Main objective and summary of the project

“The use of mobile and wireless technologies to support the achievement of health objectives (mHealth) has the potential to transform the face of health service delivery across the globe” [8]. All basic tasks in mHealth, i.e., data acquisition, collection, analysis, and presentation, handle sensitive private data. The amount and quality of data directly impacts the usefulness of the data analysis results for physicians, care takers, researchers, and family members. Missing privacy protection leads data subjects (e.g., patients) to not provide data or to provide data with low quality. Therefore, the goal of this project is to introduce "privacy by design" in mHealth through new research results to the benefit of all stakeholders in the value chain on these systems, i.e., data subjects, application developers, service providers and service users. This means to

- provide data subjects the requested level of privacy protection,
- relieve application developers from the burden of implementing privacy protection,
- minimize the costs for service providers that are introduced through privacy protection,
- take care that privacy protection does not hamper the data quality and by this the usefulness of the service for service users.

This project will be performed in close cooperation with the CESAR project (), which is concerned with the collection and mining of physiological sensor data to analyze health parameters related to Obstructive Sleep Apnea. We focus in this project on the use of Complex Event Processing (CEP) for real-time data analysis and build on our recent results on Device Communities [14]. Device Communities are formed by a set of networked devices and their users that share a well defined set of resources, like data and services, in a trustworthy overlay. To achieve the required form of privacy and to turn a device community into a Smart Community for data mining, we investigate in this project how to automatically extent queries from the application such that the privacy requirements are fulfilled. The core idea is to establish a collection of privacy protecting mechanisms (PPMs), like anynomization of data sources, k-anonymity, obfuscation, and aggregation of data from a single source over time or from multiple sources in a physical location. The PPMs shall be encapsulated such that they can be used as operators in CEP queries.

Project background and scientific basis.

Ubiquitous sensors and computing devices are today a reality and their number and different capabilities will continuously increase. Despite the importance of this research area and the substantial efforts applied, there are major unsolved privacy and security challenges, including those we aim to address in this project.

Current approaches mainly send all data from sensors to the cloud for data management and mining (e.g., TeraSwarm [7]). However, recent privacy discussions related to NSA activities indicate that centralized respectively third party solutions do not always protect privacy. Furthermore, many sensor and computing devices used are mobile and battery driven. Filtering and processing sensor data as close as possible to the source could substantially improve privacy protection and energy efficiency compared to a cloud approach.
Overlays are used to add functionality to sensor networks, like [1] and [6]. However, privacy in participatory sensing is a big and largely unsolved challenge. A good overview on the related challenges can be found in [11]. Surveys on privacy in mobile participatory sensing applications are given in [2], [12], and [13]. Privacy preserving data aggregation is addressed in [10] and [5]. Further important work includes PEPSI [4] and the work presented in [3] and [9].

**Research questions and scientific challenges**

To enforce the privacy requirements of a Smart Community, we investigate how to extend applications such that the privacy requirements are fulfilled. Given this high-level goal, we aim to contribute with new research results for the following challenges:

- Develop a methodology and tools to map a given CEP query and privacy policies to PPMs, extend the application queries with these PPMs, and place the corresponding executions on the best suited devices in the Smart Community.
- Identify vulnerabilities of Smart Communities and develop counter measures. This can include attacks from the inside, and possibly attacks from the outside.

**Scientific methods to be employed**

To drive the research we will use applications we are currently working with in the CESAR project, identify their privacy requirements, study potential attack scenarios, and define security goals and metrics to evaluate the solutions developed in the project. Languages for privacy policies will be investigated with respect to their usefulness to describe privacy needs and the capabilities of PPMs. This will serve as input for a process to extend CEP queries from applications such that the privacy requirements of a community are supported. Given this approach we will investigate counter measures to insider and outsider attacks.

We regard it as essential that the results of such a project are relevant and feasible to implement. Therefore, system design and prototype implementation will be used as the main method to validate the hypothesis.

**Research-ethical challenges:** There are no ethical challenges in this project.

**Project timeline:** The position will be for three years or four years including 25% teaching obligations. We aim also for a research stay abroad during this period, for example with our collaboration partners at National University of Singapore, Technical University of Darmstadt, or KTH Royal Institute of Technology (Stockholm).

**Applicant background and competence:** Documented experience in the areas of mobile ubiquitous computing, data management and mining, CEP, and privacy protection will be a clear advantage. Since we might offer a fourth year of funding for teaching obligations in INF3151, in depth knowledge in operating systems might be requested.

**Literature references**


