2023

A Platform as a Service Framework for Ambient Assisted Living Services

Kuijs, Hendrik Dr.

COPYRIGHT STATEMENT

[1] E.g. in the example of third party copyright materials reused in the thesis.

[2] In accordance with best practice principles such as, Marking/Creators/Marking third party content (2013). Available from: `https://wiki.creativecommons.org/wiki/Marking/Creators/Marking_third_party_content` [accessed 28th February 2022]

UNIVERSITY OF
PLYMOUTH

A Platform as a Service Framework for Ambient Assisted Living Services

by

Hendrik Kuijs

A thesis submitted to the University of Plymouth
in partial fulfilment for the degree of

DOCTOR OF PHILOSOPHY

School of Engineering, Computing and Mathematics

December, 2023

Acknowledgements

I would like to acknowledge the following people for their help during this stage of the research:

Prof. Christoph Reich	Institute for Data Science, Cloud Computing and IT Security, Furtwangen University of Applied Sciences, Furtwangen, Germany
Prof. Martin Knahl	Faculty of Business Information Systems, University of Applied Sciences Furtwangen, Furtwangen, Germany
Prof. Nathan Clarke	Centre for Security, Communications and Network Research, Plymouth University, Plymouth, United Kingdom

In addition, many colleagues have supported me energetically and morally during the process. My role models Frank, Thomas and Stefan, my colleagues in the project Carina, Michael and Timo, my PhD student colleagues Dirk, Matthias, Holger and Jan, and all my friends at work.

I would especially like to thank my family for their support, their willingness to give me space for this work at any time and to encourage me even in difficult phases: Kristin, Jana, Mum and Dad - thank you for everything!

- Dedicated to my father -

Author's declaration

At no time during the registration for the degree of Doctor of Philosophy has the author been registered for any other University award. Work submitted for this research degree at Plymouth University has not formed part of any other degree, either at Plymouth University or at another establishment.

Relevant scientific seminars and conferences were regularly attended, at which work was often presented:

Publications:

C. Fredrich, H. Kuijs, and C. Reich. An Ontology for User Profile Modelling in the Field of Ambient Assisted Living. In A. Koschel and A. Zimmermann, editors, *Service Computation 2014*, volume 5, pages 24–31. IARIA, 2014. ISBN 9781612083377. URL `http://www.thinkmind.org/index.php?view=article&articleid=service_computation_2014_1_40_10014`

H. Kuijs and C. Reich. An Ambient Assisted Living Platform as a Service Architecture for Context Aware Applications and Services. *Proceeding - 1. Baden-Württemberg Center of Applied Research Symposium on Information and Communication Systems*, 1:70–74, 2014

H. Kuijs, C. Rosencrantz, and C. Reich. A Context-aware, Intelligent and Flexible Ambient Assisted Living Platform Architecture. *CLOUD COMPUTING 2015 : The Sixth International Conference on Cloud Computing, GRIDs, and Virtualization*, pages 70–76, 2015. ISSN 2308-4294

H. Kuijs and C. Reich. Towards Privacy for Ambient Assisted Living in a Hybrid Cloud Environment. *Proceedings - 2nd Baden-Württemberg Center of Applied Research Symposium on Information and Communication Systems*, 2:41–45, 2015

C. Rosencrantz, H. Kuijs, C. Reich, B. Weber-Fiori, and M. H.-J. Winter. Entwicklung einer Informations- und Kommunikationsplattform für ältere Menschen. *ENI 2015, IT im Gesundheits-, Pflege- und Sozialbereich: Qualität und Effizienz durch IT*, 2015

H. Kuijs, C. Reich, M. Knahl, and N. Clarke. A Scalable Architecture for Distributed OSGi in the Cloud. In *Proceedings of the 6th International Conference on Cloud Computing and Services Science*, pages 109–117. SCITEPRESS - Science and and Technology Publications, 2016. ISBN 978-989-758-182-3. doi: 10.5220/0005810301090117

