The DESMOS Project

Subjects: Computer Science, Cybernetics
Contributor: Michalis Feidakis

“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.

Keywords: IoT ; smartphone ; bracelet ; localization ; crowdsourcing ; privacy

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.

2. Semantic Integration and Reasoning

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 1**) 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.

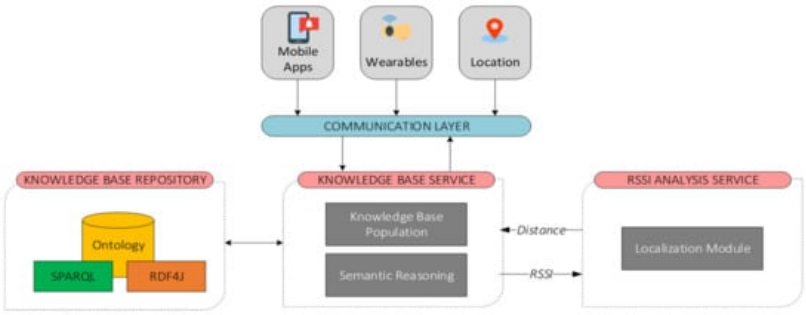

Figure 1. Semantic population and reasoning framework.

The DESMOS ontology (**Figure 2**) 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 [6] 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.

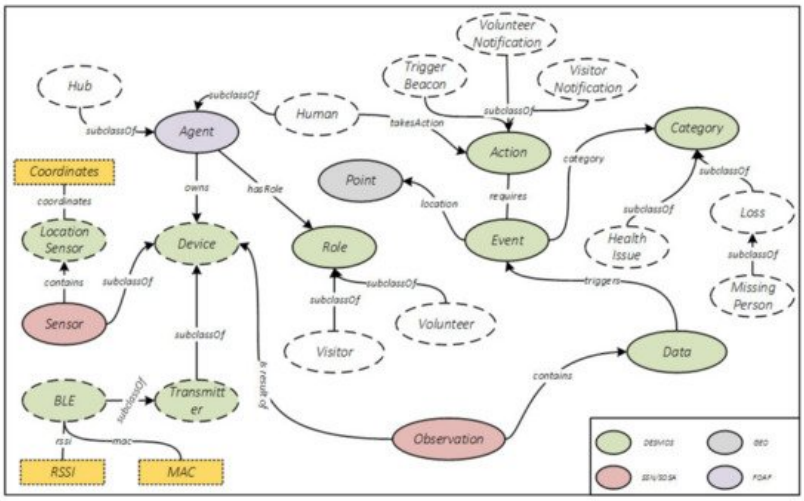

Figure 2. Abstract representation of existing ontologies with the DESMOS ontology [7].

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 3**) 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 3. Code snippet for calculating the latest observers of a missing child.

3. 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 1**, we present how the DESMOS platform adopts the seven foundational principles of privacy-by-design [8].

Table 1. 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**

Principle	DESMOS Implementation
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.

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.
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.
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.
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.
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.
6. Bravo Contreras, M.C.; Hoyos Reyes, L.F.; Reyes Ortiz, J.A. Methodology for ontology design and construction. Contaduría Y Adm. 2019, 64, 134.
7. Ntioudis, D.; Chatzimichail, A.; Meditskos, G.; Vrochidis, S.; Kompatsiaris, I. Ontology-based Reasoning for Critical Incidents in Public Events. In ESWC; CEUR Workshop Proceedings: Herakleion, Greece, 2020.
8. Eason, K.D. Information Technology and Organisational Change; CRC Press: Boca Raton, FL, USA, 1989.