IoT6 architecture

User comfort and energy efficiency use case

Dejan Drajic, Srdjan Krco

Introduction

IoT6 architecture was designed in an iterative process, starting from the initial based on the use case and derived requirements (released in 2012). In 2013, the architecture was updated based on the research outputs of the project. In the final year of the project (2014), the architecture was updated once again taking the latest developments in the project. In addition to this, IoT6 architecture was adapted and aligned according to the IoT ARM methodology [1]. This was done in order to validate our initial approach in regard to the architecture design against the work done in the domain of IoT architecture design in the community, but also to make IoT6 results easier to reuse and leverage in new projects.

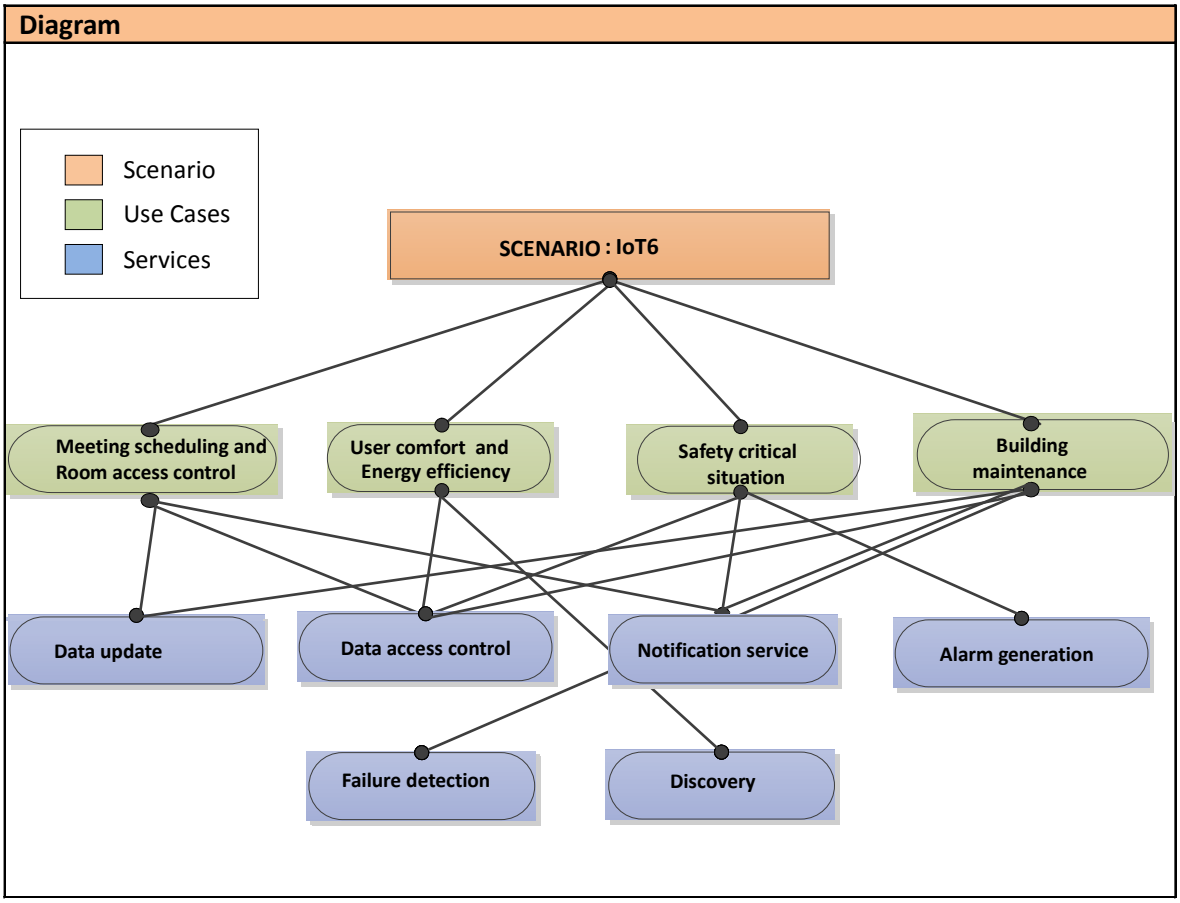
This document represents an excerpt of the final architecture document [2]. It provides description of a use case used for implementation of a proof of concept of projects main innovations and the accompanying architectural views. The use case and the architectural functional view are presented according to the IoT ARM methodology.

The purpose of the document is to showcase how IoT ARM methodology can be used. In addition to this the document should serve as a teaser for other projects, organizations and individuals to consider using IoT ARM as the basis for design of architectures for own IoT systems, thus helping easier reusability of the components and streamlining of IoT developments aiming to facilitate rapid adoption of common techniques and solutions.