C. Reich, H. Kuijs, K. Wallis, and T. Bayer. Architektur zum Schutz der Privatsphäre in AAL-Systemen. In C. Kunze and C. Kricheldorff, editors, *Assistive Systeme und Technologien zur Förderung der Teilhabe für Menschen mit Hilfebedarf – Ergebnisse aus dem Projektverbund ZAFH-AAL*, chapter 2, page 156. Pabst, Freiburg, 2017. ISBN 978-3-95853-362-2

H. Kuijs, T. Bayer, C. Reich, M. Knahl, and N. Clarke. Privacy enhancing data access control for ambient assisted living. In *CLOSER 2019 - Proceedings of the 9th International Conference on Cloud Computing and Services Science*, 2019. ISBN 9789897583650. doi: 10.5220/0007735804480455

H. Kuijs, C. Reich, M. Knahl, N. Clarke, and I. Ognjanovic. The Need for Emergency-Based Access Control in AAL Systems. *2022 11th Mediterranean Conference on Embedded Computing (MECO)*, pages 1–6, 6 2022. doi: 10.1109/MECO55406.2022.9797201. URL `https://ieeexplore.ieee.org/document/9797201/`

Presentations and conferences attended:

Service Computation 2014 The Sixth International Conferences on Advanced Service Computing, May 25 - 29, Venice, Italy

SinCom 2014 1. Baden-Württemberg Center of Applied Research Symposium on Information and Communication Systems, Villingen-Schwenningen, Germany

Cloud Computing 2015 The Sixth International Conference on Cloud Computing, March 22 - 27, 2015 - Nice, France

SinCom 2015 2nd Baden-Württemberg Center of Applied Research Symposium on Information and Communication Systems, Konstanz, Germany

ENI 2015 8. wissenschaftlicher Kongress für Informationstechnologie im Gesundheits–, Pflege– und Sozialbereich, September 28 – 29, Hall in Tirol, Austria

CLOSER 2016 6th International Conference on Cloud Computing and Services Science, April 23 - 25, Rome, Italy

CLOSER 2019 9th International Conference on Cloud Computing and Services Science, May 2 - 4, Heraklion, Crete, Greece

MECO 2022 11th Mediterranean Conference on Embedded Computing, Cyber-Physical Systems and Internet-of-Things, June 7 - 11, Budva, Montenegro

Word count for the main body of this thesis: **37,937**

Signed: Hendrik Kuijs

Date: 20/12/2023

Abstract

A Platform as a Service Framework for Ambient Assisted Living Services

by Hendrik Kuijs

The primary objective of Ambient Assisted Living (AAL) technology is to provide aid and assistance to individuals, particularly the elderly, in maintaining their independence and residing in their own homes and their known environment for an extended duration. AAL technology is becoming increasingly important due to the continuous decrease of birth-rate and increasing life expectancy, leading to a shrinking proportion of younger population in developed countries. This research proposes a cloud-based platform as a service (PaaS) for AAL that enables service providers to deliver services without the need for the user to invest in expensive technical equipment in advance, thus reducing high start-up costs. This hurdle, as identified by both peer groups and service solution vendors, stands as a pivotal challenge demanding resolution.

The PaaS for AAL focuses on adaptation and personalization, as user acceptance of AAL services depends heavily on their situational needs. To provide customization, the PaaS for AAL can dynamically adapt its functionality and presentation of information based on the context of the environment or user, such as the medical state of the user and the condition at home. To store and retrieve information about the user, an ontology-backed database is implemented, and information about the environment is provided through interoperability with existing smart home appliances, directly attached sensors, and external web services.

