Christmas.

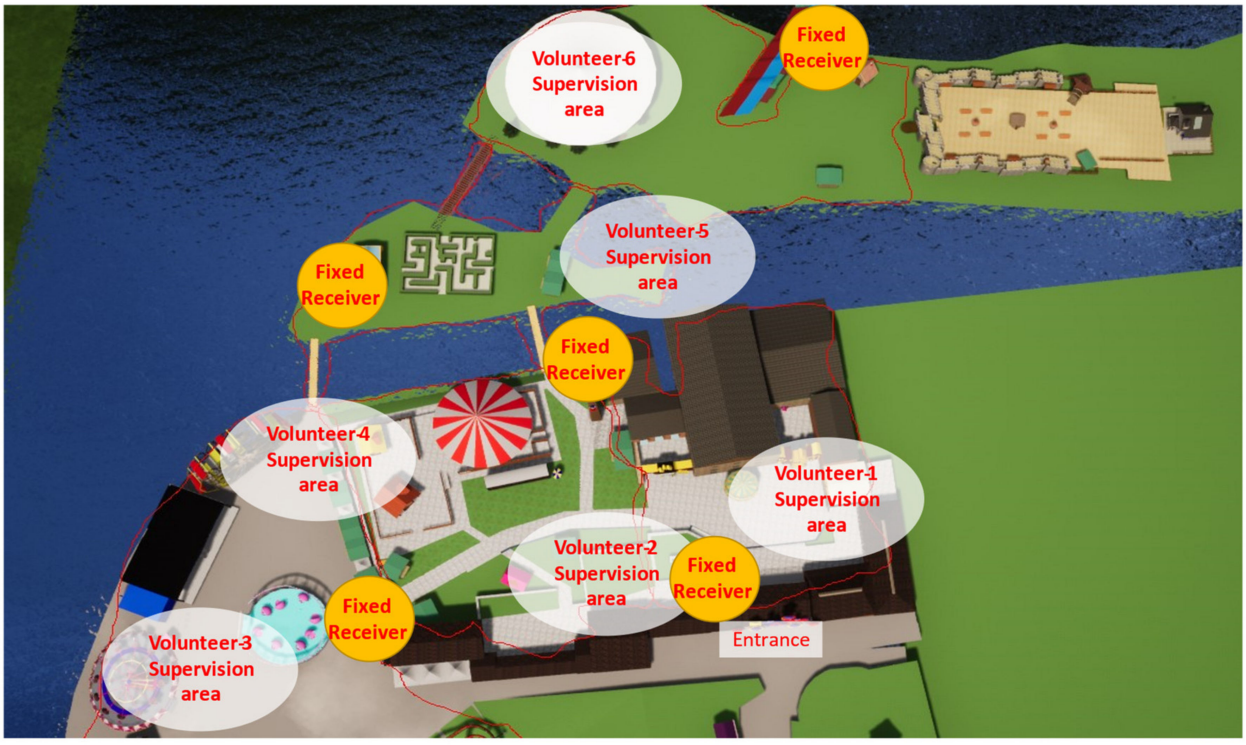

Figure 2. DESMOS installation in the Mylos Matsopoulou location. The yellow circles indicate the signal reception range of the fixed devices (approximately). The white ellipses are the possible locations of the volunteers together with the area they move and cover (red line).

From the requirements analysis, three use cases were conceived (Table 1), together with the Key Performance Indicators (KPIs) and User Acceptance Indicators (UAIs) that are analyzed in Section 4, to meet the project's operational, as well as non-operational requirements. UAIs are also derived from the UEQ scale [22] (see Section 4).

Table 1. DESMOS use cases.

Use Case	Title	Location	Purpose
Karpa	Emergency medical event treatment (CPR and AED)	Mill of Elves and City Centre	Alert the system during a cardiac or breathing emergency, and deliver all the critical information (patient's and closest defibrillator's location, find the closest volunteer), aiming at the provision of immediate CPR services and AED.
Sense	Real-time incident reporting	Mill of Elves and City Centre	Alert the system during various incidents (criminal acts, violence, theft, natural disasters, vandalism, etc.), providing all the critical information (location, descriptive media) through crowdsourcing.
ChildFinder	Locate the reported missing children	Mill of Elves	Alert the system and locate the children that have been lost in the Theme Park, providing all the critical information (child's description and last location) to staff and parents.

Use Case 1—Karpa: When a visitor needs medical assistance, he/she sends a request using the mobile application. The backend service locates the closest member flagged as a medical responder and notifies them. In parallel, the service locates the closest AED and lights its beacon (Figure 3).

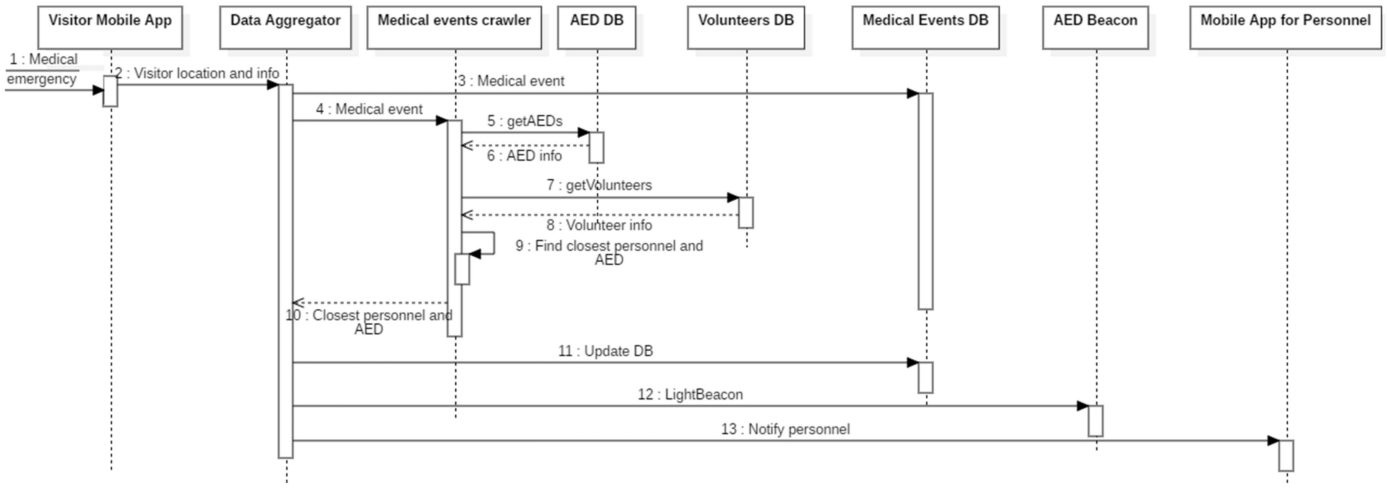

Figure 3. Use case 1—Karpa Sequence diagram.

Use Case 2—Sense: Visitors and Staff can report incidents that occur in the area. Through the backend service, the appropriate staff member is notified, while all the reported events can be monitored by the staff members (Figure 4).

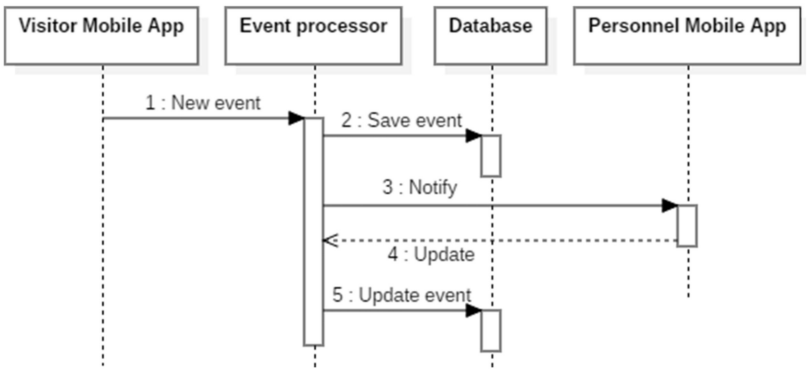

Figure 4. Use case 2—sense sequence diagram.

Use Case 3—ChildFinder: A parent notifies the service that her/his child is missing. The service estimates the child's location using data from the smart bracelet and sends a notification to the closest staff member (Figure 5).

