Behavior Monitoring application for Healthcare: Privacy Requirement Analysis

Lamya Abdullah[1,2] *

[1] Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU), Germany
[2] Uniscon GmbH, Germany

Abstract. Living in a smart environment is becoming a reality and a de-facto future life-style. Despite the luxurious purposes of smart homes in general, lots of applications are vital and life-saving, such as assistant living and healthcare applications. In this study, we are focusing on a behavior monitoring application for the purpose healthcare giving. A sensor network is deployed in the home, in order to collect data about functional abilities of fragile inhabitants. Data is processed by an activity recognition analysis to produce what is so-called activities of daily living (ADLs). Clinicians inquire and inspect daily behaviors history and trend of a subject to analyze recorded ADLs data, e.g. to detect behavior anomalies to support health diagnosis (e.g., cognitive impairments). Privacy concerns in smart home, in general, and healthcare applications, in particular, are inevitable. Service providers may work towards being compliant to the GDPR; however, it is challenging to balance and compromise the very demanding utility and privacy-preserving service. To do so, it is critically required to adopt the Privacy-by-Design (PbD) approach. Several surveys have been studying and collecting privacy threats, requirements and corresponding privacy preserving approaches in pervasive systems, in general. In this study, we aim to design a privacy-preserving architecture for behavior monitoring smart home service. This talk discusses a part of the initial phase of building the design. We run a comprehensive privacy analysis during the early phase of the traditional functional analysis. On the one hand, running privacy analysis enables the PbD approach at early stage. On the other hand, it qualifies validation of alternative designs, implementation and deployment options against privacy requirements.
The analysis includes, defining the main stakeholders (entities), data model, service modules, privacy threats at each module and levels of implementation and deployment, and a set of users privacy requirements associated with possible approaches.

* This work is supervised by Prof. Felix Freiling, and it is a joint work in collaboration with Prof. Claudio Bettini and Ph.D. Gabriele Civitarese, University of Milan.