One of the key concerns of potential AAL users according to a field test during the research is privacy-related. A PaaS for AAL places regulatory demands on protecting the user's privacy and personal information. Consequently, another part of this work focuses on the question of how general data sharing is possible based on the respective context of the user while protecting their privacy: By implementing monitoring, access control, and enforcement of privacy preserving data access, the platform for AAL is further enhanced. The extension of the introduced privacy policy language with context awareness is a significant step towards providing more robust privacy protection in AAL use cases. With a concluding evaluation survey, it can be shown that it allows for more granular control over data access and ensures that sensitive user data is only accessible when necessary and under appropriate conditions.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

The main goal of technology in the field of Ambient Assisted Living (AAL) is to support and assist people in their daily life. Especially for elderly people, this opens up the possibility, that they can stay in their own homes and their known environments longer. In addition to that, another focus is to introduce technological approaches to support the social inclusion for elderly people with reduced mobility in rural regions. A continuous decrease of birth-rate and an increasing average life expectancy lead to a future shrinking proportion of the younger population in Europe and in developed countries globally (eurostat - European Union, 2023). New nursing or day-care facilities are according to Sowa-Kofta et al. (2021) measures that the policy is taking to counteract the trend. Another viable concept is to introduce technology in the known living environment of elderly people to minimize the needed time-span for professional care facilities. And following the findings of Lewis and Buffel (2020), this is also supported by the elderly people themselves.

Completed and current AAL projects are mainly focused on delivering customizable middleware for smart home environments, and the whole computing power has to be installed in the environment itself. If new demanding services are introduced into the smart home environment, the existing computing equipment has to be renewed or extended as well.

The proposed research focuses on delivering cloud-based services for AAL. Cloud computing enables service providers (e.g. caregivers or day-care centres) to provide information, communication, and safety services without having to invest in expensive technical equipment upfront. By delivering services through the cloud, the high start-up costs can be reduced significantly, and it will be feasible for service providers and users to try out new or innovative services without the need of a high up front investment. This flexibility can be provided by a customizable Platform as a Service (PaaS) that is run by the service provider. The core cloud concept of scaling allows the client's virtual AAL system to grow with increasing demands and new features added, while not overloading the overall resources for the provider.

When examining AAL services, one can see that a large part of the functionality is based on customization and is only accepted by users if this customization also fits the situational needs of the users. Besides external influences, personal requirements are a central component for the adaptation of services in AAL environments: The services can dynamically adapt their functionality and presentation of information based on the context of the environment or the user. For example, in one scenario of the proposed solution, the medical state of the user and the outside temperature are considered, and a snow clearance service is ordered for help.

To store and retrieve information about the user (e.g. medical information, interests, or habits) an ontology backed database is implemented. Information about the environment is provided through interoperability with existing smart home appliances, directly attached sensors and external web-services. Based on the input information, the platform can make intelligent decisions and adapt the services' behaviour and feedback to the user. These changes can affect all levels of a service: User guidance and usability, security and data access. This central requirement also places regulatory demands on a project and its implementation: Services must be provided on the basis of protecting the user's privacy and personal information. The General Data Protection Regulation of the European

Union (EU GDPR) (Publications Office of the European Union, 2016, Article 25) underlines this requirement with the two principles of Privacy by Design and Privacy by Default.

When interviewing potential users of systems in the field of AAL (Rosencrantz et al., 2015), one of the key concerns is privacy-related (Dario and Cavallo, 2014, pp. 89 ff.): *"Who will have access to what data and is there a guarantee that these data won't be used in an abusive manner?"* The core request of the proposed platform is security and privacy within the PaaS, which is handled by the platform by monitoring and controlling the security layer and the ontology backed database by data access policies.

Transferred to the technical possibilities of a cloud environment, this initially results in restrictions for implementation. The PaaS is considered to run in a private cloud, as adaptation of the system to the user's need is heavily based on Personal Identifiable Information (PII). The implementation of a private cloud approach has the downside that it will not scale beyond the boundaries of the physical hardware that is used for running the private cloud. For this, the private cloud is extended by services that may run in the public cloud (e.g., third-party cloud providers). This hybrid cloud approach poses new challenges for personalization of services, as personal information is often not allowed to be passed to third parties. Privacy and security constraints have to be considered, and methods for providing adaptation of services while preserving privacy have to be introduced in the PaaS for AAL. The PaaS provides a management interface for pre-configuration and customization to add new services on demand or adjust the configuration of the platform to the user's needs or different environmental settings. As personalization in AAL is based on PII, like health information or personal contact data, the adaptation of these external services has to be made through special configuration interfaces to keep the impact on the user's privacy minimal, while not limiting functionality. These privacy policy constraints have to be monitored throughout the whole lifecycle of a service (during installation, while running or during reconfiguration).