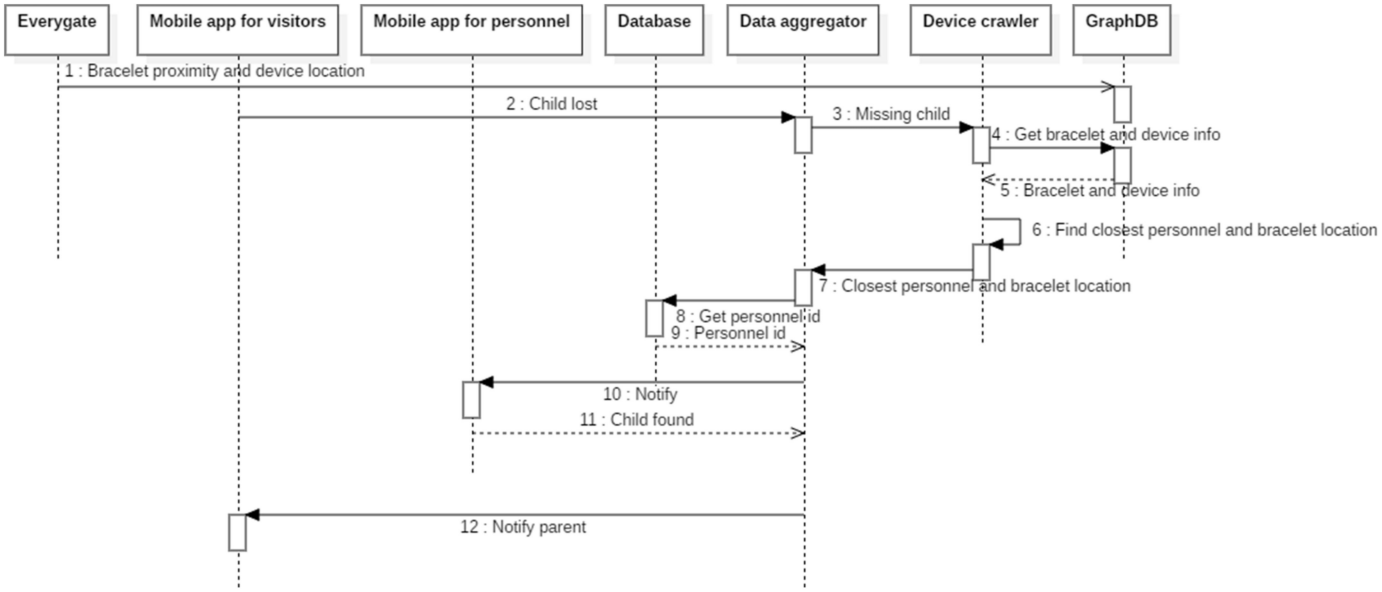

Figure 5. Use case 3—MylosChild sequence diagram.

3.2. System Architecture

The DESMOS architecture (originally published in [23], Figure 6) consists of three basic layers: (a) Hardware (mobile devices, sensors, actuators); (b) Middleware (interaction between edge components, i.e., sensors, actuators, as well as the interconnection between edge layers of DESMOS); and (c) Cloud (data storage, processing, and reporting). The cloud includes two databases: (i) For data processing; and (ii) for localization. As soon as the data arrive from the Middleware, they are saved in the first database and are also sent to the localization module. The localization module receives the coordinates and RSSI from EveryGate, then saves the values in its localization database. Finally, the data processing database is used to save all the events generated from the mobile devices deploying PostgreSQL.

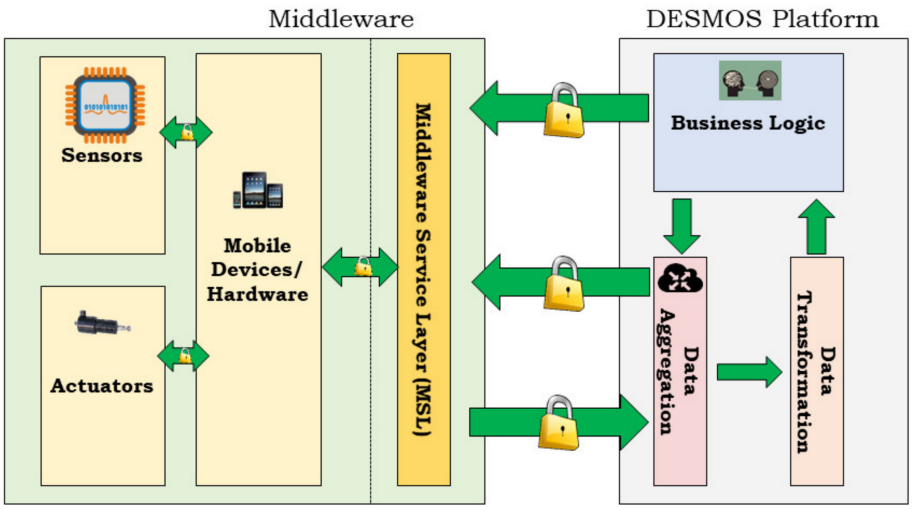

Figure 6. DESMOS architecture. Adapted with permission from ref. [23]. Copyright 2019, IEEE.

The Middleware consists of a REST API utilized for mobile devices to send data to the DESMOS Cloud. It also includes a push notification service, in which notifications from the DESMOS Cloud are pushed to mobile devices. Communication between the various models of the platform is performed using a pub/sub architecture. For data aggregation, the EveryGate platform was deployed to collect all the relevant data from the interconnected devices (smartphones, smart bands), providing high processing and storage capabilities. The EveryGate application is installed on both the DESMOS staff smartphones and the stationary nodes. In both cases, the application scans the area for bracelets (in particular, the MAC address), pushing the data collected higher into the DESMOS cloud platform for further processing and visualization. It also acquires the device's location using the best available provider (GNSS or networks). Via the MQTT protocol, these data are published to specific topics in a broker (one topic per device, in a specific subtopic location, scan results, etc.). The localization service in the DESMOS Cloud has subscribed to these topics, receiving data for processing. The components of DESMOS Cloud along with the Middleware, run on the cloud infrastructure of the laboratory, based on an OpenStack Infrastructure as a Service (IaaS) that deploys several Virtual Machines (VMs) to host the services required by DESMOS. These VMs are not exposed to the internet unless it is necessary to communicate with edge devices (e.g., smartphones).

3.3. Devices and Applications

In DESMOS, the smartphone camera and microphone were used for incident reporting by sending media files to the DESMOS platform, while the incident was taking place (i.e., fire alarm), together with the incident's location through the smartphones' GNSS positioning system (GPS, GLONASS, etc.). Regarding BLE signals, the Xiaomi Mi Band v2 and v3 smart bracelets were utilized due to their popularity and price, but mainly, following the test preliminary results that were performed, showing their efficient communication and performance with the EveryGate application. Additionally, both models were small enough and suitable for children of different ages. Moreover, their considerably reduced power consumption and capacity to operate for several days without charging were in agreement with crucial requirements from the Theme Park Administrators. Through the BLE communication advertising packet, the bracelets disseminate their MAC address to all the recipients (e.g., smartphones of mobile users or stationary stations) in an area. These recipients constantly scan to locate and record this information coming from the BLE's advertising packets, without having an established connection between the devices. BLE uses the Received Signal Strength Indicator (RSSI—signal strength of the received electromagnetic wave—to estimate the position of the subject of interest. During calibration, various RSSI measurements are taken from several different distances and locations and collected in a database [24].

Mobile Apps—DESMOS integrated system includes two different mobile applications: (i) For visitors; and (ii) for the Theme Park and Municipality personnel, including three main functionalities corresponding to the three use cases (Section 3.1, p7):

1. Report when a person alerts a medical emergency: The application provides the functionality to trigger the DESMOS System by entering information about a person's health condition and the location of the incident. This information is forwarded to the closest medical personnel.
2. Report incidents during a visit: All the tentative users (visitors, staff, administrators, volunteers) can easily report incidents (fire, acts of violence, fights, theft, vandalism, etc.) that happen near them, voluntarily contributing to the crowdsourcing mechanism of DESMOS. Easy tagging, location, and media sharing are provided from the app.
3. Report when a person (equipped with a bracelet) has gone missing: The application provides the functionality to pair the bracelet with a specific mobile device, as well as to enter the person's information and media, i.e., photos, videos. This information is saved to the device and forwarded to DESMOS only when the user triggers an alert.

Automated External Defibrillator (AED) Beacons—For sudden cardiac arrests, beacons (light bulbs) have been placed above the fixed points of external defibrillators (Figure 7). In case of an emergency, the light bulb of the closest, available (and charged) AED is automatically turned on, in order to be located and used either by the user that triggered the alert or from other experienced visitors close to the event, which critically reduces response times until trained medical professionals arrive in the location.

Figure 7. Beacons (light bulb) placed above external defibrillators.

The different hardware and software deployed per Use Case, are shown in Table 2, along with the framework used for implementing the software.

Table 2. DESMOS hardware and software per use case.

Devices and Applications	Use Cases			Purpose	Framework/Programming Language
	Karpa	Sense	ChildFinder		
BLE Bracelets (Xiaomi Mi Band v2 and v3)			✓	Tracking people's location	-
Mobile Applications for Staff	✓	✓	✓	Notification for missing children, medical requests, and environmental events	Flutter
Everygate Middleware Application	✓		✓	View and manage all the events (missing children, medical and environmental)/Toggle AED Beacons/Manage users	Native Android SDK
AED Beacon	✓			Scanning of BLE devices in the area (e.g., smart bracelets)	-
Data Aggregator	✓	✓	✓	Provide visual notification for the closest AED	Django (Python)
Event processor		✓		Collect events (missing children, medical events) from visitors, and send notifications in apps	Django (Python
Database (Events DB)	✓	✓	✓	Collect and process environmental events	PostgreSQL
Graph Database	✓		✓	Save information from data aggregator	GraphDB
Device Crawler			✓	Save the location of staff and bracelets	Java
Medical Events Crawler	✓			Calculate the bracelet's location for missing children	Java

3.4. Localization

The basic localization algorithm of the system utilizes the following workflow:

1. The received RSSI signal is fed into a Kalman filter, to remove the measurement's noise;
2. The output of the Kalman filter is transformed from RSSI to the distance of the target from each receiver;
3. The final localization is performed using the trilateration method with some modifications, to improve its robustness.

