IHouse - control hub for smart houses

Robert-Ioan Onesim

July 2017

The aim of the thesis *IHouse - control hub for smart houses* is to come up with a solution for a series of problems dealing with the Internet of Things (IoT), a field that is ever expanding and evolving in recent years.

The considerable amount of different smart devices on the market controlled by a wide variety of mobile applications and the lack of a standardization system led us to the idea of implementing an application that by combining the client (Android) and the server side (API) offers the opportunity to control and monitor a smart house, regardless of the type and manufacturer of the IoT devices. In addition, the functionality provided by the control hub (server) alongside the automation system based on rules and scenarios improve the user's lifestyle.

The first chapter (*General description*) provides detailed information about the growing importance of the Internet of Things and about the security issues of smart devices which can be extended to smart houses. Moreover, it presents the motivation and contributions in developing the project *IHouse - control hub for smart houses*.

The following two chapters (*Technologies* and *Application architecture*) describe the technologies used in developing the application and its architectural structure. Each component is depicted using logic schemas to provide a better understanding of how it works.

The fourth chapter (*Modules description*) focuses on the implementation details of the modules, each feature being presented using short descriptions and images.

The last chapter (*Conclusions*) reviews the main takeaways that

can be drawn from using *IHouse - control hub for smart houses* and the improvements that may be brought to the application.

Bibliography

- Internet Society, The Internet of Things: An Overview - Understanding the Issues and Challenges texttthttp://www.internetsociety.org/sites/default/files/ISOC-IoT-Overview-20151022.pdf
- Richardson, Leonard and Ruby, Sam.RESTful Web Services. Sebastopol:O'Reilly Media, 2007
- BitDefender LABS, Hackers Can Use Smart Sockets to Shut Down Critical Systems. `https://labs.bitdefender.com/2016/08/hackers-can-use-smart-sockets-to-shut-down-critical-systems/`