Jochen Bauer*, Christoph Konrad, Michael Hechtel, Reiner Wichert, Christian Weigand, Simon Dengler, Martin Holzwarth and Jörg Franke

ForeSight Approach to improve Privacy and Security in the Smart Living Domain

Abstract: This contribution describes how to improve privacy and security for the Smart Living domain. Core elements of this approach adapt the Privacy by Design concept to the domain of smart living and extend it to enable artificial intelligence integration. To improve security, we created a minimum framework based on an existing information security management system to offer a holistic perspective on that topic. This, we think, is necessary, primarily if legacy Internet of Things devices should be supported.

Keywords: AAL, Privacy, Security, Smart Living

<https://doi.org/10.1515/cdbme-2021-2230>

1 Introduction

The Internet of Things (IoT) devices are increasing at a rapid speed [1, 2]. If these devices share their information in a meaningful way, many existing use cases will be enriched. On the one hand, that means an enormous potential benefit for our society. On the other hand, challenges arise regarding privacy and security.

Today, web-based services offer data privacy statements, enabling the service providers to gather data and allow extensive data handling. Usually, the user who delivered the data cannot see what happened to it or knows about the access frequency. For example, if an application on an Android cell phone needs access to a specific sensor, you can grant such access once. Afterward, you will not get any more runtime information when and how many accesses have happened.

In the ForeSight project, we address privacy and security topics, among others. ForeSight strives to create an AI-driven

Smart Living Platform [3, 4]. There is a connection to other researching activities [6, 7] and European initiatives like Gaia-X [3-5].

2 Challenges

With the General Data Protection Regulation (GDPR), the rules for personal data processing have been harmonized across the EU. The main goal of the GDPR was to protect consumers and their data. Before GDPR existed, companies secretly collected data without informing their users. Today this is sometimes described in very long confusing users license agreements.

However, what is more important is that the GDPR prescribes which sensor data a company is allowed to use for analysis purposes, but not what can be derived from it. If this data is shared and aggregated, it will be possible to determine users' behavior precisely. For example, movement patterns can be recognized in chronological order from presence detectors (e.g., getting up, leaving the apartment, length of stay in the bathroom). This data sharing strategy needs to be improved with the data creator in mind.

Privacy cannot be achieved with a lack of security. This is especially challenging in smart living and AAL environments due to the nonprofessionals who administrate networks or the elderly, who are less experienced with intelligent devices. Moreover, promising smart home and AAL concepts need to consider integrating into a group of buildings or smart cities.

3 Approach

In this section, we describe our approach to address these challenges. First, we mention relevant components of our concept and then we describe a promising architecture approach, extended by relevant further thoughts to access health-related markets, i.e. with the help of DiGA, the first digital health applications (DiGA), or DiPAs.

*Corresponding author: Jochen Bauer: Lehrstuhl für Fertigungsautomatisierung und Produktionssystematik, Friedrich-Alexander-Universität Erlangen-Nürnberg, Fürther Str. 246b, 90429 Nürnberg, Germany (Christoph Konrad, Michael Hechtel, Simon Dengler, Martin Holzwarth; Jörg Franke)
Reiner Wichert, Sage Living GmbH, Pfungstadt, Germany
Christian Weigand, Fraunhofer IIS, Erlangen, Germany

3.1.1 Privacy by Design

Privacy by Design (PbD) is a helpful framework and concept to determine GDPR-specific requirements and transforms them into actions, rules, and processes of the ForeSight platform. In the center of the PbD are the elements a) Lawfulness of processing; b) Risk management (including security and privacy-related tasks); c) Technical and organizational measures (TOMs), and d) Privacy by Default (see Fig. 1).

Figure 1 Privacy by Design and corresponding components.

In ForeSight, we empower service providers, i.e., small and medium-sized enterprises, to create and operate so-called advanced smart services based on their existing business models. Therefore, we need to offer relevant PbD-specific documents or drafts of such documents to these organizations. The TOMs and the Risk Management steps can be combined with the Information Security Management System (ISMS), which will be described in the following section. The last of the four steps in Fig. 1 is the decision to go for privacy-friendly default values.

3.1.2 ISMS adaption for Smart Living

We adapted an ISMS called ISIS-12, which addresses SMEs (Small and medium-sized enterprises) to the needs of AAL- and Smart Living Systems. An ISMS is a perfect addition to

privacy-related concepts because risk management and TOMs are part of both frameworks. Security is a holistic challenge, and so we see no alternative to creating our own small ISMS.

