PhD-SafeIoT: Safety Analysis Tools for IoT Systems

Martin Steffen **Christian Johansen**
Precise Modelling and Analysis group (PMA)

The theme of this topic is the information agents of the future, also known as ubiquitous or pervasive agents. Ubiquitous information agents have computation abilities and the power to act on their physical environments. Examples include complex systems such as robot companions, self-driving cars (e.g., at Stanford or Google), as well as simpler agents as in smart homes for elderly and AAL, mobile travel devices, smart refrigerators, or electronic transactions agents. Ubiquitous agents operate in the living environments of people, interacting with (helping) people in their daily life. In consequence, the safety of the decisions and actions of such information agents is of paramount importance.

Based on our experiences from the IoTSec project *Security in IoT for Smart Grids* (NFR), we have identified the following aspects of IoT systems that need non-trivial investigations:

- the very large numbers of IoT devices that interact concurrently
- the dynamic nature of IoT systems, with addition of new kinds of devices and services
- the large amounts of generated data
- the need for open access wrt. service providers while respecting privacy of the generated data and ownership of software and hardware
- the need for location awareness (indoor, GPS, relative) in many applications
- the need for network awareness (WiFi, mobile, intranet, internet) in many applications

In particular the combination of these aspects create challenging research questions. To attack these research questions our main goal is to develop and implement

> *a semantic framework for development and modeling of IoT systems, including related modeling and analysis methodology as well as tool support.*

We define the following **objectives**:

1. *IoT abstraction mechanisms*: we will develop abstraction mechanisms that allow open access combined with privacy and ownership, including

   1.1. *IoT concurrency and communication:* we will develop support for the concurrency and communications mechanisms needed in the modeling of IoT systems/networks, including WiFi networks.

2. *dynamic IoT service development*: we will develop support for dynamic addition of new kinds of devices and services, including

   2.1. *location awareness:* we will develop support for locations and neighborhoods, migration, and changing environments.

3. *information safety and privacy*: we will develop language and analysis support for safety and privacy issues. This includes static and dynamic notions of privacy and location.
4. *scalability:* We aim at scalable modeling and analysis methods for IoT systems.

The success of these objectives will be addressed by means of prototypes and tools, case studies, scalability results, and theoretical soundness investigations. The expressiveness, naturalness and suitability of the modeling framework will be evaluated through case studies and comparisons.

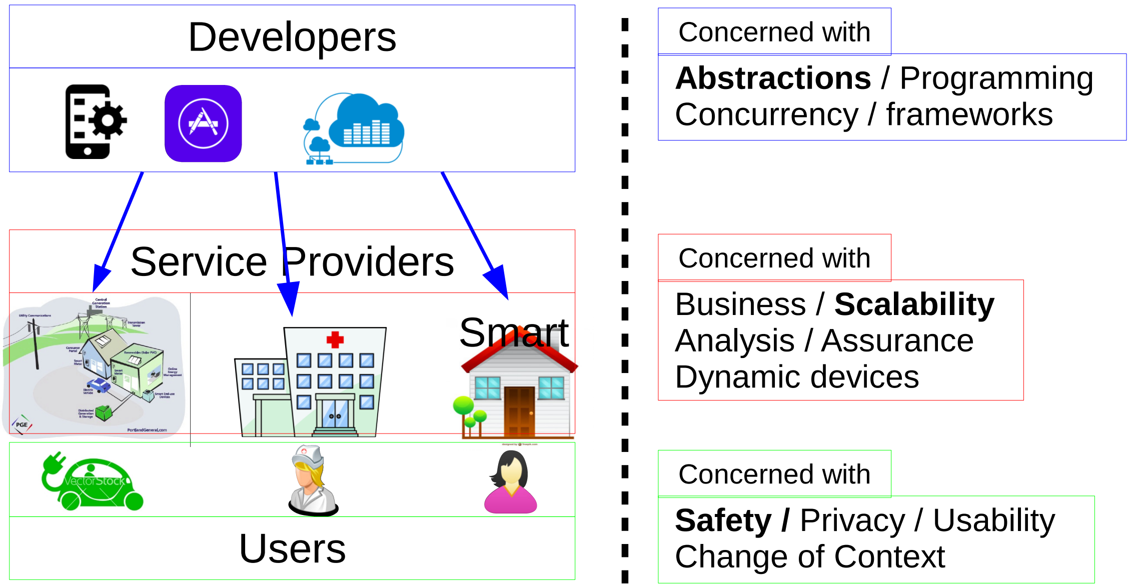

Figure 1: Sketch of the Objectives and their Motivation in the IoT enabled services and infrastructures, along with the main actors (end Users, Developers, and novel Service Providers) and their concerns. Our three main application areas are SmartGrid, eHospitals, and SmartHome

Scientific merit, concept and approach

As suggested by the UbiNet project SafeIoT considers communication and interaction as primitive concepts of IoT computation. Computation, regardless of the form in which it may manifest itself (like sensing, acting, actuating, analysing, evaluating, searching, etc.), is not done on a single entity any more, but on many computation devices at the same time, concurrently, close or distributed, and an entity may not even be aware of its purpose in the overall goal of the computation. Therefore, fundamentally we understand IoT computation as **an amalgam of communication/interaction and concurrency/distributivity.**

The Actor model has been suggested as a general model for service oriented distributed systems including IoT systems. However, *object orientation* offers a program structure that is better suited for reuse and offers a notion of response. The combination of the two paradigms in the form of active objects with asynchronous methods has the benefits of both modeling paradigms.

With distributivity comes the notion of *location and migration* (movement between locations). Therefore, the computation mechanism envisioned in SafeIoT would *encompass a notion of location with a general form of mobility*. Furthermore, IoT entities/systems must be *reflective and aware*, of both their behaviour and goals, as well as of the environment surrounding them. This can be achieved through logics and models with suitable abstractions.

A representative example showing the importance of location is in eHospitals (from ITU):

> *Many companies are today implementing systems based on the indoor location of medical personnel, and of devices such as terminals, beds, and patients. Their goal is to have the medic walk with a locating device and be logged-in/out of the terminals and be displayed the timely required medical info for the current patient. Applications include logging of medical procedures.*

Collaborations:

- ITU Copenhagen
- University of Liverpool