In detail, the received RSSI values from the different receivers are first processed by a Kalman filter. The latter is a recursive algorithm dealing with time series, containing statistical noise and other inaccuracies, and estimates a more accurate value of them based on the least-squares method [25]. In our case, the Kalman filter is used to eliminate the high noise levels of the RSSI measurements.

Assuming a static state, the transition matrix A_k is set to an identity matrix, and since there is no control, the control matrix B_k is set to zero. As the state is modeled directly, the observation matrix H_k is also set to identity. Therefore, the transition and observation model can be turned down to:

$$x_k = A_k x_{k-1} + B_k u_k + w_k = A_k x_{k-1} + w_k \quad (1)$$

$$z_k = H_k x_k + u_k = x_k + u_k \quad (2)$$

where w_k and u_k describe the Gaussian noise.

The prediction step of the Kalman Filter is then:

$$\hat{x}_{k|k-1} = \hat{x}_{k-1|k-1} \quad (3)$$

$$P_{k|k-1} = P_{k-1|k-1} + R_k \quad (4)$$

where R_k is the process noise that is set to a small value (0.008).

The Kalman gain is computed as:

$$K_k = P_{k|k-1}(P_{k-1|k-1}Q_k)^{-1} \quad (5)$$

where Q_k is the measurement noise that is set to the variance of the measurements.

The final update is:

$$\hat{x}_{k|k} = \hat{x}_{k|k-1} + K_k(\hat{x}_{k|k-1} - z_k) \quad (6)$$

$$P_{k|k} = (1 - K_k)P_{k|k-1} \quad (7)$$

After the Kalman filter prediction, the new estimated RSSI values are converted into distance using:

$$RSSI = -10n\log_{10}(d) + C \quad (8)$$

where d is the distance between the target and the receiver, n is the signal propagation exponent, and C is the RSSI value for the distance of one meter between the receiver and target.

After computing the distance of the target from each receiver, we can compute the target's position in terms of coordinates, using the trilateration method (Figure 8). Trilateration is a method of computing the position of a point based on its distance from three (or more) other known points. Given the fact that the A, B, and C points have coordinates (x1,y1), (x2,y2), (x3,y3) and distances d1,d2,d3 from the target point, the coordinates (x, y) of the target point can be computed using:

$$(x - x_i)^2 + (y - y_i)^2 = d_i^2, i = 1,2,3 \quad (9)$$

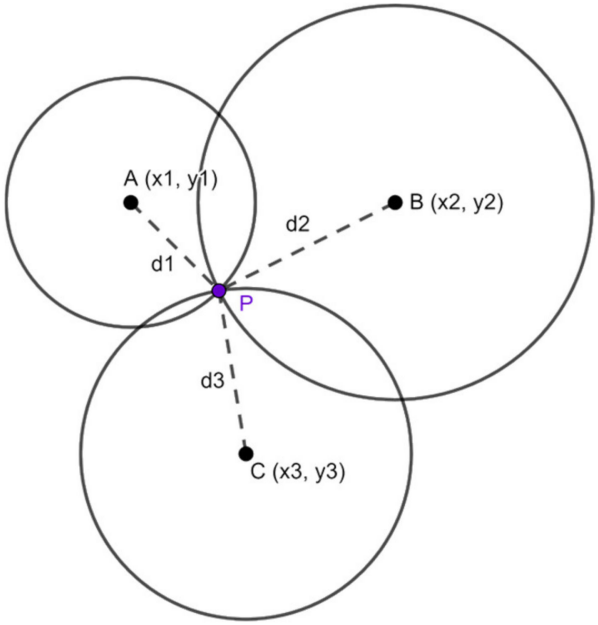

Figure 8. Trilateration method.

The basic algorithm of trilateration is due to the fact that the three circles intersect in exactly one point, which is the target point. This case is optimal and rarely occurs in real conditions. The RSSI noise, even after performing Kalman filtering, deviates the distances randomly resulting in circles that do not intercept to exactly one point. In this case, we must perform a modification of the classic trilateration method, which is the weighted trilateration proposed in [11].

In this specific work, we describe the different scenarios of the three circles intersecting in an area or not intersecting at all. For example, in the case where the circles intersect in an area (Figure 9), the weighted trilateration method is as follows. First, the centre MP of the triangle (P1, P2, P3) is computed using the equations:

$$MP_x = (P1_x + P2_x + P3_x)/3 \quad (10)$$

$$MP_y = (P1_y + P2_y + P3_y)/3 \quad (11)$$

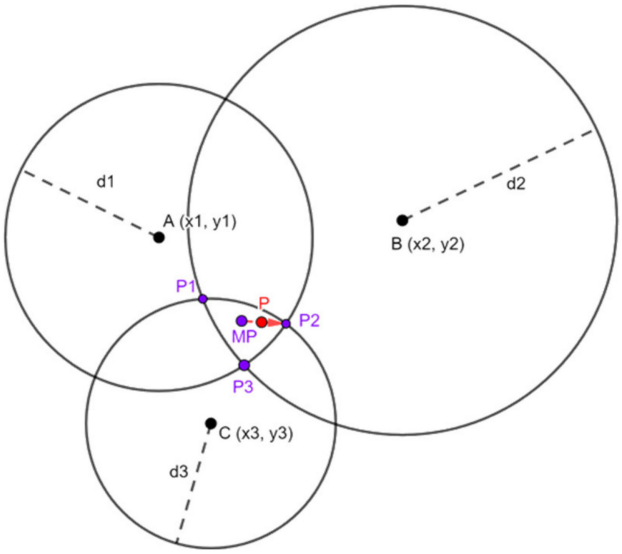

Figure 9. Weighted trilateration when the circles intersect in an area.

From the MP, we move towards the intersection of the two circles with the smaller radius, which is point P2. The movement is then determined by the weight of the equation:

$$w_{3\,1} = r_3/r_1 \tag{12}$$

This weight is the fraction of the two smaller radiuses. The coordinates of the final point P are then computed using the equations:

$$P_x = MP_x + (1 - w_{3\,1}) \times d \times \cos\theta \tag{13}$$

$$P_y = MP_y + (1 - w_{3\,1}) \times d \times \sin\theta \tag{14}$$

3.5. Semantic Integration and Reasoning

This section describes the semantic integration and reasoning framework, which was developed for semantically encoding and analyzing information relevant to the DESMOS application domain. The Knowledge Base Service (KBS) (Figure 10) is a key component of the system's architecture since it is the main interface to the DESMOS ontology. KBS is connected to a message broker that allows KBS to interact with other components, either by receiving incoming messages (e.g., sensor data that will be populated into the ontology) or by sending messages to other components of the system (e.g., reasoning results). KBS consists of two sub-components: (i) Knowledge Base Population (KBP) component that is responsible for integrating data to the ontology; and (ii) the Semantic Reasoning (SR) component that implements localization algorithms and rule-based reasoning techniques to discover connections between different entities of the ontology. Additionally, a localization component of the described framework is responsible for further analyzing sensor data coming from wearable devices (i.e., RSSI) and for enhancing the reasoning capabilities of the KBS.

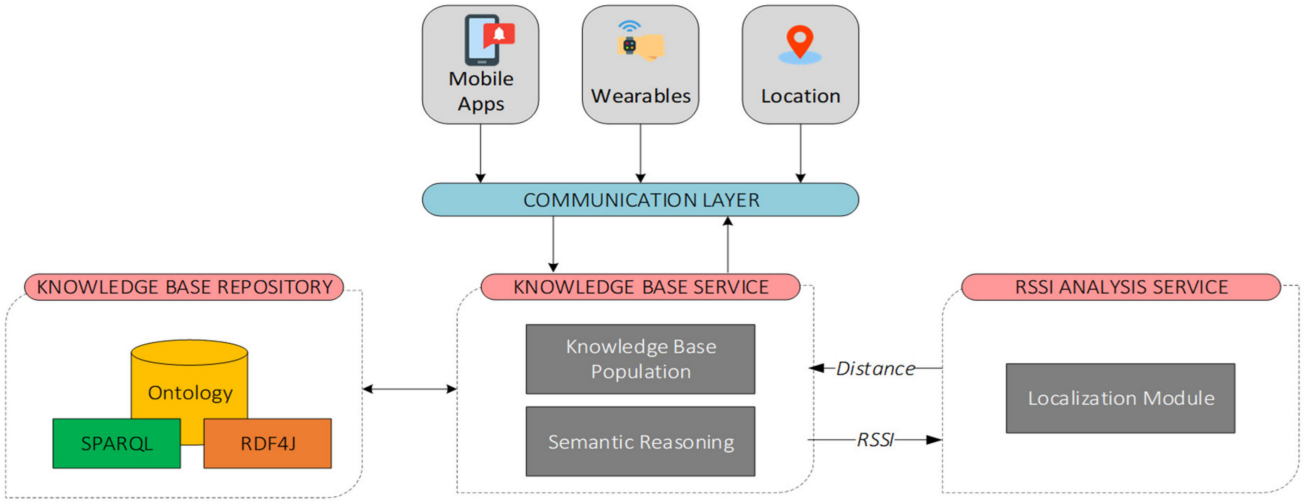

Figure 10. Semantic population and reasoning framework.

