The open area of user-centric privacy protection in the Internet of Things

Alexia Dini Kounoudes
adini-01@cs.ucy.ac.cy
University of Cyprus
Nicosia, Cyprus

Georgia M. Kapitsaki
gkapi@cs.ucy.ac.cy
University of Cyprus
Nicosia, Cyprus

ABSTRACT

The Internet of Things encounters the EU General Data Protection Regulation. The main objective is the protection of the user's privacy and personal data across the EU nations. Due to the vast amounts of data collected and shared across IoT devices, the privacy of the users has become a major issue in research, since users are not always aware about how their data are being collected and shared in IoT environments. Our goal in this work is to propose the steps needed for developing a user-centric privacy framework that complies with the GDPR requirements, while empowering the users to have control over their personal data.

CCS CONCEPTS

• **Security and privacy → Privacy protections**.

KEYWORDS

privacy protection, privacy framework, Internet of Things, GDPR

1 OUR APPROACH

For the purposes of this work we have studied the state-of-the-art on user privacy protection within the Internet of Things (IoT). We have identified the main challenges of the EU General Data Protection Regulation (GDPR) [1] according to [2] and based on them, we have devised a list of GDPR characteristics that user-centric privacy frameworks should satisfy in order to protect the user privacy and personal data, while providing a personalised user experience, in various IoT environments. Each characteristic in the our list has been mapped to the challenges and is considered in the privacy framework architecture we propose. The main contribution of this study is to suggest the necessary steps for the implementation of a user-centric IoT privacy framework (Figure 1) that enforces the user privacy preferences according to the GDPR requirements, based on the functionalities and methods proposed by different works.

The proposed steps illustrate how the users can be assisted with the right processes and tools which will empower them to have full control of their personal data. Examples of these steps include the specification of the privacy preferences of the user, either by keeping or altering the default privacy settings, or by defining them, which are then compared with the policy statement provided by the third party when making a data request. The comparison of the policies of the two parties will be used in the privacy risk analysis for the requested data and assist the framework to provide the necessary recommendations to the user, which can be either recommending optimal settings or data transformation, or both.

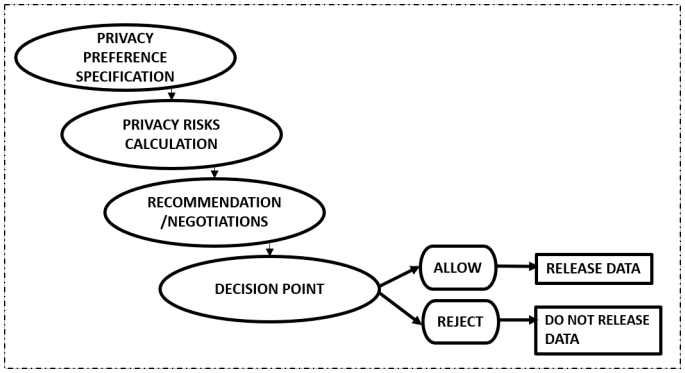

Figure 1: Example of the proposed steps

2 FUTURE WORK

We intend to implement the privacy framework in a smart water management system, where big data analytics and machine learning techniques will be used for the detection of data privacy vulnerabilities to enable the user to take decisions based on the findings. The framework will be integrated in an existing platform and evaluated using relevant mechanisms.

Another area of application is the Internet of Toys, a subset of the IoT, including all internet connected toys having the ability to record, store and share information about their child users. Context information, such as the user location, can allow a child predator to identify the location and trace back to the child. Therefore, it is very important to develop innovative technologies to enable the parents to monitor and control the children's data privacy. We plan to develop such technologies and integrate them in the privacy framework, assisting parents to secure their children's privacy.

REFERENCES

[1] 2018. 2018 reform of EU data protection rules. https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en. [Online; accessed 23-December-2018].
[2] Sandra Wachter. 2018. Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR. *Computer law & security review* 34, 3 (2018), 436–449.

womENcourage '19, September 16–18, 2019, Rome, Italy