Future Generation Computer Systems 56 (2016) 701–718

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

A comprehensive approach to privacy in the cloud-based Internet of Things☆

Martin Henze [a,*], Lars Hermerschmidt [c], Daniel Kerpen [b], Roger Häußling [b], Bernhard Rumpe [c], Klaus Wehrle [a]

[a] Communication and Distributed Systems, RWTH Aachen University, Germany
[b] Sociology of Technology and Organization, RWTH Aachen University, Germany
[c] Software Engineering, RWTH Aachen University, Germany

HIGHLIGHTS

- Observation: Adoption of cloud-based IoT is hindered by severe privacy concerns.
- We protect potentially sensitive data before it is uploaded to the cloud.
- We support service developers in developing privacy functionality for a service.
- We shift decisions about privacy from developers and providers to users.
- We provide users with a transparent and adaptable interface for configuring privacy.

ARTICLE INFO

Article history:
Received 15 November 2014
Received in revised form
15 June 2015
Accepted 12 September 2015
Available online 25 September 2015

Keywords:
Privacy
Cloud computing
Internet of Things
Model-driven development
User acceptance

ABSTRACT

In the near future, the Internet of Things is expected to penetrate all aspects of the physical world, including homes and urban spaces. In order to handle the massive amount of data that becomes collectible and to offer services on top of this data, the most convincing solution is the federation of the Internet of Things and cloud computing. Yet, the wide adoption of this promising vision, especially for application areas such as pervasive health care, assisted living, and smart cities, is hindered by severe privacy concerns of the individual users. Hence, user acceptance is a critical factor to turn this vision into reality.

To address this critical factor and thus realize the cloud-based Internet of Things for a variety of different application areas, we present our comprehensive approach to privacy in this envisioned setting. We allow an individual user to enforce all her privacy requirements before any sensitive data is uploaded to the cloud, enable developers of cloud services to integrate privacy functionality already into the development process of cloud services, and offer users a transparent and adaptable interface for configuring their privacy requirements.

1. Introduction

The proliferation of the Internet of Things (IoT), which enables the world wide interconnection of an incredible large amount of smart things, allows to effectively realize systems that significantly improve everyday's life, ranging from pervasive health care and assisted living to smart cities [1,2]. However, these smart devices often suffer from extremely constrained processing and storage resources, and a limited energy budget, as they are often powered by battery. In order to overcome these limitations, one of the most promising approaches is to interconnect the IoT with the cloud and thus benefit from the elastically scalable and always available resources provided by the cloud computing paradigm [3–9]. The cloud-based Internet of Things simplifies storage and processing of collected data, allows using the same data in multiple services, eases the combination of data from several users, and supports user mobility. At the same time it prevents information fragmentation over several databases.

☆ This is a significantly extended and rewritten paper based on the work *User-driven Privacy Enforcement for Cloud-based Services in the Internet of Things* by Henze et al. (2014) presented at the 2014 International Conference on Future Internet of Things and Cloud.

* Correspondence to: Informatik 4 (COMSYS), Ahornstr. 55, 52074 Aachen, Germany. Tel.: +49 241 80 21425.
E-mail address: henze@comsys.rwth-aachen.de (M. Henze).

http://dx.doi.org/10.1016/j.future.2015.09.016
0167-739X/

Although the necessary technologies for both, IoT and cloud computing, are readily available today, the interconnection of these two paradigms in application areas such as assisted living and public mobility assistance is gravely hindered by severe privacy concerns of individual users [2,10–12]. In order to develop such a system that is accepted and hence employed by a wide range of users, it is of up-most concern to ensure users' control over their data. Notably, an individual user might still want to rate, e.g., in the context of pervasive health care, health higher than privacy in case of an emergency. For this, it is crucial to anchor privacy aspects of *individual* users within the system.

However, cloud services are typically not developed solely for one specific user, but instead target a large group of heterogeneous customers [13]. Hence, it is infeasible to decide on all privacy aspects already during the development of a cloud service as privacy by design might suggest. Instead, in order for users to accept such a service, privacy choices must be left to the user. This, however, significantly increases the complexity of designing and developing cloud services and at the same time puts a tremendous burden on the user who often has no awareness of the (technical) consequences of her privacy choices. Therefore, we strive to encompass both domains, end-user's as well as service provider's perspective with our comprehensive understanding of cloud-based IoT services.