The DESMOS ontology (Figure 11) semantically represents key aspects of the DESMOS project: (a) Mobile and wearable devices; (b) sensor data such as location and RSSI; (c) visitor alerts; (d) localization results, as well as personnel assignments to critical incidents. The ontology is designed following a methodology for ontology design and construction [26] and implemented using Web Ontology Language (OWL2), which is based on existing ontologies such as SSN, SOSA, Geo (i.e., WGS84), and FOAF. The ontology is hosted by GraphDB, a highly efficient and robust Knowledge Base Repository built upon RDF4J—an open-source modular Java framework for working with RDF data that also supports SPARQL.

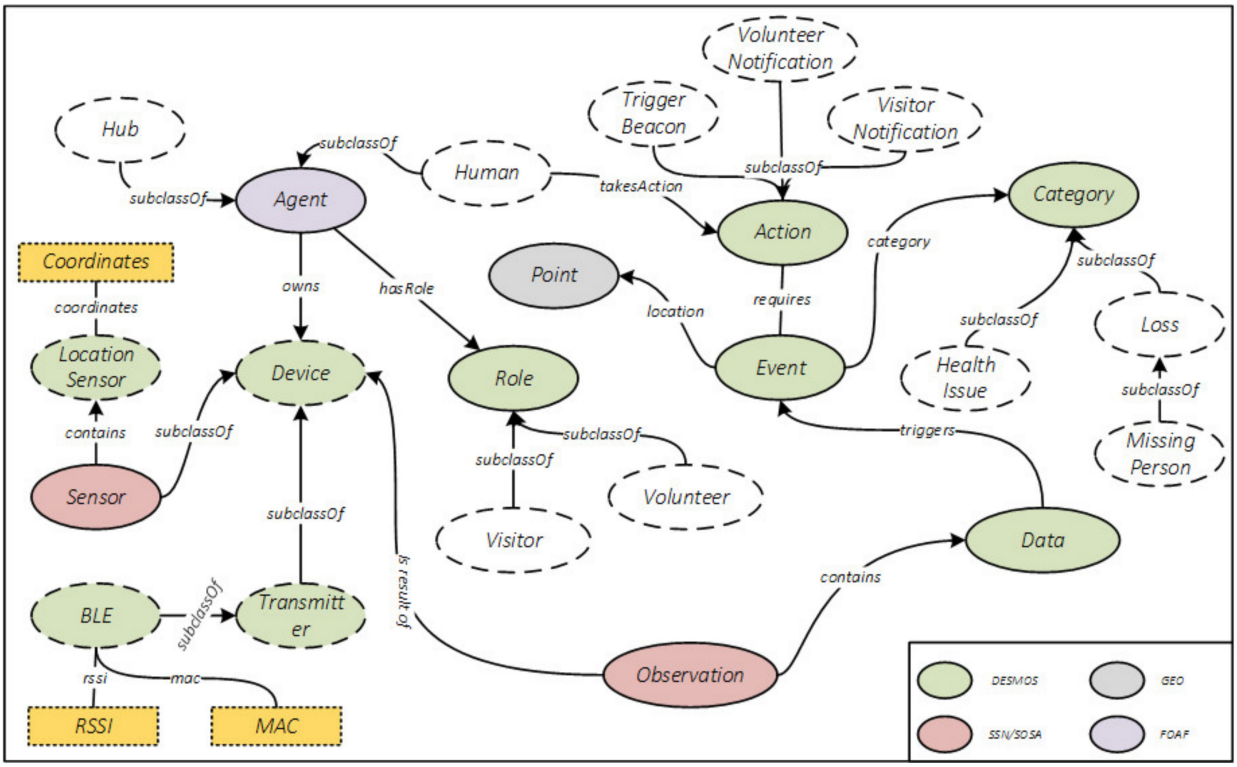

Figure 11. Abstract representation of existing ontologies with the DESMOS ontology [27].

In addition to monitoring the message broker and populating data into the ontology, KBS also implements a semantic reasoning mechanism to discover connections between ontology entities during various events such as a medical incident or a lost child alert. This mechanism is a combination of Java, Python, and a set of SPARQL queries. For instance, in a lost child use case, the system calculates the location of the child and then informs the nearest volunteer. More specifically, based on the latest RSSI signal broadcasted by the wearable device and received by volunteers or by fixed nodes, the system calculates the distance of the latest observers from the missing child, and finally calculates the location of the child using trilateration.

The following SPARQL (Figure 12) finds the three latest observers of the child, considering their observations on the child's wearable device.

```
SELECT ?imei (MAX(?time) as ?instanceTime) {
        ?s rdf:type sosa:Observation ;
                sosa:isObservedBy ?o ;
                desmos:isDataOf ?p ;
                sosa:resultTime ?time .
        ?vol sosa:hosts ?o ;
                desmos:imei ?imei .
        ?p desmos:mac ?mac .
        FILTER(?mac = STR(mac))
} GROUP BY ?imei
ORDER BY DESC(?instanceTime)
LIMIT 3
```

Figure 12. Code snippet for calculating the latest observers of a missing child.

3.6. Privacy

DESMOS adopted a security and privacy-by-design principle so that users' data are protected both at rest and while in transit. For the former, various mechanisms have been implemented, i.e., physical access to servers is restricted to only the necessary personnel for maintenance, virtual access to the servers is restricted only to the system administrator, allowing only specific ports, etc. For the latter, Transport Layer Security (TLSv1.3, RFC8446, https://datatracker.ietf.org/doc/html/rfc8446, (accessed on 24 June 2021)) is used in all the communications between the platform components, ensuring data integrity, confidentiality, and privacy. For API protection, the OAuth 2.0 standard is deployed, allowing only registered users to access information through the API. Users register to the platform under the supervision of the administrator, defining which user has access to which data. Additionally, uploading data to the API is possible only with the right application credentials, permitting only specific applications to upload data to the platform.

In compliance with the General Data Protection Regulation (GDPR, 2018 Reform of EU data protection rules. https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-changes_en.pdf, European Commission, accessed on 25 May 2018), no data are sent to the platform, unless the user sends them explicitly and willingly. Users have full control of the data sent each time, in all three use cases. Specifically, for the Karpa Use Case, users' location, together with their sensitive data, is only sent to the platform when they request help, without tracking in real-time. In the Sense Use Case, users decide if they wish to send the report, and at what time. Moreover, it is not possible to track the user who sent the report, unless they include this information. For the ChildFinder Use Case, a smart bracelet is matched with a child only when the parent asks for help to find his/her child. Finally, all the user's data can be deleted upon his/her request. The user must agree to the respective privacy policy before using the application.

In Table 3, we present how the DESMOS platform adopts the seven foundational principles of privacy-by-design [28].

Table 3. DESMOS adoption of the seven foundational principles of privacy-by-design.

Principle	DESMOS Implementation
Anticipate and prevent privacy breaches before they happen	Data encryption and Access Control
Privacy as the Default	Users decide if and when they share their information
Privacy Embedded into Design	Design the system concerning user's privacy
Full Functionality	No trade-offs were made in the functionality of the system and its security
End-to-End Security	Use of TLS
Visibility and Transparency	Development of well-tested technologies and informing users about what data is being processed and why
Respect for User Privacy	Design the system for user's privacy

The success of the above approaches can be confirmed from the results of the two pilots, where the system received mostly positive feedback, and the fact that many users are willing to pay for DESMOS services.

4. Results and Discussion

In line with the Big-Bang integration testing strategy [29], the DESMOS integrated system included two versions, requiring the simultaneous connection of all the standalone modules, and testing of the whole system, without performing integration tests—all the modules have been tested independently during development. The Big-Bang integration is quite effective, saving time in the integration process and testing, with the tradeoff that subsystems will operate with minimum bugs. The first integration took part during the DESMOS final testing phase (June–July 2020) and was evaluated during the A-Pilot

(July–October 2020). Errors and failures were adjusted during November 2020, and the DESMOS second integration was released during December 2020 (docker version), constituting the outcome of the project.

The evaluation process of DESMOS included the KPIs and UAIs described in Table 4 to meet the project's operational, as well as non-operational requirements. UAIs are derived from the UEQ scale [22], which deploys 26 pairs of contradictory questions, allowing the end-user to rate the User Experience of the different services provided by an application. The UEQ rating scale also offers a comparative analysis tool, using a database with results from other products, and consists of 20,190 users evaluating 452 different products. The questionnaires were both online and printed (handed in the pilot's sites), always following the GDPR rules.

Table 4. Key performance and user acceptance indicators.

