A privacy-conscious Internet of Thing

Dipartimento di Ingegneria "Enzo Ferrari", Università di Modena e Reggio Emilia
marcello.missiroli@unimore.it

Abstract
This position paper explores the need of establishing an open and privacy-aware platform for a privacy-aware and user-centered data marketplace. A hypothetical scenario is described along with a straightforward solution and a novel, privacy-aware one.

1. Introduction

We commonly refer to the "Internet of things" [IoT] as a network of low-powered, embedded devices connected to the web. This paradigm, that integrates heterogeneous technologies and protocols, has a very large development potential: some state that up to 50 billions of "things" will be connected by 2020 [1], thus becoming even more important than the web we know today. While the concept itself is not new, dating back to 1999 [2], we are now experiencing strong interests both in academic and commercial world.

However, the IoT is more that a simple collection of "objects": tracking technologies, wired and wireless sensors, actuator networks, enhanced communication protocols, distributed intelligence are all – or will all be - part of the system [3], offering novel ways for the user to be reachable and to share and access data.

It is, however, still unclear what will the users have to pay, not only in monetary terms, but – in particular - in terms of privacy and control. We have already witnessed a similar situation in the mobile app arena: users carelessly install software that have a great deal of control on the handset, and pay little attention to device access, privacy settings and terms of use.

The introduction of billions of low-power, internet-enabled devices, each with its own privacy and security problems is likely to put the average user in a very weak position.

2. Possible scenario

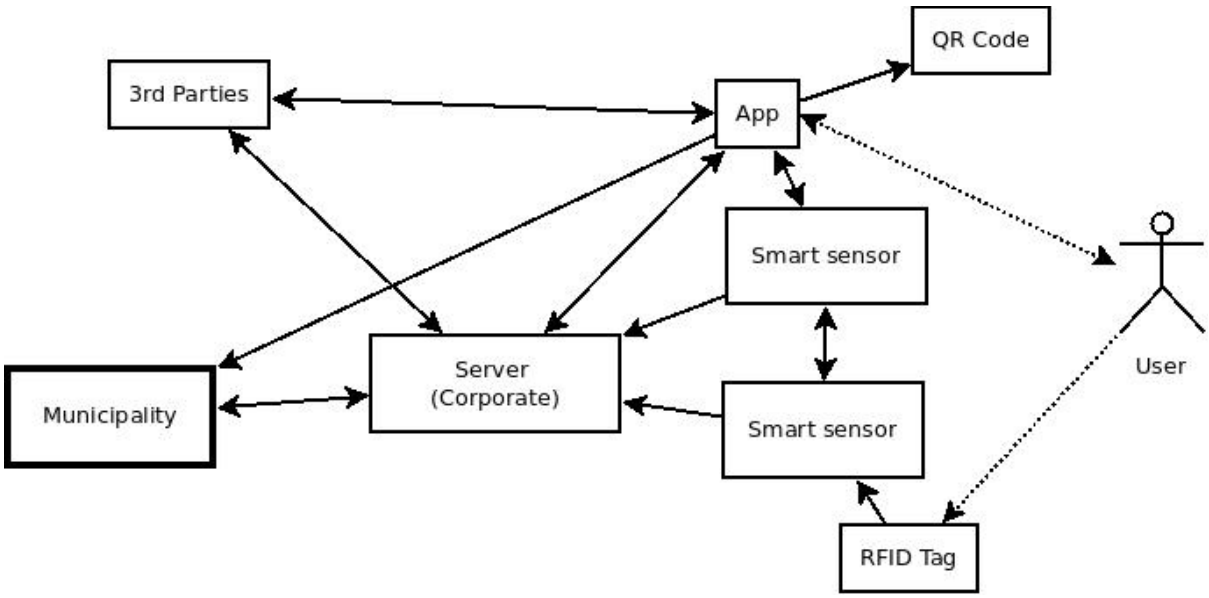

Figure 1: Straighforward solution

To clarify, let us consider the following hypothetical scenario, and see how it might be solved using common practices.
A city municipality wants to monitor the waste separation habits of its citizens (paper, glass, organic, etc.). Each family participating in the initiative collects wastes in separate containers, which are individually numbered and categorized by a QR code, RFID, NFC or similar tagging technology, with the help of a smartphone or an embedded device. When the container is full, the family takes the garbage to a collection point, where it is weighted and sent to the recycling plant. At this point, information is sent to the municipality, using a connected device (a smart sensor) located at the collection point. As a reward, a good-behaving family might receive a discount for waste disposal fees.
Using the currently established way of developing application, the municipality will probably

- develop a specialized app for the main smartphone platforms and distribute it via the usual app marketplaces.
- maintain a centralized server for collecting information.
- develop smart sensors and devices for waste weighting and data transmission.
- deploy devices on waste depos or other waste handling locations.

An implementation schematics is shown in Figure 1.

3. Problems

The above solution has the advantage of being straightforward and low-cost, but suffers from a number issues concerning the final user privacy:

- Data sent by the user is linked to a personal account; this may be exploited in order to track single users and infer their personal information and habits.
- The user sends a lot more information than he's required to – especially in case of automatic data transmission: in this case, the time of day of the delivery and the preferred location of disposal.
- The user has no idea of what will happen to his data: it might be used as stated, but it might also be re-used later or even or sold to unknown third parties, if any of the involved entity is malicious or simply honest-but-curious [4].
- The central server and the mobile application can be hacked, possibly exposing various kind of user information – even sensitive ones.
- This is a one-off solution: a different company requiring similar data must build everything again from scratch.

