Internet of Things describes a general concept for the ability of items in the physical world to sense and collect data from the surroundings, and then share that data across the Internet where it can be processed and utilized for various interesting purposes. These sensors can use various types of local area connections such as RFID, NFC, Wi-Fi, Bluetooth LE, and Zigbee. Sensors can also have wide area connectivity such as GSM, GPRS, 3G, and LTE. These capabilities have certainly opened the door for several applications, including self-parking automobiles (e.g. Volvo S90), automatic ordering of groceries and other home supplies (e.g. Amazon Dash Wand), and receiving warnings on your phone or wearable device when the IoT devices detect some physical danger in the designated sensing areas (e.g. Bosch smart smoke detectors).

To realize this technology, several design challenges have to be efficiently tackled. For example, supplying power to this proliferation of IoT devices and their network connections can be expensive and logistically difficult. In addition, IoT widely triggers privacy concerns related to our personal data. Whether real-time information about our physical location or updates about our weight and blood pressure are to be streamed over wireless networks and potentially around the world, hence severe privacy threats dramatically emerge. Another example of the IoT challenges arises from developing solutions independently of each other, utilizing different platforms and frameworks resulting in many different devices that cannot integrate with one another. Therefore, it is imperative to achieve interoperability between different platforms and technologies so that IoT can reach its wide scale adoption and commercialization potential.

In this seminar, we identify the different IoT architectures along with their emerging challenges. We discuss the low power design of such systems and how we can manipulate the collected data to reduce the overall energy consumption. We also discuss new protocols for data communication and localization while providing protection against possible privacy threats. For data collection, we consider the potential of sensing the crowd and the mechanisms used as a motive for users to participate in data collection. We also cover the data aggregation and processing either in the nearby Fog nodes or in the cloud.

Note that this is an INFOTECH seminar targeting English-speaking students.