AKE2: Encryption for Internet of Things

Block course of 4 SWS in October 2019 by

Wai-Kong Lee, UTAR, Malaysia

What is Internet of Things (IoT)? It is a technology advancement moving towards connecting many things (if not everything) in our daily life to the Internet. With IoT, many innovative applications can be realized, including Smart Home, Smart Metering, Smart Healthcare, Industry 4.0 and Smart Agriculture. Since the sensor nodes in IoT may be collecting sensitive data from us (e.g. heartrate and electrical usage), the user privacy can be easily exposed. Moreover, some IoT applications allow users to perform control actions (e.g. lighting, motor movement and electrical appliances), which may cau se catastrophic consequences if they are being controlled by malicious attackers. Hence, we need security countermeasures to protect the communication in IoT!

This course introduces the basic concepts in cryptography and relates them to the security issues in IoT. Students will be exposed to the theoretical background of public key and secret key cryptography, followed by some advanced techniques to implement them in resource constrained microcontroller. Finally, advanced cryptosystem that allow computation on encrypted data (homomorphic encryption) will be introduced, which can be useful for secure data aggregation on IoT gateway.

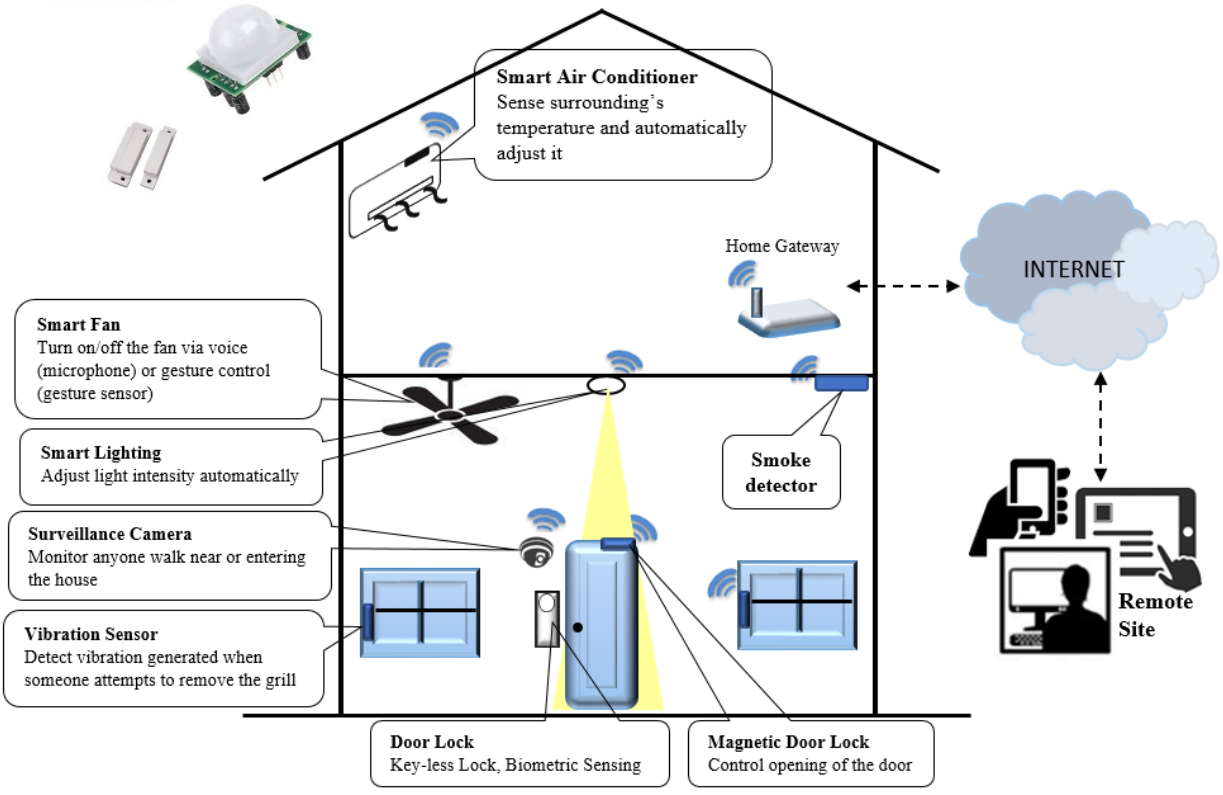

Figure 1: Smart Home, an example of IoT application