	Requirements	Use Case		
		Karpa	**ChildFinder**	**Sense**
Functional (Key performance Indicators—KPIs)				
1.	The application starts successfully	☒	☒	☒
2.	The visitor creates an alert	☒	☒	☒
3.	The alert is forwarded to the platform	☒	☒	☒
4.	The alert is directed to the closest staff/volunteer (response time < 5 s)	☒	☒	☒
5.	Request status is updated by the staff	☒	☒	☒
6.	The child is located successfully on the map	□	☒	□
7.	Parents are notified to proceed to the correct meeting point	□	☒	□
Non-Functional (User Experience/User Interaction—UX/UI)				
1. 2. 3. 4.	Efficacy: Performs a task to a satisfactory or expected degree Effectiveness: Produces the desired output Usability/learnability: Easy to learn and use Sense of security/privacy: User's control of the application/protection of personal data	☒	☒	☒
5. 6. 7. 8. 9. 10.	Attractiveness: Users' look and feel of the application Perspicuity: Usability of the application Efficiency: Response time of the application Reliability: Users' security and control of the interaction Interest: Users' motivation Innovation: Originality and creativity of the application	☒	☒	☒

The initial schedule included the DESMOS evaluation in two phases: (a) Initial, during Spring 2020 (Trikala Food Festival, May 2020); and (b) final, during Christmas 2020 (Christmas Park at the Mill of Elves). Due to the COVID-19 pandemic, there was a 4-month time shift, while the project's two pilots were accomplished in line with the lifting of lockdown restrictions, each time. Moreover, although the DESMOS system was evaluated in real settings, both pilots were never tested in overcrowded areas. The final evaluation was accomplished in three different phases (Table 5):

- Testing phase (Alpha Testing, June 2020, 1 month): During this phase, standalone components were tested and evaluated, obtaining responses for improvements, according to the system requirements and KPIs, before evaluating the system in a wider community and real settings. This phase included tests carried out by both individuals and groups of experts, in the partner's locations –Athens (UNIWA, iTrack), Thessaloniki (CERTH), Trikala (e-Trikala)—as well as during technical and plenary meetings in Trikala (May 2019, December 2019, July 2020). The finalized components were

integrated into the first version of the DESMOS integrated platform (initial) that fed the first pilot (A-Pilot) of the project.

- A-Pilot (July–October 2020, 4 months): In the A-Pilot, the first integrated system was evaluated in real settings in Trikala City Center and the Mill of Elves, involving 99 participants (visitors, volunteers, staff). After evaluating the A-Pilot results, the second version of the DESMOS integrated platform was deployed.
- B-Pilot, (December 2020–May 2021, 6 months): In the B-Pilot, the final version of the DESMOS integrated system was evaluated in real settings in Trikala City Center and the Mill of Elves, involving 331 participants (visitors, volunteers, staff).

Table 5. DESMOS evaluation phases.

Phases	Testing (1 Month) 20 June	Pilot-A (4 Months) July–20 October	Pilot-B (6 Months) 20 December–21 May
Location	UNIWA, CERTH, Trikala City Centre, Mill of Elves	Trikala City Centre Mill of Elves	Trikala City Centre Mill of Elves
Purpose	Alpha Testing	KPIs, UAIs	
Participants	N/A	99 (56 males, 43 females)	331 (191 males, 140 females)
Number of Tests	N/A		181
Roles	Experts, Staff	Experts, Visitors, Volunteers, Staff	
Use Cases		All three Use Cases	
DESMOS solution	Standalone Components	First Integrated system	Second Integrated system

For demographics, post evaluation in total, and intention to use in the future, an additional questionnaire was provided by the project team. In Figure 13, descriptive diagrams are provided for both pilots.

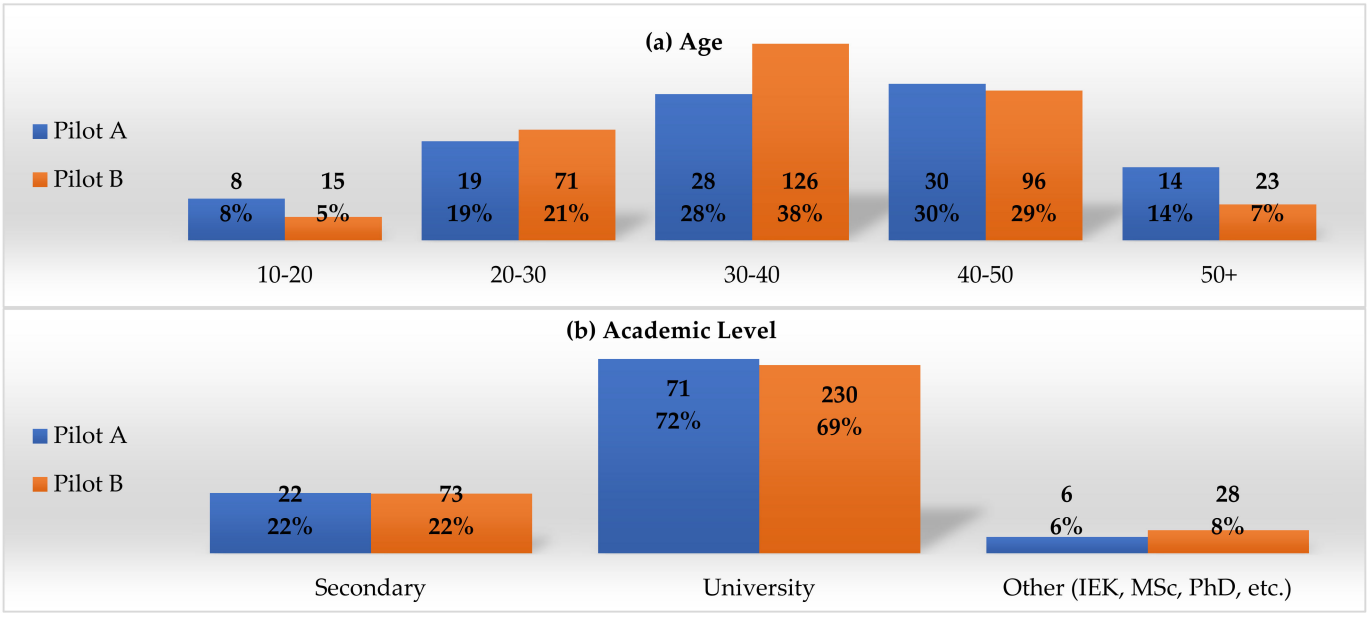

Figure 13. *Cont.*

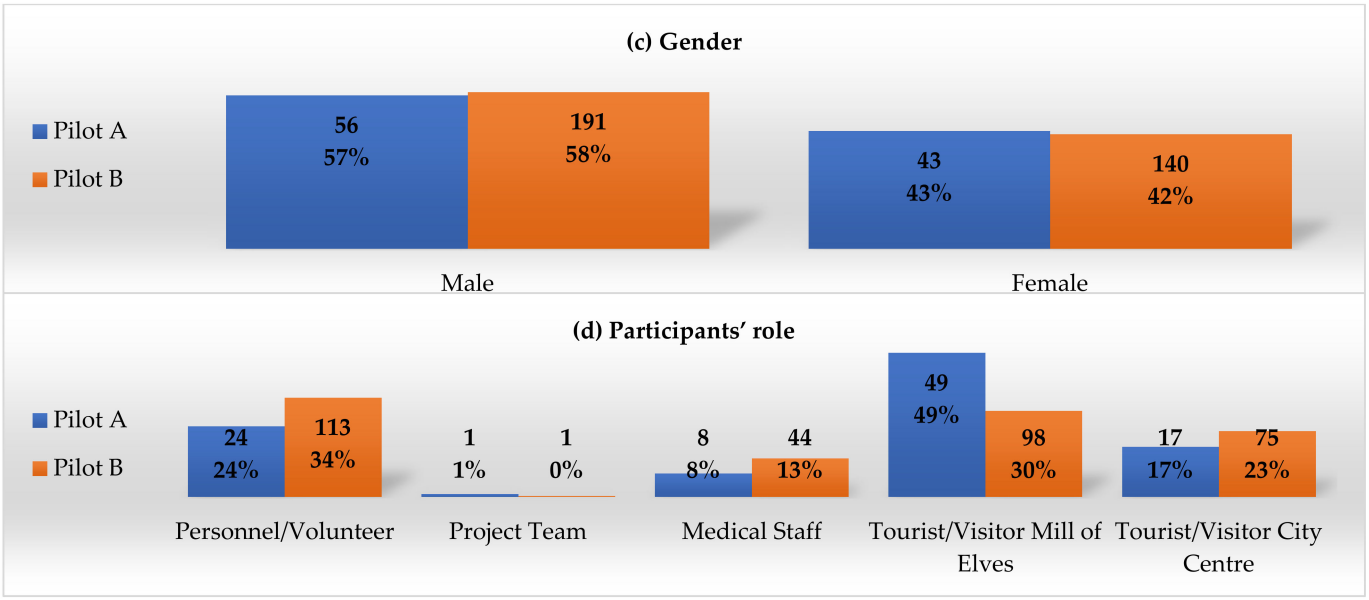

Figure 13. DESMOS A & B–Pilots demographics regarding (**a**) age, (**b**) academic level, (**c**) gender, and (**d**) participants' role, in absolute numbers and percentage.

