Longevity of Smart Homes

Peter Zdankin
Supervised by Torben Weis
University of Duisburg-Essen

Abstract—**Progress in the field of IoT has enabled home automation and the interconnection of devices to a smart home. These smart homes are composed from various systems and physical devices and are interconnected according to an architecture. The system architectures are not optimized for the aspect of longevity of their installations. In our research, we focus on threats to the longevity of such systems and additionally apply these insights to the field of smart cities.**

Index Terms—**Smart Home, Longevity, Internet of Things, Cloud, Smart city**

I. Introduction

The internet of things has enabled pervasive applications such as smart homes to reach the consumer market. A smart home can enhance the comfort through automation, such as motion detected lighting or security measures, but may also reduce ongoing costs through scheduled heating. Important aspects of smart homes are:

- components - the required hardware and physical devices
- architecture - the semantic connectivity between the components e.g. server-centric
- platform - the software that users can interact with to control the smart home

As time progresses, each of these may be imperiled to the threats of aging software and hardware systems, such as discontinued services or breaking updates. The required devices are often integrated solutions, such as light bulbs with included chips that enable this communication. A partial replacement of these chips is therefore often not possible and devices must be replaced entirely, if a fault occurs. In addition, the accessories are expensive and difficult to install when compared to non-smart accessories. Therefore, longevity in smart homes is desirable. With our research, we want to contribute to how IoT systems in general and smart homes specifically can optimize for longevity, which problems need to be addressed and how they could be solved.

II. Related Work

Longevity in the field of software engineering is a well-recognized problem and a research programme exists [1]. However, longevity in the context of smart homes is not understood sufficiently. Complex systems may be composed of various different components that need to communicate with one another. One way of doing so could be through a public API, which is provided by the vendors to communicate with the respective components. This API may change and as such may cause incompatibilities in between these components. According to Winters, there are three strategies that can be used when updating APIs. They may not be updated at all and are a fixed standard, may be updated periodically or updated frequently [2]. While rules such as semantic versioning exist and should make breaking changes less common, there may be the need to perform updates that break dependencies in favor of e.g. security issues [3]. Wu et al. created a program to audit changes of APIs in Java programs by inspecting their binary files [4]. A service-oriented architecture (SOA) may be used to enable miscellaneous systems to communicate with each other through a set of rather abstract services, which may act like black boxes. Using an SOA for smart homes has been done to manage lights in a smart office in the experiments of Degeler et al. [5]. Chen et al. shown how service updates in an SOA can be executed [6].

Smart cities are described in the works of Zanella et al. and a proof of concept was done in the city of Padova [7]. They can help to improve energy management, transportation and other infrastructure [8]. Smart homes, as the building blocks of smart cities, should support these tasks [9].

III. Research Challenges

In this section, we present the main research challenges that we have identified in the longevity of pervasive IoT applications, such as smart homes.

A. Aspects of Longevity in Smart Homes

The first research challenge is to analyze currently deployed smart home systems under the aspect of longevity. Initially, we need to define the term of longevity in the context of smart homes. We then need to evaluate what could compromize that longevity. As smart home architectures may vary depending on the implementation, in previous work we defined common patterns between them and classified different kinds of architectures. Through this classification we could identify several threats to the longevity of these architectures and argued about the potential impact of threats on those architectures. We concluded that no smart home architecture is sufficiently secured against the dangers that could arise in the lifetime of smart homes [10].

B. Functionality preserving updates

The second research challenge consists of finding ways to update several interconnected accessories in for example smart homes, while preserving core functionality. Usually, all kinds of smart home accessories can be updated independently from each other and may break dependencies between devices. If smart home accessories would describe their capabilities to other devices as a set of predefined services, dependencies in between devices could be expressed as a required set of these services. Updates for accessories could then add or remove some services from an accessory and this way alter the established dependencies. If the set of available services and the changes through updates were analyzed, the implications of updates could be predicted. We want to use this approach to solve problems that are difficult in current architectures. Smart home accessories can be updated individually and often enough there is a set of accessories that may have available software updates. Ideally, all devices are updated to their latest respective version, which could cause some devices being incompatible with one another if they are updated. Rolling back the firmware is not always possible and such an *update dead end* could be prevented, if all updates of the smart home are considered before updating. By inspecting the current dependencies and all the implications that available updates have on the set of available services, an ideal update configuration is to be found that ideally preserves the existing services while adding new features and security. Supporting non-technical users to solve this problem is a research topic that is going to be investigated. We want to implement such a mechanism and evaluate the feasibility of such an approach to manage a multitude of updates for smart home accessories.