Figure 2 Steps of ISIS-12 an ISMS for SMEs.

The first step is to create a security guideline (see Fig. 2) as one of the critical documents. Afterward, all people need to be informed how to work with this framework. Usually, a small security team needs to be found with their specific roles. Steps 04, 05, 06, and 07 are related to network infrastructure, software management tasks, and risk calculations. ‘Step 08, Step 09, and Step 10 are to identify and schedule the correct TOMs. In step 11, there will be an internal audit to see what needs to be changed, and afterward, in step 12, an external auditor visits the site and evaluates the system's current state. Based on the reduced complexity of this adapted framework the intended user will be more likely to quickly learn how to use their smart home and AAL applications in a secure way.

3.1.3 Architecture, Roles and Stakeholders

Our architectural approach is based on the ideas of Gaia-X. Following this cloud-based concept is improving data sovereignty by adding an abstraction layer for Infrastructure as a Service Providers. In a simplified description, each use case and each software module is represented as a service, which will declare its functions, parameters, and constraints with the help of a service description file. Such a service registered itself in a service registry component with all other services. At runtime, these services interact. To integrate IoT devices, we offer different ways to aggregate data and enrich this data with semantic information, i.e., with the help of SENSE-WoT (an adapted version of the Web of Things ontologies and semantics for smart living environments) [https://www.projekt-sense.de/sensewot] and transfer the data to the cloud. Now, we want services to describe their specific

data requirements and corresponding purpose. Furthermore, we added a logging mechanism that the frequency of such data access operations would be transparent because each service needs to log an event when an interaction with another service happens.

Figure 3: Common stakeholders and roles in a smart living environment and the idea of dynamically changeable access rights.

The approach of rights distribution on a role and group basis enables a fine-grained distribution of rights for different data points of the smart home devices and forms a fundamental building block for service development in Gaia-X. Based on the stored user profile, various user attributes can additionally be queried in a data protection-compliant manner. For example, a service requiring a phone number cannot be booked, if the user has not stored a corresponding number..

Users are also assigned to their apartments so that a type of linked data is also applied here to obtain additional meta-information. In addition, access to the apartment is supplemented by various roles. Thus, the following persons have access to parts of the apartment in descending order as based on their needs: owner, tenant, occupant, third party (craftsman), guest. The minimum principle has to apply to everyone having only the minimum necessary rights to avoid misuse of rights.

The whole access issue is protected by the open-source identity and access management Keycloak, where both humans and machines have to authorize, authenticate and authenticate themselves to ensure the most significant possible protection for personal data. Keycloak is based on the previously available Gaia-X architecture around meta-information such as self-descriptions and access management to access services. Identification is to take place using Gaia-X-compliant options such as the eID card

3.1.4 Runtime Permissions and Reports

Therefore, our approach is to apply the access rights to application services and applications, as is done in a similar way to Android OS with their apps. In contrast to the apps approach, however, this does not only have to take place at the sensor level, but also at the level of data analysis and situation and behaviour detection. Using a hierarchical approach, this assignment of rights down to the sensor level must then also be made possible along the data structure. This would enable users to assess which access rights they would like to grant a company over their life and lifestyle, and we are sure that this will enable a fairer handling of user data and privacy protection. To improve the transparency for the data creator, each known user will view the data access logs and limit and revoke access rights whenever he wants.

3.1.5 DiPA and DiGA

The new Digital Health Care Act (DVG), came onto the market in the middle to end of last year. These apps on prescription are aimed directly at the patient and therefore require a layman's understanding, especially in safety and security. Of course, the same also applies to digital care applications (DiPA) aimed at the care market. The legislature has paid the most outstanding possible attention to safety here. At the very least, DiGAs must meet the requirements of class I-IIa medical devices and be approved as such. Due to the tightening of the new Medical Device Regulation (MDR), however, digital applications mostly fall into class IIa based on Rule 11 and thus place high demands on the manufacturer. In addition, the legislator now demands from the manufacturer and operator of a DiGA to operate at least an ISO 27001 certified Information Security Management System (ISMS). For the upcoming DiPAs, the requirements will decrease. For example, it is not expected here that DiPAs will have to be approved as medical devices. Nevertheless, it remains to be seen which information security provisions will ultimately find their way into legislation.

In the end, however, it always depends on the manufacturer and its will, ability and diligence implementing the individual requirements. A uniform communication platform (backend) that has been tested for information security would certainly be helpful [8].