User comfort and energy efficiency use case

The structure of the IoT6 proof of concept scenario is presented in the figure below. It consists of 4 use cases, which in turn consist of several services. In this white paper, we will address the User comfort and energy efficiency use case only together with two related services: data access control and notification service. For the details of other use cases and services we refer the reader to the project deliverable [1],[3]

User comfort and energy efficiency use case focuses on the correct operation of building automation devices and systems. In order to control the sensors through a mobile client, it is first necessary to discover them in the environment. Further to this, the system should act autonomously to the furthest extent possible and has to assure a good balance of user comfort and energy efficiency according to the environmental situation and the predicted amount of locally available energy. Therefore, the incorporation of local sensors (e.g., brightness sensor) as well as the weather situation into control strategies is required. The use case is presented according to the IoT architecture reference model (IoT ARM), that represents one of the the most prominent pieces of work in the domain of IoT architecture design.



Use case description

The employee uses a Building Automation Services App installed on a mobile device (e.g., a tablet or smart phone) to control the room environment (e.g., temperature, light). This application uses the Global Resource Discovery system to identify nearby sensors and actuators and communicates with a multi-protocol IoT6 Gateway which in turn communicates with legacy devices to control the environment (actuators). The application (mobile client) also interacts with a Local CMS responsible for the overall coordination of the energy monitoring and assuring user comfort based on the users' preferences.

The Meeting Reservation Tool communicates energy saving requests to the local CMS. The local CMS detects that the light intensity is too low by using the light intensity sensor values provided by the tablet/smart phone (Building Automation Services App) and thus it increases the brightness by turning on more lights in collaboration with the IoT6 Multi-protocol Gateway (the gateway controls legacy devices and obtains information from an Internet weather service which is used by CMS to set light intensity to a proper level).

At the beginning of the meeting the weather station reports cloudy weather and thus the power production of the photovoltaic system providing power to the office building can be considered low. The

room temperature set point is decreased to save energy. During the meeting the weather station reports sunny weather, which means that more renewable energy will become available to partially cover the energy consumption of the HVAC devices. In this case, the temperature set point is increased again to the comfort temperature level.

Actors Involved (& Role played)

Administrator: a system administrator with permissions to register profiles and permissions for users.
User A: A physical person that interacts with a particular component in the IoT6 system.

Devices: smartphone, tablet, light switch actuator, temperature sensor

Legacy Devices*: RFID reader/door opener/light actuator/heating valve/sun blind actuator/brightness actuator/ legacy alarm device (legacy device)*: devices of this class communicate via protocols that are different from the IPv6 protocol; in IoT6 are referred to as "legacy protocols". Legacy devices are therefore usually integrated into the IoT6 through some form of gateway.

Physical Entities: phenomena which are observed in the system, i.e. presence of the sensors and actuators in office**.**

Information: virtual entity as a passive digital artefact, which is the digital representation of the physical entities, a report about a presence

Building Automation Services App: a resource, i.e. application that runs on a mobile device and can be used to wirelessly access devices. It may also be used to wirelessly activate or deactivate pre-configured setups. Apart from that, the application allows reception and distribution of messages from a brightness sensor installed at the hosting mobile device.

Global Resource Directory (GRD): a resource at which devices of the IoT6 are registered and which can be used to search and discover devices based on certain criteria. It can be used to locate services available within a particular area.

IoT6 Multi-protocol gateway (IoT6 GW): a resource that provides an IoT6 stack interface for legacy devices which can be deployed on a smart board. The IoT6 GW thereby provides oBIX objects for interaction with legacy devices and as such acts as a layer of abstraction between IoT6 and heterogeneous legacy devices and their associated networks.

Local Control and Management System (CMS): a resource that handles execution of scenes in form of rules. These rules may be used to perceive the environment and its status and make the system act accordingly. Further to this, the component may also host legacy devices connected to the IoT6 through a local CMS as a gateway.

Meeting Reservation Tool (SaaS): a resource, i.e. application that allows a human controller to schedule a meeting for a smart meeting room. The human controller can thereby fix the date when the meeting will start and for how long the meeting will last. Additionally, the Meeting Reservation Tool allows specification of a list of RFID tags representing people who are allowed to enter the meeting room (i.e., meeting attendants).

