Towards a privacy aware information system for emergency response

Alba Morales
The Open University
alba.morales-tirado@open.ac.uk

Enrico Daga
The Open University
enrico.daga@open.ac.uk

Enrico Motta
The Open University
enrico.motta@open.ac.uk

INTRODUCTION

Intelligent Systems in Smart Cities capture and exchange a large variety of information, for example, environmental data, localisation, biometric and personal data, health records, among others, in order to improve the quality of services.

On one hand, such systems could represent an important, lifesaving resource for public services aimed at addressing emergency situations (e.g. firefighters, police), by providing access to a large amount of diverse information. On the other hand, they are also a threat with respect to data protection and privacy when disclosing all sort of personal and sensitive information.

Since not all the information available can be used or helpful for handling the emergency we have the challenge of ensuring that the least possible amount of sensitive information is exchanged, therefore reducing the risk of unwanted disclosure and misuse. Thus, being aware and include a privacy-by-design approach when managing personal and sensitive data is essential in the context of emergency systems.

This work aims to analyse the privacy issues that Intelligent Systems face when sharing information with public services to attend emergency situations. By characterising these issues, we aim of informing the knowledge requirements for designing an Intelligent System that only allows valuable and helpful information to be exchanged, minimising personal and sensitive data disclosure.

BACKGROUND AND RELATED WORK

Smart Cities have put in place a set of different Intelligent Systems (IS) that are constantly monitoring, sharing and storing a heterogeneous range of information with the aim to help at improving and planning public services (e.g. transportation, energy and water consumption, environment, education, health, social), for the benefit of their citizens (van Zoonen, 2016). It is clear that the information collected by such systems is diverse and ranges from public data to private and sensitive data, according to its objective (Wang et al., 2015). For instance, systems that assist daily activities for elderly people by monitoring biometric data of the patient (Aleksandar Rodić et al. 2016), or applications that aim to help citizens with respiratory problems by monitoring air pollution and its location to suggest safe routes (Mateo Pla et al. 2016), video surveillance systems capturing and recording images/videos of citizens (Dufaux and Ebrahimi 2005), are some examples of IS that manage sensitive information. In addition, the information generated by Intelligent Systems is becoming essential for the development and function of Emergency Systems which rely on the detailed information given by the Smart Cities to improve citizen's safety and attend emergency situations (Garcia et al. 2018; Palmieri et al. 2016; Patsakis et al. 2015). However, data privacy breaches appear in the context of Smart Cities Systems, as mention before, mainly because these systems gather an exceptional volume of information that can compromise citizen's privacy (Martinez-Balleste et al. 2013). Therefore, in the context of emergency systems, providing access to this information represents an important resource (Chehade et al., 2018), but in the same way, this massive disclosure of information constitutes a threat with respect to data protection and privacy when this information contains personal and sensitive data.

APPROACH

As not all information available is important or helpful for emergency services, we have the challenge to assure the minimal possible amount of personal and sensitive information is shared. Thus, protecting people's privacy and preventing disclosure and misuse (Ding et al. 2016). However, since this information is heterogeneous and comes from many different sources, the need for one intelligent layer that can govern this diversity is imperative. In this context, semantic technologies can play a crucial role (d'Aquin et al. 2015), for example, in governing the multiplicity of data, processes, and policies involved (Daga et al. 2015, 2016). Our approach consists of developing an ontology for discriminating between sensitive and not sensitive information. Giving a person in danger the ontology should be able to automatically evaluate what is the information necessary to help this person and, at the same time, assuring that the minimal and sufficient information is disclosed, hence avoiding data privacy issues and providing emergency services/systems with helpful information.

RESULTS

To illustrate how privacy issues arise when Intelligent Systems share information with emergency systems, we selected a use case scenario (Srinivasan et al. 2016) to exemplify the case of a fire event. Next, with the purpose to learn how privacy issues are handled in a given emergency event (a fire event), we conducted an extensive survey in a large organisation: The Open University. The University and its Health & Safety Department provide a great amount and well structure documentation that is not limited only to fire events (for instance covers topics as First Aid, Accident, Incident and near-miss information and Display Screen Equipment (DSE)). Furthermore, it complies with Statutory Instruments and British Standards. Therefore, it constitutes a good, paradigmatic and concrete case study. At first, we analysed the relevant information and the procedures in case of fire events stated in the University's documentation, then we familiarised ourselves with the organisation's fire safety guidelines and regulations. Next, we identified the data privacy issues to later extract the requirements that a privacy-aware Intelligent System has to consider. Finally, we analysed the findings in the light of an Intelligent System solution. The list of competency questions in Table 1 is our first output of this work in progress poster that we want to present and discuss with the audience.