4. Position

While some say that the loss of privacy and control is inevitable [5] and a necessary trade-off for accessing advanced technologies, we argue that it doesn't have to be this way: it should be possible for user to offer sensor data, device related access and services without relinquishing unnecessary information.
The proposed solution is to create a common platform, that will put the user back in control and with a potential economic leverage with respect to the big information heavyweights. The platform should allow automated user data offer, search and interchange for any kind of data, but in particular for data collected by small connected device.
The platform should be based on the following two key elements:

1. **Privacy-aware architecture** [6]:
   this will ensure that data are not used in an unexpected way by the system.
2. **Complete transparency**:
   the system will use open protocols from the ground up, allowing easy integration and interoperability of various low-level communication protocols between devices and guaranteeing that the terms of services are upheld.

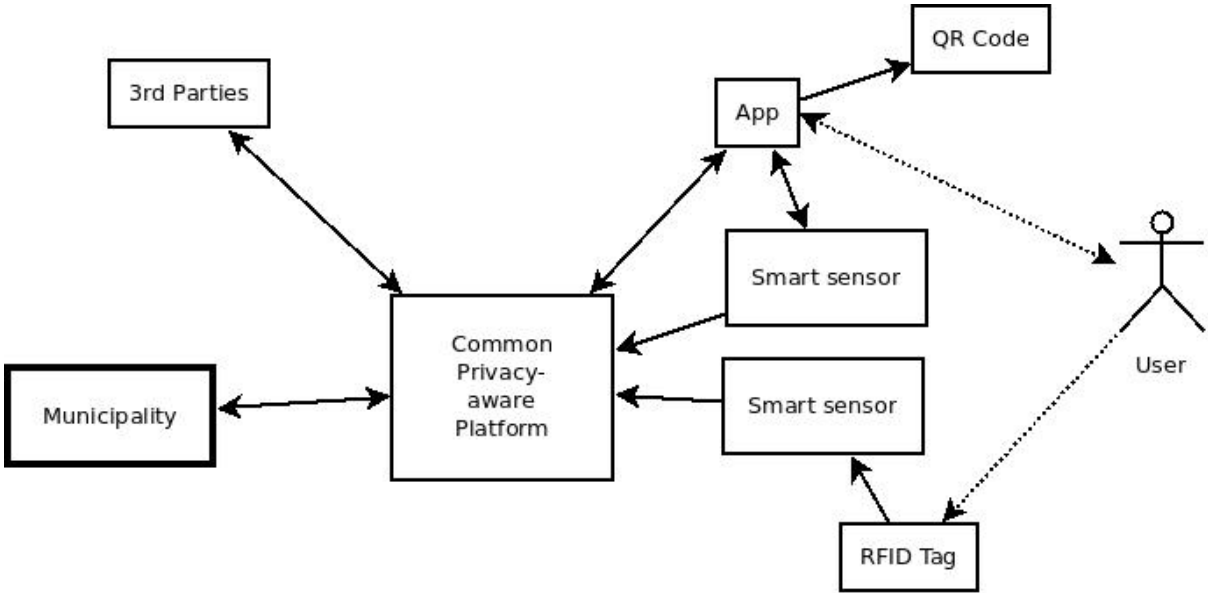

Figure 2: Privacy-aware solution

Applying this architectural model to the scenario described above would yield the following beneficial results:

- The municipality will receive only aggregated data of waste separation of each user.
- The user habits will not be tracked by the municipality or any other party.
- The municipality can bargain to obtain more precise data, if needed.
- User data will not be sent to third parties.
- The scheme could easily be applied to other municipalities by reusing the existing hardware and software products.

An implementation schematics is shown in Figure 2.

5. Future works

Our group is currently working on defining the basic elements and components of the platform, though still in the early stages. We are considering the integration of existing technologies and architectures, such as Daidalos [7], various reputation systems, BETaaS [8], and vehicle-based technologies.

References

1. Fehske, Albrecht, et al. "The global footprint of mobile communications: The ecological and economic perspective." *Communications Magazine, IEEE* 49.8 (2011): 55-62.
2. Ashton, Kevin. "That 'internet of things' thing." RFID Journal 22 (2009): 97-114.)
3. Atzori, Luigi, Antonio Iera, and Giacomo Morabito. "The internet of things: A survey." Computer networks 54.15 (2010): 2787-2805.
4. O. Goldreich, Basic Applications, vol. 2, 2004, Cambridge university press
5. Riederer, Christopher, et al. "For sale: your data: by: you." *Proceedings of the 10th ACM WORKSHOP on Hot Topics in Networks*. ACM, 2011.
6. Wicker, Stephen, and Robert Thomas. "A privacy-aware architecture for demand response systems." *System Sciences (HICSS), 2011 44th Hawaii International Conference on*. IEEE, 2011.
7. Aguiar, Rui L., et al. "Designing networks for the delivery of advanced flexible personal services: The Daidalos approach." *Proc. IST Mobile & Wireless Telecommunications Summit, Lyon* (2004).
8. Mingozzi, E., et al. "An open framework for accessing Things as a service." *Wireless Personal Multimedia Communications (WPMC), 2013 16th International Symposium on*. IEEE, 2013.
9. CRIS - Interdepartemental Research Center on Security and Safety, [Online] http://cris.unimore.it/en

Marcello Missiroli is Ph. D. candidate at the University of Modena and Reggio Emilia. His main research interests are in privacy and security field. He is part of CRIS (Interdepartemental Research Center on Security and Safety [9]), a permanent workshop focusing on Computer Science Security

within the Engineering Faculty “Enzo Ferrari” of the University of Modena and Reggio Emilia. He has only recently returned to the academic research, after serving a long period as CS teacher in technical schools.