Services

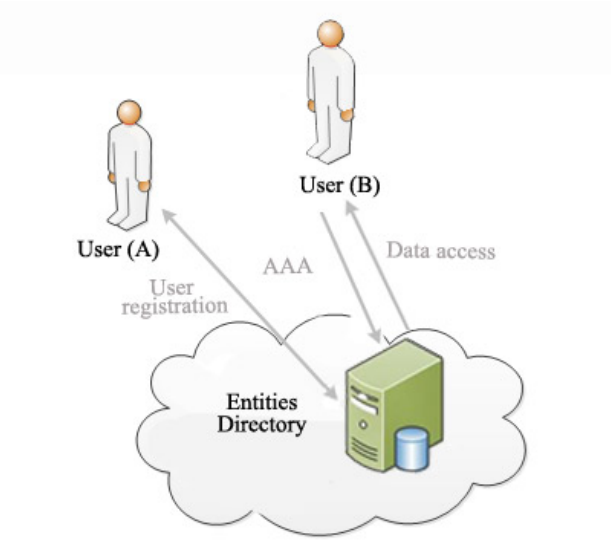
IoT *Services* provide well-defined and standardized interfaces, hiding the complexity of accessing a variety of heterogeneous *Resources*. The interaction with a *Physical Entity* can be accomplished via one or more *Services* associated with the corresponding *Virtual Entity*. This association becomes important in the process of look-up and discovery. An IoT *Service* can thus be defined as a type of *Service* enabling interactions with the real world. The following services are involved in the user comfort and energy efficiency use case:

- Data access control
- Discovery.

Data access control service

This service provides access to the system components through implementation of all authentication, authorization and accounting (AAA) mechanisms. Access to the virtual entities is provided for the registered users only. Data access is restricted to registered users allowing only those having a digital profile with sufficient privileges to retrieve certain information. Data access control handles several users' roles. The user creation and management is one of the key components in the platform. The platform should manage several types of user accounts as well as the user authentication in the system. Data access control should be performed in such a way to limit the access and grant it to a trusted group only. Figure below represents the IoT context view for the data access control service, outlining the main entities relevant for the service and their relationship.

IoTContext View



Actors Involved (and Role played):

- **User (A):** User with permission to register a new virtual entity, i.e. a profile for other users.
- **User (B):** A person that accesses the entities directory.
- **Information:** A virtual entity as a passive digital artefact, which is a digital representation of physical entities. In this case, the main information includes the user identification as well as the other associated information such as roles, permissions etc.
- **Entity directory:** Resource that contains global information about physical entities, services and other resources.

Service Requirements:

- Device ID registration/User registration
- User data anonymization
- Entities directory
- Secure communication between the user and the platform (AAA)
- Profile and virtual identity management must be supported
- Context and influence on privacy policies must be properly formalized
- Identification and authentication mechanisms for involved actors must be provided
- Entities directory (to implement Users Directory)
- Depending on access control policies, access requests will be evaluated

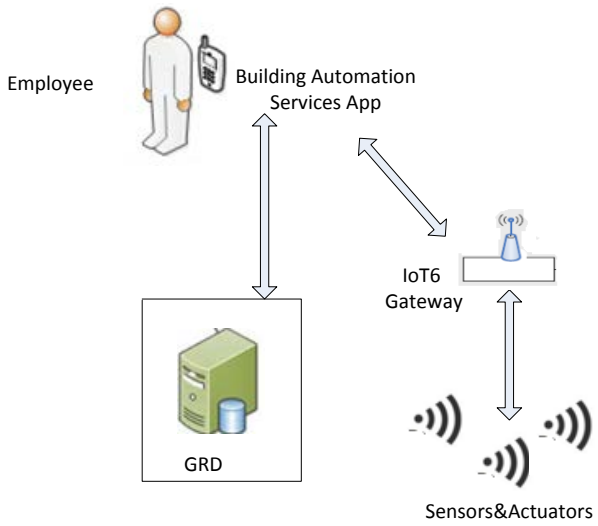
Service Features:

- User management AAA
- Secure communication between the user and the platform
- Data access to virtual entity in the entity directory
- User interface to show access result

Discovery Service

This service allows physical entities (nearby sensors and actuators) to be discovered using Building Automation Services App installed at a mobile device (e.g., a tablet or smart phone) and saved as virtual entity in the application. Building Automation Services App uses the Global Resource Directory system to identify nearby sensors and actuators. After that Building Automation Service App (mobile client) communicate with appropriate discovered devices (legacy HVAC devices and actuator) via multi-protocol IoT6 Gateway and performs environmental control.

IoT Context View



Actors Involved (and Role played):

- **Administrator: A** system administrator with permission to register the profile and permissions for users. System management.
- **Users:** A physical person, employee
- **Physical Entities: P**henomena which are observed in the system, presence of the nearby sensors or actuators
- **Information:** Virtual entity as a passive digital artefact, which is the digital representation of the physical entities, information about the presence of the person.
- **Global Resource Directory (GRD):** A resource at which devices of the IoT6 are registered and which can be used to search and discover devices based on certain criteria. It can be used to locate services available within a particular area.
- **Devices:** Sensors, actuators, smart phones, and tablets.

