# **Security challenges:**

Ensuring security of IoT devices and services is compared to the degree of trust that every users give to the internet. Security in IoT is essentially related to the capacity of users to belief in their environment. Due to the progressively connected devices to the Internet, the possibility of potential risk grow. Low secured IoT devices could become an entry for cyberattack by permitting harmful persons to re-program a device or destruct the system. In the same time, a poor device design can uncover user data to theft by leaving data streams unprotected. The high dependence on IoT devices and internet services will also increase the pathways for offenders to procure access to devices.

In this reason, security of IoT devices and services is a crucial point for the whole system. Our dependency to these devices can influence immediately on our life.

## **3-1 Home Intrusion Scenario:**

Most houses still using the old security and alarm systems, which is a standard solution usually focus on a simple alarm system that make a noise when a fire detector, motion detector or other sensor is activated. Unfortunately, these systems are ignored because of their inefficiency. An alternative is to control the house by a company via a monitoring systems which manipulate various devices aimed to supervise the house situation.



Figure 7: Home security sensors

This system offer a very inexpensive and flexible installation that will cover all the security needs. It’s possible to choose the right equipment for each case. The challenge in this solution is how to protect our privacy with this kind of systems (composed by Indoor and Outdoor Cameras)? In this scenario, user need to get more control than the company itself, which means that an adapted access control system must be deployed in order to protect both privacy and home. In this scenario, the security system is triggered when outdoor and/or indoor cameras detect an unexpected movement in away mode and sends automatically a notification alert to the homeowner along with a picture or video taken by the installed camera. Using a motion sensor detector, a light switches and a smart thermostats user can setup the behavior of his smart home based on his comfort. E.g. when movement is detected, the light switches on automatically, the heating adjust the home temperature of the home owner before his waking up by triggering the outside temperature. Moreover, using a smart door lock the home owner can remotely control his house by giving access to guests (e.g. receiving a video call, photo of the one who’s on the door) so he can disarm the alarm system and unlock the door.

## **Fire alarm:**

A Fire alarm system is provided by a company serving an emergency-call system and the other company providing the off-site monitoring. When receiving an emergency call from an apartment, the central monitoring station will call an ambulance and a volunteer fire department.

To prevent unnecessary calls to the emergency services and avoid their disturbance action should not be taken by the sensor itself but by the homeowner who should react promptly.

## **Home Heating Scenario:**

In smart home some intelligent control are added in order to get more comfort, reducing energy and saving money. It provides to users the possibility to decide which areas of the home are heated, when they are heated and to what temperature. For more satisfaction, rooms’ radiators arrange themselves based on automatic schedules and they can also be controlled from a smartphone. Creating different zones permits to only heat the parts of the home that the user wants, which help him to save energy and money waste.

As an example, when a special room (for old person or sensitive animal) is becoming too hot, the simple solution is to open the window, which causes a lot of waste especially in winter. An intelligent solution is to put a detector in the window to switch off the room’s radiators when the window is opened in the aim to reduce wasted heat and save costs.

From another point of view, the system needs a high security in order to prevent an attacker from gaining access to the entire system and changes the heating system where ageing person and animal inside the house can be victim to malicious behavior.

In this scenario, the company can control the system usage when an energy waste is detected without any user intervention.

In this scenario, the homeowner can limit the access of the company with the aim of preserving his privacy.

## **Health Scenario:**

|  |
| --- |
| Figure 11- Whithings scale[9] |

Different health gadget are available in the market, but the majority don’t care about interoperability with other systems such as android, iOS. The product proposed in this study can be used in a smart home directly by users to check health issues. It a scale gather which sense information like blood pressure, heart rate, etc.… The data captured is automatically transformed to the cloud via a hub installed at home using Wi-Fi protocols. On the other side, a doctor gets a notification of all the body state. This monitoring system can be used to send ambulance as quickly as possible if any health problems occur

|  |
| --- |
| The challenge in this scenario is to secure the access to the equipment because it is directly linked to an external network (Doctor, Hospital) and it contains many precious data about the patient. An offender can directly attack the hub to make a connection to the cloud and get all the private information. It is judged crucial to secure this part because if we suppose that a wrongdoer gets access to the heating system in the same time and the homeowner suffer from breathing problems a crime can happen easily. |
|  |

To prevent the analysis of data sent by the scale to the doctors of the homeowner when an unauthorized user uses the scale an access control is needed.