In this paper, we present UPECSI, our solution for **U**ser-driven **P**rivacy **E**nforcement for **C**loud-based **S**ervices in the **I**oT. UPECSI takes a comprehensive approach to privacy for the cloud-based IoT by providing an integrated solution for privacy enforcements that focuses on individual end-users and developers of cloud services at the same time. UPECSI consists of several technical components and organizational processes. More specifically, with UPECSI, we present the following core contributions: (i) individual, user-driven enforcement of privacy requirements already before any potentially sensitive data is handed over to the cloud, (ii) a novel technique for designing and implementing cloud-based services that integrates privacy functionality into the development process, and (iii) an easy to understand, flexible, and transparent approach for users of different privacy expertise to configure their individual privacy settings. These contributions of our comprehensive approach to privacy in the cloud-based IoT allow us to lay the foundation for bringing the IoT and cloud computing together in a user-accepted fashion.

This paper is structured as follows: In Section 2 we describe and discuss the application areas and network setting of our envisioned scenario. Based on this, we derive and present privacy concerns of end-users and privacy considerations of service providers that arise in a scenario like this in Section 3. We present important related work in Section 4. In Section 5, we formalize the challenges and requirements for realizing privacy-preserving cloud-based services for the IoT. To address these challenges and requirements, we present the main contribution of this paper, the design and implementation of UPECSI, in Section 6. We discuss in detail how this addresses and overcomes the identified challenges in Section 7. Finally, we conclude this paper in Section 8.

2. Scenario

The following section outlines our envisioned scenario. We address both the societal and, especially, technical point of view by discussing exemplary application areas from the contexts of assisted living and interactive mobility assistance in public spaces. Driven by these application areas, we derive and present an overview of the underlying network scenario of our system.

2.1. Application areas

Our two subsequently presented application areas focus around a 75-years-old widowed female retiree, who, besides tending her close relationships to family members and friends, appreciates having a wide range of options to live independently. In the first application area, *assisted living*, we consider this lady controlling her room/building automation related systems, e.g., screening mechanical, lighting, heating/ventilating/air conditioning (HVAC), and security systems along with monitoring her vital signs by a number of unobtrusive sensors in her apartment. These sensors deliver information to the cloud offering fast access to, for instance, family members and third parties such as medical personnel (e.g., doctors), health care providers (HCPs), or technical staff (e.g., building service engineers).

In the second application area, *public mobility assistance*, we envision this lady being comfortable with seamlessly taking an assisted living service with her on her portable and/or wearable devices. By doing so, this service takes a proactive role as a "personalized companion" by providing seamless mobility chains for aged users. Such a service enables people with limited mobility traveling independently by combining technical assistance systems (e.g., via smartphones and devices such as Google Glass) and public transportation: The entire route is covered from the starting point to the destination, including not only the public transport services (timetables of buses, trams, taxi services, etc.) but adding additional service value by including information on the local and regional conditions of the route because existing barriers (stairs, etc.) might be recorded, classified, and cataloged with their position data. Whereas today such services are already in development which aim primarily at assisting independent living of the elderly in their preferred environments [14,15], we deem it necessary to add additional benefit to such concepts by (i) integrating privacy enforcement (e.g., concerning mobility patterns, fingerprints, etc.), (ii) offering more functionality in terms of adaptable and transparent configurations (to the end-user as well as further stakeholders, e.g., including end-user's relatives and other affiliated persons, as well as other trusted third party actors), and, finally, (iii) generating higher user acceptance.

Our envisioned scenario is influenced by social forces such as aging (western) societies and the therefore increasing role of technology in supporting formal and informal care/assistance. Focusing on older life as well as current and, especially, future needs for health and social care, we have to consider the changing social structure of older life [16]. Departing from general demographic developments (e.g., increasing share of people aged 65 years or above in the total population and longer span of "older" life phases due to rising life expectancy), aging societies have to face inextricably linked pressing forces. On the one hand, they have to cope with economic frictions (expectations about the quality of health care systems stemming from certain standards of living vs. financial constraints and shortage of skilled labor in the public health services sector) as well as eminent societal processes on the other hand. In this context, some of the most important societal changes to be highlighted might be singularization (increasing number of the elderly un-/deliberately living alone with their families/relatives distributed over large geographical areas due to increased mobility in society), differentiation (e.g., not one common understanding but many individualistic approaches of how health and social care should be provided), and changing gender roles (due to "feminization of aging" indicating at the increasing number of women in old and, especially, very old age groups).

Hence, our overall scenario with its application areas serves as adequate example to derive design requirements for our system to be user-accepted and provides us with a promising evaluation setting by keeping in mind the differentiation and variability of old/very old age, i.e., including different age cohorts with a plurality of norms, consumer/consumption habits, and technology experiences/knowledge. However, our technical foundations are applicable to much broader contexts ranging from building management systems over intelligent transportation systems to smart manufacturing.