In addition to these technological aspects from a service level perspective, personal data is usually shared through the platform with other stakeholders for AAL. Therefore, the second part of this work is about the question of how general data sharing is possible based on the respective context of the user. The context is not only seen as information about the user, but also as a trigger for information release. And to meet recent legal obligations, policies and methods must be in place to protect the privacy of the user, the older person, at all times.

1.1 Aims of the Thesis

The thesis's objectives can be divided into two main parts: In the first part of the thesis, the core functionalities of a PaaS are elaborated, and the core functionalities are transferred to a platform for AAL. The basic architecture of PaaS for AAL will be presented, and the principal mode of operation and its advantages over previous platform approaches will be discussed.

The subsequent section delves into inquiries surrounding context-aware service adaptation and the safeguarding of the fundamental private information of platform users. The primary aim of this research is to create an access control system supported by a privacy policy, empowering users to dictate which data can be accessed by specific users or services. These user-defined rulesets can be set during installation and changed based on new requirements or events during runtime. What sets this access control system apart is its automatic adaptation to the real-time context during runtime.

1.1.1 Architecture

The architecture part deals with the established technical approaches of AAL platforms and the transition into cloud technology. Special attention is paid to scalability and ensuring service availability.

1. What design considerations are necessary to introduce cloud-computing

flexibility into the AAL services landscape through a PaaS?

   (a) Hypothesis: The basic technology for current AAL projects can also be operated in the cloud.

   (b) Hypothesis: Distributed computing allows local services to be extended or replaced with services in the cloud.

2. Can the benefits of cloud computing bring advantages for AAL to provide scaling and therefore more flexibility for end-users?

   (a) Hypothesis: Scaling and load balancing compute resources in the cloud increase the availability and stability of AAL services.

In the realm of cloud service delivery, alongside its advantages, the paramount consideration remains security. Safeguarding data and systems should consistently underpin the provisioning of services within the cloud infrastructure.

1.1.2 Service Adaptation and Context-Aware Access Control

Given that user context forms the core information for service adaptation in AAL systems, predominantly comprised of user data, any discussions surrounding this domain necessitates a simultaneous consideration of data protection and privacy measures. The research questions of interest are:

3. How can context be used to provide adapted services within the platform while protecting privacy?

   (a) Hypothesis: Adaptation based on PII is crucial for the acceptance among end-users for services in AAL.

   (b) Hypothesis: A privacy policy for data access control with the possibility to treat the context as a central concept can lead to new use-cases for system adaptation.

4. Does a context change have an impact on the user's attitude to privacy?

(a) Hypothesis: During emergencies, individuals exhibit a greater inclination to share personal information with third parties compared to their usual behaviour within an AAL system's regular operations.

(b) Hypothesis: Explicitly set rules for data access control during emergencies are an added value for AAL systems and create trust in the entire system.

The research of the second part is based on results of the concluding discussion of the first part of the thesis, but also has direct impact to service delivery through the cloud.

1.2 Structure of Thesis

Following this introduction, the theoretical foundations for the work are presented.

Chapter 2 introduces AAL, its stakeholders, the economic relevance, as well as context as a key concept. Cloud computing is presented in Chapter 3 together with the main characteristics, the different actors in cloud environments, the economic relevance of cloud computing, and the benefits and risks for moving healthcare-services to the cloud. The benefits and risks for security and privacy of cloud computing is followed by an overview of the current legislative requirements for data protection, as well as the state of privacy in cloud computing and AAL is presented in Chapter 4. Chapter 5 gives an introduction to existing platforms, platform concepts, and discussed approaches of platforms for AAL and marks the end of the fundamental chapters.