4.1. Key Performance Indicators (KPIs)

The results regarding KPIs for both pilots are described in Table 6. In both pilots, the Sense Use Case was carried out with absolute success, since KPIs were technically more feasible. Similarly, in the Karpa Use Case, most requirements were met, with a high success rate. The response time was low for A-Pilot use cases Karpa (38%) and ChildFinder (33%). However, this was improved in the B-Pilot (83% and 82%, respectively). Similarly, the child location success rate was improved from the A-Pilot (28%) to the B-Pilot (77%). The improved success rates derive from: (i) The improvements that were applied in the second version of DESMOS after the A-Pilot's evaluation phase; and (ii) the increased number of volunteers and personnel that participated in the B-Phase.

Table 6. Results according to the key performance indicators (KPIs) set.

Functional Requirements ®	A-Pilot			B-Pilot		
	Karpa	**Sense**	**ChildFinder**	**Karpa**	**Sense**	**ChildFinder**
R1. The application starts successfully	23/42 55%	33/33 100%	20/40 50%	193/193 100%	74/74 100%	91/91 100%
R2. The visitor creates an alert	42/42 100%	33/33 100%	40/40 100%	193/193 100%	74/74 100%	91/91 100%
R3. The alert is forwarded to the platform	42/42 100%	33/33 100%	40/40 100%	193/193 100%	74/74 100%	91/91 100%
R4. The alert is directed to the closest staff/volunteer (response time <5 s)	16/42 38%	33/33 100%	13/40 33%	160/193 83%	74/74 100%	75/91 82%
R5. Request status is updated by the staff	23/42 55%	33/33 100%	20/40 50%	160/193 83%	74/74 100%	75/91 82%
R6. The child is located successfully on the map	N/A	N/A	11/40 28%	N/A	N/A	70/91 77%
R7. Parents are notified to proceed to the correct meeting point	N/A	N/A	20/40 50%	N/A	N/A	70/91 77%

4.2. User Acceptance (UX/UI)

Data collection was implemented with questionnaires, both online and in print. Responses were anonymized, while respondents signed a consent form, following the EU GDPR legislation (Regulation (EU) 2016/679 of the European Parliament) (EUR-Lex-

32016R0679-EN-EUR-Lex, https://eur-lex.europa.eu/eli/reg/2016/679/oj (accessed on 24 June 2021)).

The UEQ scale includes 26 contradictory questions evaluating six main criteria in UI/UX:

1. Attractiveness: Users' look and feel of the application;
2. Perspicuity: Usability of the application;
3. Efficiency: Response time of the application;
4. Dependability: Users' security and control of the interaction;
5. Stimulation: Users' motivation;
6. Novelty: Innovation and novelty of the application.

All the responses were provided in a 7-Likert grading system, represented in a [−3, +3] scale for further analysis. According to the distribution of average responses per UI/UX criterion:

- In A-Pilot, the DESMOS application is within the acceptable (orange) zone and the desirable (green) zone, in which the total percentage of negative responses is less than 11% (Figure 14a). In comparison with the average trendline derived from the UEQ database, *Efficiency, Stimulation, and Novelty* achieve higher scores than the rest of the criteria (Figure 15a). In line with the qualitative analysis, lower *Attractiveness, Perspicuity, and Efficiency* indicators highlight that, although the application is simple and easy-to-use, it should provide more information. *Dependability* lower values are connected to many respondents' requirements for a limited collection of personal data. In total, the DESMOS application is considered innovative, stimulative, simple, and efficient, but not so attractive or secure. Regarding effectiveness, many respondents highlighted the application's incapacity to report more than one event in each submission or the direct alert of first respondents (national emergency center, police, fire brigade), especially in cases of emergency. Finally, regarding DESMOS sustainability, almost half of the respondents stated that they were willing to pay for DESMOS services (EUR 1–2 ->24%, EUR 2–3 ->25%, do not know ->27%).
- In B-Pilot, and after considering the A-Pilot evaluation results and feedback, the DESMOS application seems to move closer to the desirable (green) zone, with remarkable improvement in all the criteria, especially in *Attractiveness and Novelty* (Figure 14b). Higher scores in *Attractiveness*, *Perspicuity*, *Stimulation*, and *Novelty*, as well as in conjunction with the respondent's respective comments, reveal that the application is easy-to-use and easy-to-learn, novel, informative, and stimulating. However, efficiency and dependability still marginally exceed the levels of neutral performance. In line with the qualitative analysis, direct alerts from the first respondents also appeared in the B-Pilot's responses, together with the request for more rich-in information and an effective user interface. Comparing the DESMOS application to the UEQ scale average, DESMOS is in the "Average" zone, moving closer to the "Good" level (Figure 15b). Finally, regarding DESMOS sustainability, again close to half of the respondents stated that they were willing to pay for DESMOS services (EUR 1–2 ->31%, EUR 2–3 ->10%, do not know ->25%).

From the distribution of answers in both pilots (Figure 16a,b), it appears that the percentage of negative responses is less than 15%, in all the UEQ items, with the most negative responses referring to reliability. For the overall reliability of each one of the components of the questionnaire, the UEQ uses Guttman's Lambda-2 coefficient [30], an alternative to the well-known Cronbach's alpha. The coefficient's values were respectively 0.90 for attractiveness, 0.81 for perspicuity, 0.91 for efficiency, 0.79 for dependability, 0.87 for stimulation, and 0.87 for novelty (A-Pilot), which is the lower bound for the reliability of a scale. This means that most of the variance is due to the true scores and not due to errors. In addition, the coefficient's values were similar for the questionnaire of the B-Pilot.

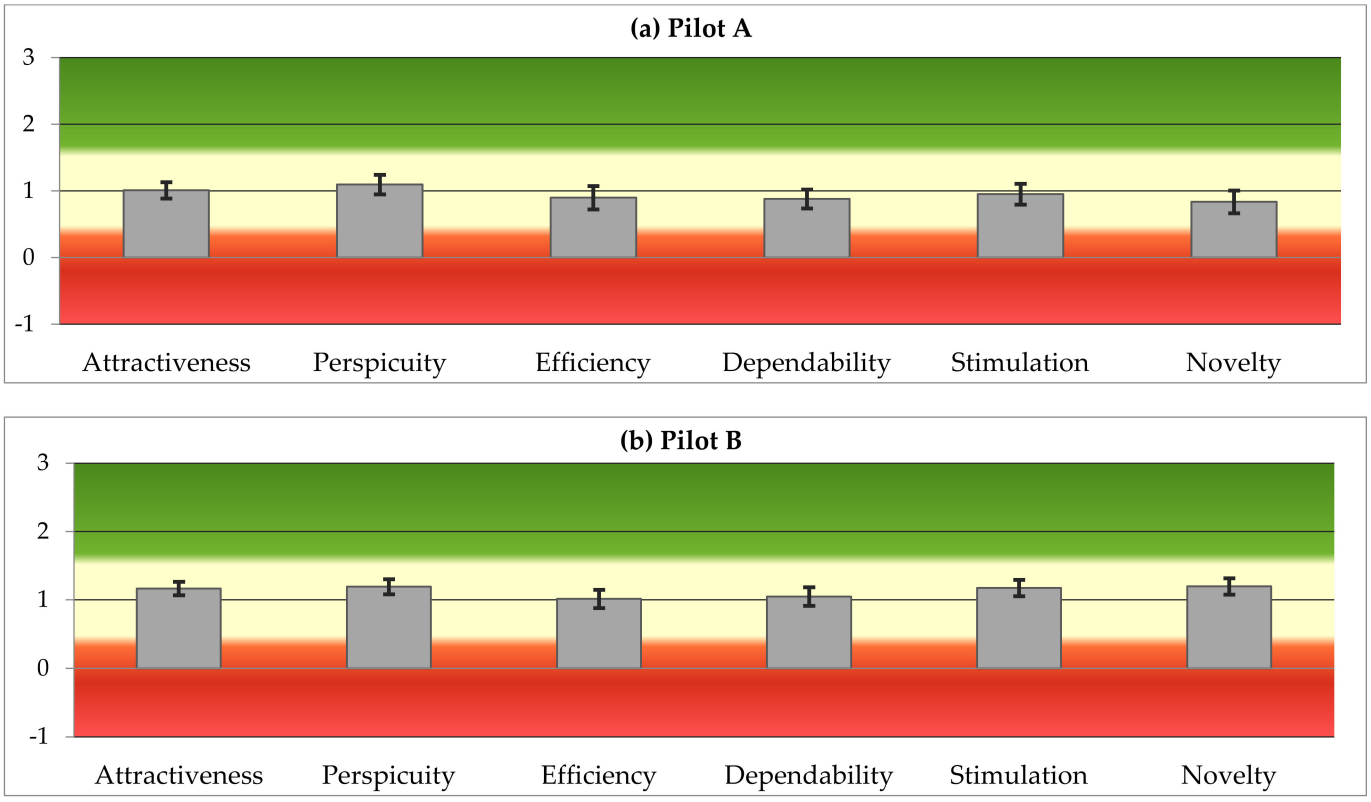

Figure 14. Variation of user responses per UI/UX topic in the A & B–Pilots (scale: −3 to 3).