3.1.6 Smart City Compatibility

Since the different domains of Smart Living are increasingly connected in order to enable common data analysis and new business models for assistance services even across domain boundaries, the importance of protecting these domain boundaries from the IT security point of view as well as from the point of view of privacy protection will continue to grow in the future. For this purpose, new security concepts must be created to protect the borders between these domains to a high degree. This also applies to the scaling in a spatial perspective: for this purpose, the area close to the body with personal health sensors or the smart phone must be separated from the apartment in which the user is staying. The apartment, in turn, is located in the building with other apartments, but access between the apartments must be limited because not everyone has the same rights in all apartments, but on the other side it makes sense to use their data for building management. The same applies to the individual buildings in the quarter and also to several quarters in a smart city approach. Different security levels have to be implemented at each of these borders and the closer we get from the city to the apartment and to the body space, the more stringent restrictions on privacy have to be implemented.

4 Implementation

The proof of concept is currently developed. In an intelligent kitchen environment, we demonstrate our current approach at the end of 2021. Due to the dynamic Gaia-X project progress and the decision that our efforts shall be compatible with the Gaia-X ecosystem, we use the same technologies, such as Keycloak, Open Shift, and semantically enriched information.

5 Discussion

The goal to maximize data sovereignty is ambitious, primarily due to the named challenges. In the AAL or smart living domain, we have a unique situation that we can distinguish between different people. Therefore ForeSight is an excellent match to identify relevant further requirements if you address each person as a known system user.

The AI and IoT integrations are changing the requirements on the platforms dramatically. ForeSight uses several smart home middleware systems, such as openHAB, so it is possible to support several legacy systems. The idea of

extending the cloud-based access-rights management from the cloud to the local network is helpful and probably necessary, but this is a smart-home-middleware-specific task and so much effort, if more than two middleware platforms are addressed.

The integration of AI is challenging as well because albeit its enormous potential, it is hard to define the possible data usage right from the beginning. It seems helpful if there is a way to change such decisions and definitions at runtime as well.

Author Statement

Research funding: This work was supported by the BMWi (ForeSight). Authors state no conflict of interest.

References

- [1] Smart Home Market by Product, Software & Services | COVID-19 Impact Analysis | MarketsandMarkets™. [Online]. Available: <https://www.marketsandmarkets.com/Market-Reports/smart-homes-and-assisted-living-advanced-technologie-and-global-market-121.html> (accessed: Jul. 14 2021).
- [2] IDC: The premier global market intelligence company. IDC Forecasts Double-Digit Growth for Smart Home Devices as Consumers Embrace Home Automation and Ambient Computing. [Online]. Available: <https://www.idc.com/getdoc.jsp?containerId=prUS47567221> (accessed: Jul. 14 2021).
- [3] Bauer J, et al. ForeSight - An AI-driven Smart Living Platform, Approach to Add Access Control to openHAB In: M. Jmaiel, M. Mokhtari, B. Abdulrazak, H. Aloulou, and S. Kallel, editors. Lecture Notes in Computer Science, impact of digital technologies on public health in developed and developing. [S.l.]: Springer Nature; 2020:432–440.
- [4] Bauer J, et al. ForeSight - Platform Approach for Enabling AI-based Services for Smart Living. In: J. Pagán, M. Mokhtari, H. Aloulou, B. Abdulrazak, and M. F. Cabrera, editors. LNCS sublibrary, vol. 11862, How AI impacts urban living and public health: 17th International Conference, ICOST 2019, New York City, NY, USA, October 14-16, 2019, Proceedings. Cham: Springer International Publishing; 2019:204–211.
- [5] G. Hoppe et al. GAIA-X: A Pitch Towards Europe Statusbericht zu Anwenderökosystemen und –anforderungen. 2020.
- [6] SENSE – Semantisches, interoperables Smart Home. [Online]. Available: <https://www.projekt-sense.de/> (accessed: Jul. 14 2021).
- [7] Aarts E, Wichert R. Ambient Intelligence. In: Bullinger, editors. Technology Guide: Principles, Applications, Trends. Berlin, Heidelberg, New York: Springer; 2009:244-249
- [8] Hanke S, Mayer C, Hoefftberger O, Boos H, Wichert R, Tazari MR, Wolf P, Furfari F. UniversAAL - an Open and Consolidated AAL Platform. In: Wichert R, editors, et al. VDE: Ambient Assisted Living: 4. AAL Congress 2011. Berlin: Springer Science+Business Media; 2011:127-140