C. Self-contained Smart Home Systems

An issue with smart homes are external services, that could be discontinued eventually. In this research challenge, we want to find ways on how to make smart homes independent of these services. We want to research the exact purposes, that external services serve, and how these can be made independent of the provider, to have the option to pull these external services away from other server and set it up in a local network. Approaches like virtualization in the form of containers, that can be hosted in the cloud, but also local networks, may be a promising approach that will be investigated. Proving the solution can be done by inspecting which components of a smart home still require to communicate with external services, and whether it is possible to completely cut the connection to them. Secure user management as well as the process of firmware management will require research in this context.

D. Privacy, Security and Ownership of Second Hand Smart Homes

If the ownership over a smart home changes, this could introduce a set of privacy and security issues. The users of smart homes must be certain that previous owners do not have access to any information about their smart home. Equally, when the ownership over a smart home is transferred, the previous owners need to be certain that none of their personal data remain in the smart home. Initially, we will inspect the state of the art in smart home platforms and which solutions they offer. We then will categorize how the different approaches to this problem, if any, differentiate and why some accessories do not feature these solutions. Furthermore, we need to inspect how the ownership itself is transferred because local hosting of smart homes could cause issues with this. Resetting all devices to factory settings will also cut all links between devices, which would cause much work to reestablish all connections. We therefore want to explore solutions that delete personal information, but leave structural information about the connectivity inside a smart home intact.

E. Longevity of Smart Cities

Smart cities and urban networks are comparable to smart homes on a much bigger scale in terms of size and complexity. In the last research question, we will try to find parallels between smart homes and smart cities and which insights that were gathered during our research can be transferred to smart cities. For this, we will research what work has been done in the implementation of smart cities, which architectures are used to connect a whole city and how the longevity of these can be asserted.

IV. Conclusion

This research has the goal of long-lasting IoT systems, that can deal with possible problems that may occur over time. We are currently developing update strategies for smart homes and want to visualize the impact of individual updates on the dependency graph.

Acknowledgement

I would like to thank my supervisor Torben Weis for his guidance and support and my colleague Marian Waltereit for his help in this research project.

References

[1] P. D. R. H. Reussner. (2012) SPP 1593: Design for Future - Managed Software Evolution. [Online]. Available: https://gepris.dfg.de/gepris/projekt/198572722?context=projekt&task=showDetail&id=198572722&

[2] T. Winters, "Non-atomic refactoring and software sustainability," in *2018 IEEE/ACM 2nd International Workshop on API Usage and Evolution (WAPI)*, June 2018, pp. 2–5.

[3] T. Preston-Werner. (2019) Semantic Versioning 2.0.0. [Online]. Available: https://semver.org

[4] W. Wu, B. Adams, Y. Guéhéneuc, and G. Antoniol, "Acua: Api change and usage auditor," in *2014 IEEE 14th International Working Conference on Source Code Analysis and Manipulation*, Sep. 2014, pp. 89–94.

[5] V. Degeler, L. I. L. Gonzalez, M. Leva, P. Shrubsole, S. Bonomi, O. Amft, and A. Lazovik, "Service-oriented architecture for smart environments (short paper)," in *2013 IEEE 6th International Conference on Service-Oriented Computing and Applications*, Dec 2013, pp. 99–104.

[6] J. Chen and L. Huang, "Supporting dynamic service updates in pervasive applications," in *2011 IEEE 35th Annual Computer Software and Applications Conference*, July 2011, pp. 273–278.

[7] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of things for smart cities," *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 22–32, Feb 2014.

[8] S. Mehrotra and R. Dhande, "Smart cities and smart homes: From realization to reality," in *2015 International Conference on Green Computing and Internet of Things (ICGCIoT)*, Oct 2015, pp. 1236–1239.

[9] S. Ghosh, "Smart homes: Architectural and engineering design imperatives for smart city building codes," in *2018 Technologies for Smart-City Energy Security and Power (ICSESP)*, March 2018, pp. 1–4.

[10] P. Zdankin, M. Waltereit, V. Matkovic, and T. Weis, "Towards longevity of smart home systems," in *PerIoT 2020: 4th International Workshop on Mobile and Pervasive Internet of Things (PerIoT 2020)*, Austin, USA, Mar. 2020.