Chapter 6 introduces the prerequisites essential for PaaS in the context of AAL by leveraging the outlined existing approaches. Additionally, it elaborates on specific use cases that establish the groundwork for further development and subsequent evaluation. The first part of the implementation of this research is presented in Chapter 7, introducing the architecture of SpeciAAL, a PaaS for AAL services, with its underlying technological approaches. This is done by combining

different existing approaches for AAL systems and the mechanics of the Open Service Gateway initiative (OSGi) framework with a PaaS delivery platform and additional mechanisms for scaling AAL service modules. Functional evaluations of the main concept of scaling are described directly afterwards. This is followed by the introduction to service adaptation in the SpeciAAL platform itself and a field test with users from the target group of this first stage of the research in Chapter 8.

The discoveries from the field test pave the way for the second primary segment of this research: The context-aware approach of data access is introduced in Chapter 9 and the main aspects of the developed context-aware privacy policy is shown. This addition to the platform is evaluated by a survey that is presented in Chapter 10. A conclusion to all aspects of this research, the lessons learnt and an outlook on future developments, and opportunities, is given in the final Chapter 11.

Chapter 2

Ambient Assisted Living

The main topic of this work is the development of a platform for services in the field of AAL. AAL emerged out of technologies which are known as Ambient Intelligence (AmI). As the technological foundation for sensitive and adaptive environments AmI can respond to actions of individuals or real-world objects and cater for their needs.

2.1 General Definitions for Ambient Assisted Living

According to Aarts and Wichert (2009) interaction with AmI ...

Definition 1. *"[...] is expected to result in enhanced efficiency, increased creativity and greater personal well-being." (Aarts and Wichert, 2009)*

The most promising area of innovation for AmI which provides intelligent, unobtrusive, and ubiquitous assistance is seen in AAL. This development is fostered by two social and political phenomena:

The increasing average life expectancy and a decrease in birth-rate lead to a continuously shrinking proportion of the young working population in developed countries world-wide (Department Of Economic And Social Affairs, 2023). Families are getting smaller, and extended families that can care for their elderly relatives are slowly disappearing.

Politics try to compete with this trend by introducing programs for new nursing or day-care facilities (Zander-Jentsch et al., 2019). But without trained personnel and already existing facilities, one key concept is to minimize the needed time-span for professional care facilities by introducing technology in the known living environment of the target group. Surveys indicate that this trend is supported by elderly people who want to stay at home as long as possible (Lewis and Buffel, 2020).

Another major technological field for AAL is seen in Information and Communication Technology (ICT) as new goals are introduced to improve the quality of live for an ageing population (Lupescu, 2009). Older people are motivated and assisted to stay active and participate in their community. This prevents social isolation, promotes societal inclusion, and helps people stay independent and counteracts reduced capabilities which are more prevalent with age.

With a gerontechnological perspective by Blackman et al. (2016) AAL has its roots in traditional assistive technologies for people with disabilities, universal design approaches to accessibility, usability, and acceptability of interactive technologies as well as the AmI computing paradigm as described above (El Murabet et al., 2020). Blackman et al. (2016) developed a taxonomy for different projects in the field of AAL. They divided the existing projects into three generations:

- The **first generation** of AAL is about wearable devices that can track the user's vital functions and can be used to initiate emergency alarms. But the user often has to trigger the alarm himself, and this often leads to false alarm or no alarm at all because the user does not wear the wearable. If the user is incapacitated, it may not be possible for him to trigger the alarm when needed.

- The **second generation** of AAL is about home sensors and the response to emergency and detection of hazards is done automatically. The system can recognize the user, the behaviour, and changes in daily activity patterns over a period of time. The collected data can be interfaced by contextual data,

such as daytime, or weather information. The weakness of this approach is that some users find the embedded sensors in their known environment to be intrusive.

- The **third generation** is an integration of the first and second generation with the addition of services that emerged out of new developments of ICT. Examples would be training devices (or modern activity trackers), that can not only monitor the vitality information and health state of the user, but also encourage him to go on with everyday training or even connect him with other people in a training community. Prevention of emergencies and monitoring of health status is enriched by assistance for tasks in the daily life of the user. It is not only about providing help but also to encourage, support and provide the user with information that will enable him to participate in social activities.