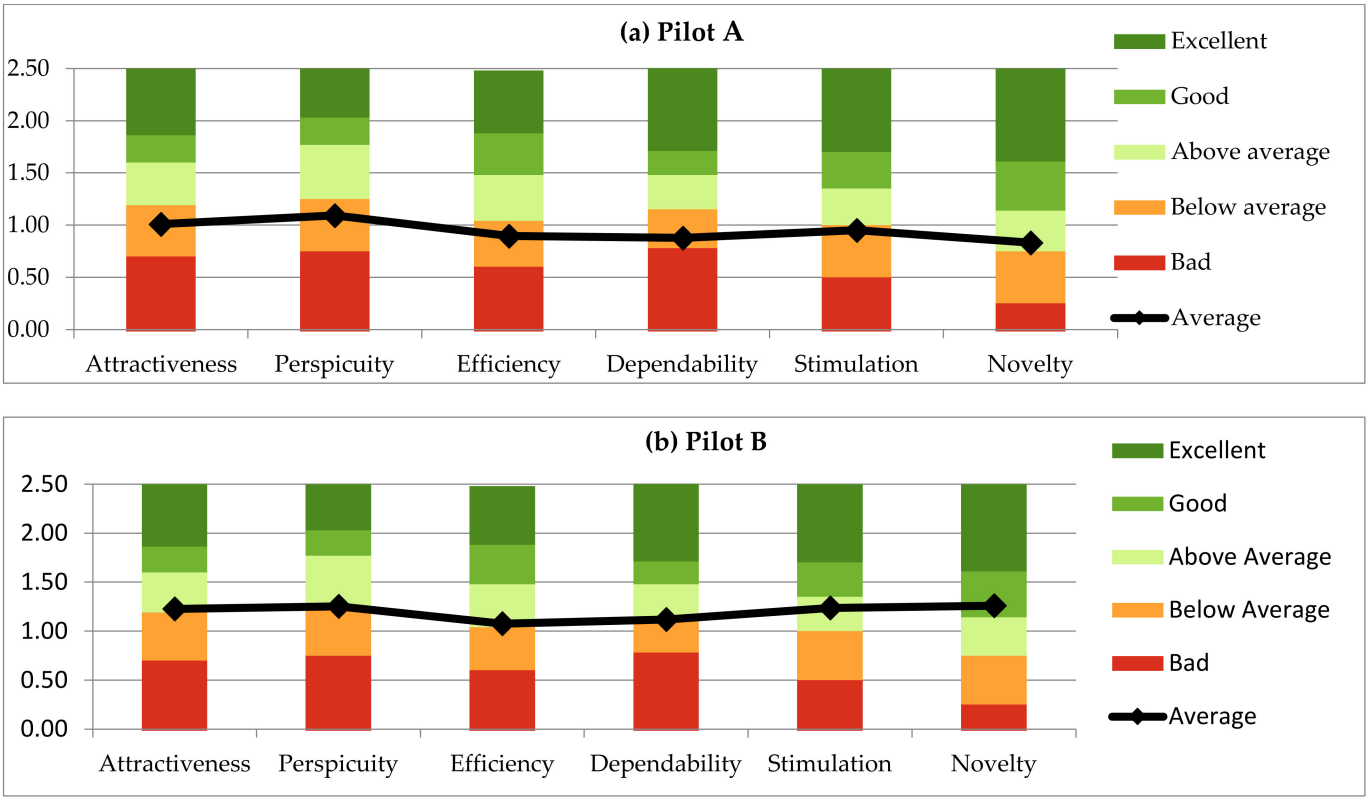

Figure 15. User responses per UI/UX topic in the A & B–Pilots compared to the UEC average (scale: −3 to 3).

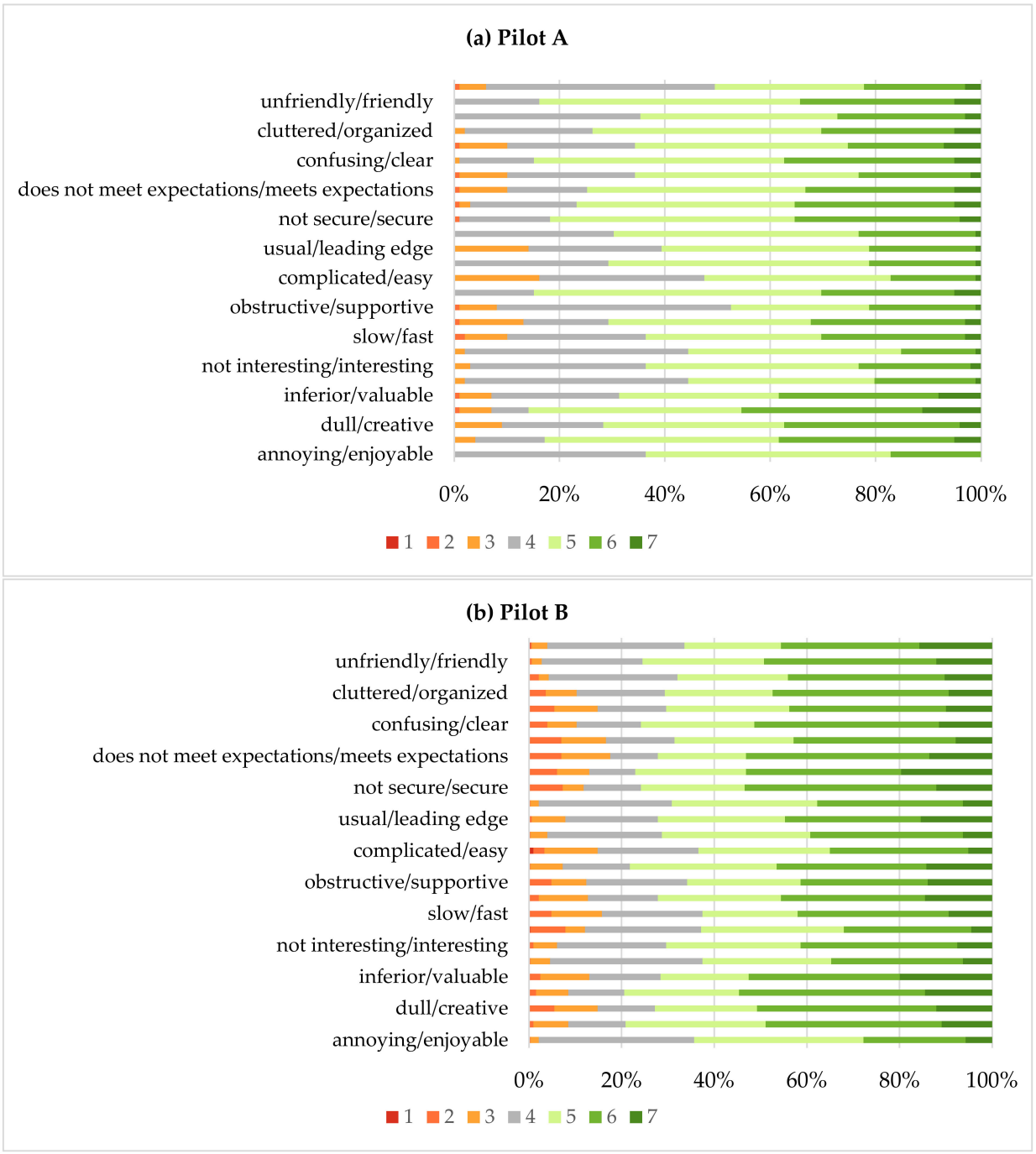

Figure 16. Distribution of answers per UEQ item in the A- and B -Pilots (scale 1–7).

5. Conclusions

In the current work, we presented the design, implementation, and evaluation of DESMOS, a novel ecosystem for the interconnection of smart things (mobiles, devices, beacons), applications, and infrastructures (Everygate, cloud), to provide a secure environment for visitors and tourists in crowded places. Despite the COVID-19 pandemic, two pilots validated the DESMOS integration, providing localization through BLE, and semantic reasoning in line with privacy and security-by-design. The DESMOS application is considered innovative, stimulative, simple, and efficient, but with some privacy issues (i.e., requires additional personal data), while minor improvements (i.e., direct connection with first respondents) could also raise the system's effectiveness. High scores in crowdsource KPIs reveal that the DESMOS holds the capacity to provide crowdsourcing

towards the collaborative reporting and analysis of situations, in order that humans can act as sensors and use devices to prevent or even mitigate critical situations. The latter, of course, requires experimentation in real crowded places, in order that crowdsourcing can operate with consistency. This also applies to localization, since the improvement from the A-Pilot to the B-pilot reveals that the number of nodes has a crucial role in the localization's accuracy—the more nodes utilized, the more information retrieved for the position estimation.

Future steps and open research issues include: (a) Testing under real conditions, with a high density of people, improvement of user interface expressiveness, and the application's effectiveness, in order to further raise the DESMOS accuracy, responsiveness, and privacy, to cope with critical situations with no failure tolerance; (b) deploying federated learning for visitors, which empowers the application's capacity to make predictions about the chance that a child gets lost, simply by entering the child's details in the app; (c) having a variety of sensors scattered in the site, in order that the motion patterns of the visitors can be inferred, thus, better managing the flow of people.