Number	Competency Questions
CQ1.	Is the IS able to differentiate between public and private information?
CQ2.	What information can be considered as public, private or sensitive information?
CQ3.	Is the IS able to understand the impact of sharing sensitive and non-sensitive information?
CQ4.	Is it possible for the IS to identify trusted services or systems?
CQ5.	Is the intelligent system able to discriminate what information could be necessary in order to attend the emergency?
CQ6.	What is the level of detail of information required to attend a specific emergency event?
CQ7.	Is the intelligent system able to discriminate what information could be sufficient in order to attend the emergency?
CQ8.	Is the intelligent system capable of assuring the minimality of the data shared in order to attend the emergency?
CQ9.	How to preserve data security of information stored after it was used by an emergency system?

Table 1 Competency questions

CONCLUSIONS AND FURTHER WORK

Undoubtedly, data privacy concerns are present in Intelligent Systems that collect, store and share any type of information. In emergency situations, the IS deal with a large amount of personal information, that once shared with emergency systems might derive in privacy disclosure. This work in progress poster aims at presenting the initial results towards a proposed approach of building an ontology capable of (i) discriminating between sensitive and not sensitive information, (ii) disclosing as minimal information as possible and equally important (iii) serving necessary and sufficient data to help the emergency.

REFERENCES

Aleksandar Rodić, Milica Vujović, Ilija Stevanović, and Miloš Jovanović. (2016). "Development of Human-Centered Social Robot with Embedded Personality for Elderly Care." *New Trends in Medical and Service Robots*, Mechanisms and Machine Science.

Chehade, S., Matta, N., Pothin, J.-B., and Cogranne, R. (2018). "Data Interpretation Support in Rescue Operations: Application for French Firefighters." *2018 IEEE/ACS 15th International Conference on Computer Systems and Applications (AICCSA)*, IEEE, Aqaba, Jordan, 1–6.

Daga, E., d'Aquin, M., Gangemi, A., and Motta, E. (2015). "Propagation of Policies in Rich Data Flows." *Proceedings of the Knowledge Capture Conference on ZZZ - K-CAP 2015*, ACM Press, Palisades, NY, USA, 1–8.

Daga, E., d'Aquin, M., Adamou, A., and Motta, E. (2016). "Addressing exploitability of Smart City data." *2016 IEEE International Smart Cities Conference (ISC2)*, IEEE, Trento, Italy, 1–6.

Ding, D., Conti, M., and Solanas, A. (2016). "A smart health application and its related privacy issues." *2016 Smart City Security and Privacy Workshop (SCSP-W)*, IEEE, Vienna, Austria, 1–5.

Dufaux, F., and Ebrahimi, T. (2005). "Smart video surveillance system preserving privacy." A. Said and J. G. Apostolopoulos, eds., San Jose, CA, 54.

d'Aquin, Mathieu; Adamou, Alessandro; Daga, Enrico; Liu, Shuangyan; Thomas, Keerthi and Motta, Enrico (2014). Dealing with diversity in a smart-city datahub. In: *Proceedings of the Fifth Workshop on Semantics for Smarter Cities*, CEUR Workshop Proceedings, CEUR-WS.org, pp. 68–82.

Garcia, L., Parra, L., Taha, M., and Lloret, J. (2018). "System for Detection of Emergency Situations in Smart City Environments Employing Smartphones." *2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, IEEE, Bangalore, 266–272.

Martinez-Balleste, A., Perez-martinez, P., and Solanas, A. (2013). "The pursuit of citizens' privacy: a privacy-aware smart city is possible." *IEEE Communications Magazine*, 51(6), 136–141.

Mateo Pla, M. A., Lemus-Zúñiga, L. G., Montañana, J.-M., Pons, J., and Garza, A. A. (2016). "A Review of Mobile Apps for Improving Quality of Life of Asthmatic and People with Allergies." *Innovation in Medicine and Healthcare 2015*, Y.-W. Chen, C. Torro, S. Tanaka, R. J. Howlett, and L. C. Jain, eds., Springer International Publishing, Cham, 51–64.

Palmieri, F., Ficco, M., Pardi, S., and Castiglione, A. (2016). "A cloud-based architecture for emergency management and first responders localization in smart city environments." *Computers & Electrical Engineering*, 56, 810–830.

Patsakis, C., Papageorgiou, A., Falcone, F., and Solanas, A. (2015). "s-health as a driver towards better emergency response systems in urban environments." *2015 IEEE International Symposium on Medical Measurements and Applications (MeMeA) Proceedings*, IEEE, Torino, Italy, 214–218.

Srinivasan, R., Mohan, A., and Srinivasan, P. (2016). "Privacy conscious architecture for improving emergency response in smart cities." *2016 Smart City Security and Privacy Workshop (SCSP-W)*, IEEE, Vienna, Austria, 1–5.

van Zoonen, L. (2016). "Privacy concerns in smart cities." *Government Information Quarterly*, 33(3), 472–480.

Wang, P., Ali, A., and Kelly, W. (2015). "Data security and threat modeling for smart city infrastructure." 2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC), IEEE, Shanghai, China, 1–6