- Advances in Artificial Intelligence (AI) lead to the **fourth generation** of AAL. By introducing algorithms to analyse data within AAL solutions, these sophisticated systems possess the capacity to adapt and improve through learning from data, providing tailored assistance and aid. They adopt a co-design methodology that engages end-users, caregivers, and stakeholders, fostering the development of user-centric and inclusive solutions (Guerra et al., 2023).

AAL projects and services can be divided in four different areas of application (Georgieff, 2008):

- **Health and health care:** This area is focused on health prevention and functional rehabilitation at home. The applications range from remembering assistance systems for medication or exercise programs to emergency systems, that are triggered by sensor data or vitality and movement data of the user.

- **Household and supply:** This includes the growing market of smart home products, that can communicate with other products or external services to

deliver a richer service to the user (Miele & Cie. KG, 2022). Another trend is to re-think user interfaces for a better user experience, by using easily comprehensible displays or implementing help-dialogues to guide the user through complex tasks.

- **Safety and privacy:** Applications in this area range from devices that are secured against accidental operation, and presence detectors to alerting-functionality or automated emergency calls.
- **Communication and social environment:** Technology is used to support social integration by providing easy to use interfaces to get connected to family members, neighbours or other social networks. This initial communication and social inclusion can lead to more mobility and a better access to cultural or leisure activities.

2.2 Components of an AAL System

The European Ambient Assisted Living Innovation Alliance (AALIANCE) is working on a common roadmap for scientific and industrial projects for AAL (Broek et al., 2010). Following their definition, parts of AAL systems can be broken down to five technology areas:

- **Sensing** or metering information anytime and anywhere, whether in or on a user's body, in or on appliances, or in the user's environment.
- **Reasoning** the collected data and transforming them into knowledge in context of the user's life and environment.
- **Acting** based on the transformed knowledge in an automatic, instantaneous or delayed way by multi-modal interfaces in multiple spaces.
- **Communication** not only between sensors and actuators, but also between complete systems that have their own sensors and their specialized reasoning systems.

- **Interaction** between the system itself and the user by coping with specific requirements and the abilities of the user.

2.3 Economic Outlook of Ambient Assisted Living

To discern the relevance for research and development in the field of AAL it is necessary to understand the potential market growth for the next few years.

If you follow the market overview of recent years, you can see a change from a dedicated consideration of Ambient Assisted Living (AAL) as a separate market branch in earlier statistics (Statista, 2016) to a subsumption under the topic area of smart homes (Zavialova, 2022): AAL is primarily assigned to the area of *Security* there, even if it is pointed out that individual products for AAL can occur in all market segments of the smart home market (Smart Appliances, Control & Connectivity, Home Entertainment, Comfort & Lighting, and Energy Management).

The following numbers are worldwide trends based on 152 countries across all continents in the digital market that represent 90% of the world economic power based on the global gross domestic product (Statista, 2022c).