Service Requirements:

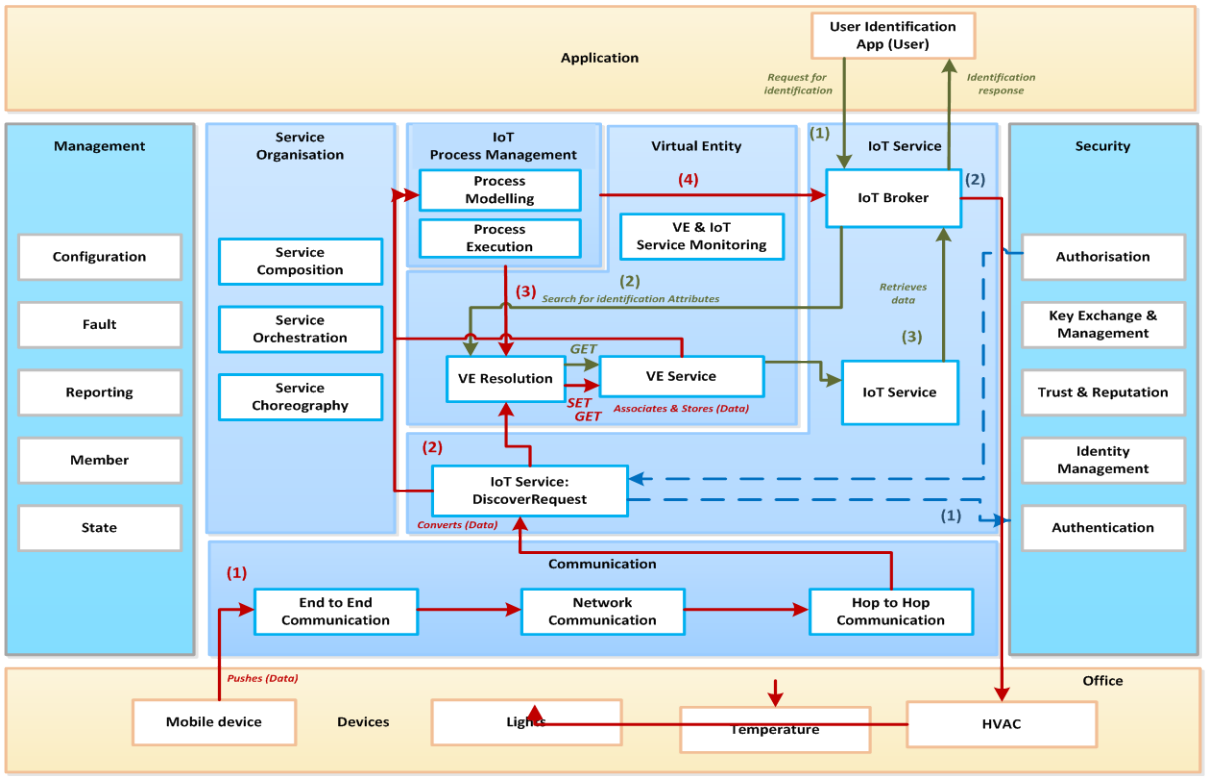
- Global resource directory
- Reliable storage
- Profile and virtual identity management must be supported
- Identification and authentication mechanisms for involved actors must be provided

Service Features:

- Discovering sensors and actuators
- Profile creation and management tool supporting virtual identities
- Secured access (with different levels of security available) to all information
- Building Automation Services Application
- Initiation of actions (sensors and actuators).

IoT Functional View

Figure below shows the IoT6 functional view, built using IoT ARM functional view as the basis. Information flow is overlaid, outlining interaction and the flow of information for the User comfort and energy efficiency use case.



Conclusions

The use case presented is one of the use cases used to drive implementation of a proof concept for the project results. It combines several IoT devices, web services, user applications and users in the context of a smart building, thus highlighting the power of IPv6 and IoT to integrate heterogeneous entities in a working system. At the same time, the document provides a brief outline of how Iot ARM methodology can be used to describe a use case and how architectural views for such use case look like if that methodology is used. The upside of following this approach is that it becomes easily visible and identifiable which entities, components and relationships between different use cases can be reused, thus facilitating more rapid development and implementation of IoT solutions.

References

[1] Internet of Things Architecture, IoT-A project,, deliverbale D 1.5 - Final Architectural Reference Model for the IoT, http://www.iot-a.eu/public/public-documents/d1.5/view

[2] IoT6 project, deliverable D1.4 – Updated version of IoT6 Architecture and SOA Specifications, http://iot6.eu/deliverables

[3] IoT6 project, deliverable D7.2 – Components Instantiations and validation report, http://iot6.eu/deliverables

[4] IoT6 (Internet of Things) project, http://iot6.eu/