Author Contributions: Conceptualization and methodology, M.F., C.K., C.P., G.M., S.V. and I.K.; software, C.C., D.N. and D.G.K.; validation, C.K., L.G., M.F., A.T., C.P. and G.G.; formal analysis, C.K., L.G., A.T., M.F., C.P. and G.G.; investigation, resources and data curation, M.F., C.C., C.K., L.G., V.-R.X., D.N., A.T., D.G.K. and G.G.; writing—original draft preparation, M.F. and C.C.; writing—review and editing, all; supervision, project administration, funding acquisition, M.F., C.K., C.P., A.T., G.M., S.V. and I.K. All authors have read and agreed to the published version of the manuscript.

Funding: This research has been co-financed by the European Union and Greek national funds through the Operational Program Competitiveness, Entrepreneurship and Innovation, under the call RESEARCH-CREATE-INNOVATE (project code: T1EDK-03487).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data is contained within the article.

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

References

1. Qin, S.; Man, J.; Wang, X.; Li, C.; Dong, H.; Ge, X. Applying Big Data Analytics to Monitor Tourist Flow for the Scenic Area Operation Management. *Discret. Dyn. Nat. Soc.* **2019**, *2019*, 8239047. [CrossRef]
2. Ganzha, M.; Paprzycki, M.; Pawlowski, W.; Szmeja, P.; Wasielewska, K. Streaming semantic translations. In Proceedings of the 2017 21st International Conference on System Theory, Control and Computing (ICSTCC), Sinaia, Romania, 19–21 October 2017; pp. 1–8. [CrossRef]
3. Zhang, Z.; Jing, J.; Wang, X.; Choo, K.K.R.; Gupta, B.B. A crowdsourcing method for online social networks security assessment based on human-centric computing. *Hum. Cent. Comput. Inf. Sci.* **2020**, *10*, 23. [CrossRef]
4. Perera, C.; Zaslavsky, A.; Christen, P.; Georgakopoulos, D. Context Aware Computing for the Internet of Things: A Survey. *IEEE Commun. Surv. Tutor.* **2014**, *16*, 414–454. [CrossRef]
5. Kasnesis, P.; Toumanidis, L.; Kogias, D.; Patrikakis, C.Z.; Venieris, I.S. ASSIST: An agent-based SIoT simulator. In Proceedings of the 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT), Reston, VA, USA, 12–14 December 2016; pp. 353–358. [CrossRef]
6. IDC. IDC_ The Premier Global Market Intelligence Firm. [WWW Document]. Consumer Enthusiasm for Wearable Devices Drives the Market to 28.4% Growth in 2020. 2021. Available online: https://www.idc.com/getdoc.jsp?containerId=prUS47534521 (accessed on 16 June 2021).
7. iTrack. EveryGate—Enabling a Connected Planet [WWW Document]. iTrack Services Ltd. 2021. Available online: https://www.m2massociates.com/ (accessed on 7 September 2021).
8. Andritsopoulos, F. Method and System to Deliver Telematics Solutions. U.S. Patent Publication No. 20190122457, 2019.
9. Yang, B.; Guo, L.; Guo, R.; Zhao, M.; Zhao, T. A Novel Trilateration Algorithm for RSSI-Based Indoor Localization. *IEEE Sens. J.* **2016**, *20*, 8164–8172. [CrossRef]
10. Sasiwat, Y.; Buranapanichkit, D.; Chetpattananondh, K.; Sengchuai, K.; Jindapetch, N.; Booranawong, A. Human movement effects on the performance of the RSSI-based trilateration method: Adaptive filters for distance compensation. *J. Reliab. Intell. Environ.* **2020**, *6*, 67–78. [CrossRef]
11. Cantón Paterna, V.; Calveras Augé, A.; Paradells Aspas, J.; Pérez Bullones, M. A Bluetooth Low Energy Indoor Positioning System with Channel Diversity, Weighted Trilateration and Kalman Filtering. *Sensors* **2017**, *17*, 2927. [CrossRef] [PubMed]

12. Ismail, M.I.M.; Dzyauddin, R.A.; Samsul, S.; Azmi, N.A.; Yamada, Y.; Yakub, M.F.M.; Salleh, N.A.B.A. An RSSI-based Wireless Sensor Node Localisation using Trilateration and Multilateration Methods for Outdoor Environment. *arXiv* **2019**, arXiv:1912.07801.
13. Rahman, M.N.; Hanuranto, M.T.I.A.T.; Mayasari, S.T.M.T.R. Trilateration and iterative multilateration algorithm for localization schemes on Wireless Sensor Network. In Proceedings of the 2017 International Conference on Control, Electronics, Renewable Energy and Communications (ICCREC), Yogyakarta, Indonesia, 26–28 September 2017; pp. 88–92. [CrossRef]
14. Finster, S.; Baumgart, I. Privacy-aware smart metering: A survey. *IEEE Commun. Surv. Tutor.* **2014**, *16*, 1732–1745. [CrossRef]
15. Ning, Z.; Xia, F.; Ullah, N.; Kong, X.; Hu, X. Vehicular social networks: Enabling smart mobility. *IEEE Commun. Mag.* **2017**, *55*, 16–55. [CrossRef]
16. Gong, T.; Huang, H.; Li, P.; Zhang, K.; Jiang, H. A medical healthcare system for privacy protection based on IoT. In *Proceedings of the 2015 Seventh International Symposium on Parallel Architectures, Algorithms and Programming (PAAP), Nanjing, China, 12–14 December 2015*; IEEE: New York, NY, USA, 2015; pp. 217–222.
17. Katsadouros, E.; Chatzigeorgiou, C.; Feidakis, M.; Kogias, D.; Patrikakis, C.Z. Private Incident Reporting Using Onion Networks. In *IOT4SAFE@ ESWC*; CEUR Workshop Proceedings: Herakleion, Greece, 2020.
18. Xia, X.; Ji, S.; Vijayakumar, P.; Shen, J.; Rodrigues, J.J. An efficient anonymous authentication and key agreement scheme with privacy-preserving for smart cities. *Int. J. Distrib. Sens. Netw.* **2021**, *17*, 15501477211026804. [CrossRef]
19. Dutta, J.; Pramanick, P.; Roy, S. NoiseSense: Crowdsourced context aware sensing for real time noise pollution monitoring of the city. In *Proceedings of the 2017 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), Bhubaneswar, India, 17–20 December 2017*; IEEE: New York, NY, USA, 2017; pp. 1–6.
20. Olariu, S. Vehicular Crowdsourcing for Congestion Support in Smart Cities. *Smart Cities* **2021**, *4*, 662–685. [CrossRef]
21. Larman, C.; Basili, V.R. Iterative and incremental developments a brief history. *Computer* **2003**, *36*, 47–56. [CrossRef]
22. Schrepp, M.; Hinderks, A.; Thomaschewski, J. Design and Evaluation of a Short Version of the User Experience Questionnaire (UEQ-S). *Int. J. Interact. Multimed. Artif. Intell.* **2017**, *4*, 103. [CrossRef]
23. Chatzimichail, A.; Chatzigeorgiou, C.; Andritsopoulos, F.; Karaberi, C.; Meditskos, G.; Kasnesis, P.; Kogias, D.G.; Gorgogetas, G.; Tsanousa, A.; Vrochidis, S.; et al. Smart Interconnected Infrastructure for Security and Safety in Public Places. In Proceedings of the 2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS), Santorini, Greece, 29–31 May 2019; pp. 297–303. [CrossRef]
24. Chatzimichail, A.; Tsanousa, A.; Meditskos, G.; Vrochidis, S.; Kompatsiaris, I. RSSI Fingerprinting Techniques for Indoor Localization Datasets. In *Internet of Things, Infrastructures and Mobile Applications, Advances in Intelligent Systems and Computing*; Auer, M.E., Tsiatsos, T., Eds.; Springer International Publishing: Cham, Switzerland, 2019; pp. 468–479. [CrossRef]
25. Welch, G.; Bishop, G. *An Introduction to the Kalman Filter. ACM SIGGRAPH 2006 Courses*; Association for Computing Machinery: New York, NY, USA, 1995.
26. Bravo Contreras, M.C.; Hoyos Reyes, L.F.; Reyes Ortiz, J.A. Methodology for ontology design and construction. *Contaduría Y Adm.* **2019**, *64*, 134. [CrossRef]
27. Ntioudis, D.; Chatzimichail, A.; Meditskos, G.; Vrochidis, S.; Kompatsiaris, I. Ontology-based Reasoning for Critical Incidents in Public Events. In *IOT4SAFE@ ESWC*; CEUR Workshop Proceedings: Herakleion, Greece, 2020.
28. Eason, K.D. *Information Technology and Organisational Change*; CRC Press: Boca Raton, FL, USA, 1989. [CrossRef]
29. Cavoukian, A. *Privacy by Design: The 7 Foundational Principles*; Information and Privacy Commissioner of Ontario: Toronto, ON, Canada, 2009.
30. Guttman, L. A basis for analyzing test-retest reliability. *Psychometrika* **1945**, *10*, 255–282. [CrossRef] [PubMed]