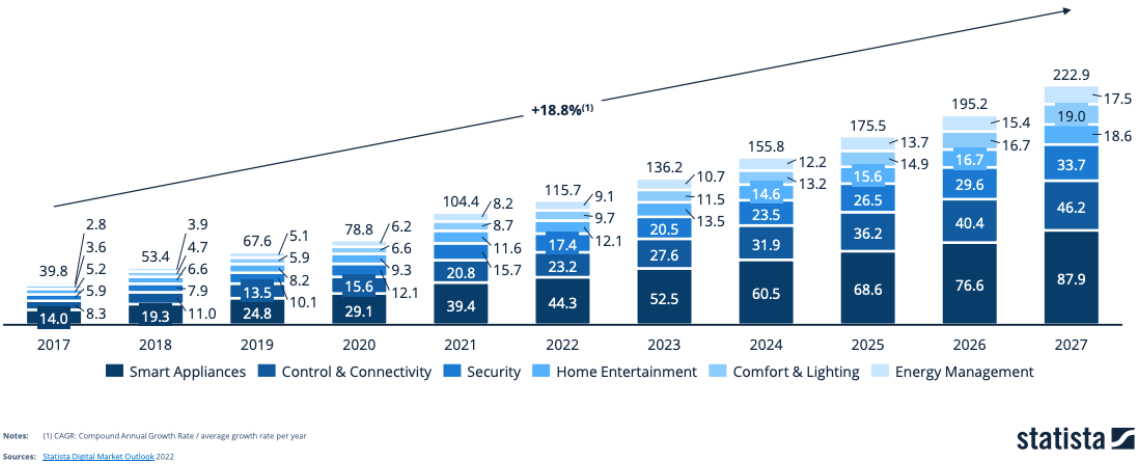

Figure 2.1: Smart Home Market revenue (in billion US$) is estimated to increase at an average growth rate of 18.8% from 2017 to 2027 (Zavialova, 2022)

The Smart Home market is expected to be constantly growing by an average rate of 18.8% worldwide in the next four years (see Figure 2.1) with total revenues rising from 39.8 billion USD in 2017 to 222.9 billion USD in 2027 including *Smart*

Appliances (87.9 billion USD), *Control and Connectivity* (46.2 billion USD), *Home Entertainment* (18.6 billion USD), *Energy Management* (19.0 billion USD), *Comfort and Lighting* (17.5 billion USD), and Security (27.8 billion USD) (Zavialova, 2022).

Accordingly, the total number of *Smart Homes* is also increasing significantly from 140.6 million homes in 2017 to an expected 672.6 million homes in 2027 (see Figure 2.2 (Zavialova, 2022)) as the technological advances and potential lower costs are attracting architects, developers, and device manufacturers.

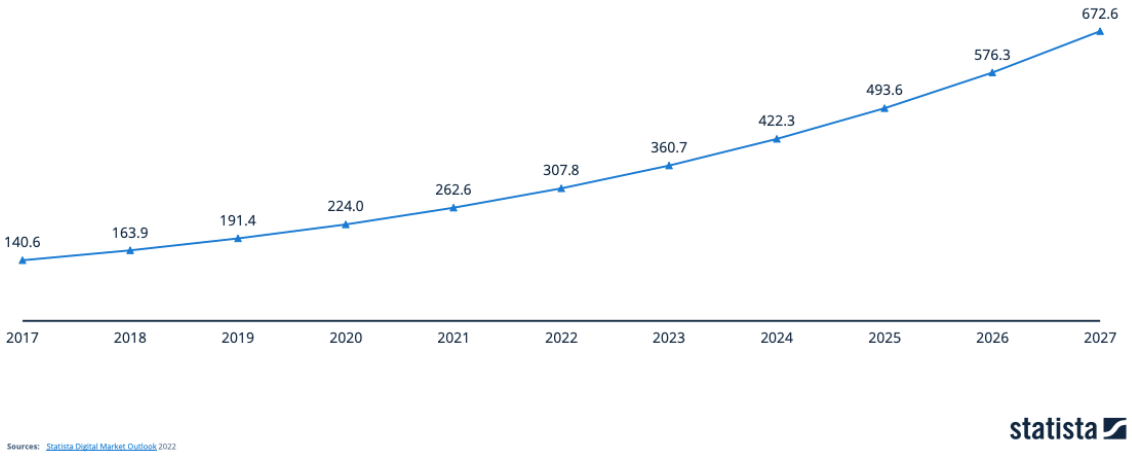

Figure 2.2: The global number of smart homes (in millions) are expected to increase from 2017 to 2027 (Zavialova, 2022)

The market for AAL devices is considered a great opportunity for companies from any industry because its small size in 2016 also means no strong competition. The market forecast also looks good, and here, too, the figures are rising steadily between 2017 and 2027 (see Figure 2.3). While in 2017, 140.6 million smart homes worldwide were equipped with a security component, this figure is expected to rise to 672.6 million smart homes by 2027.

However, according to Zavialova (2022), there are still barriers to adoption, particularly among elderly people who may be hesitant to use digital technology. Usability and simplicity are key factors for companies looking to create AAL products. There is potential for cross-selling AAL products with security devices, and the market for AAL devices is expected to grow as medical treatments improve and the population ages.

The figures also speak a clear language here, as the average household is less and

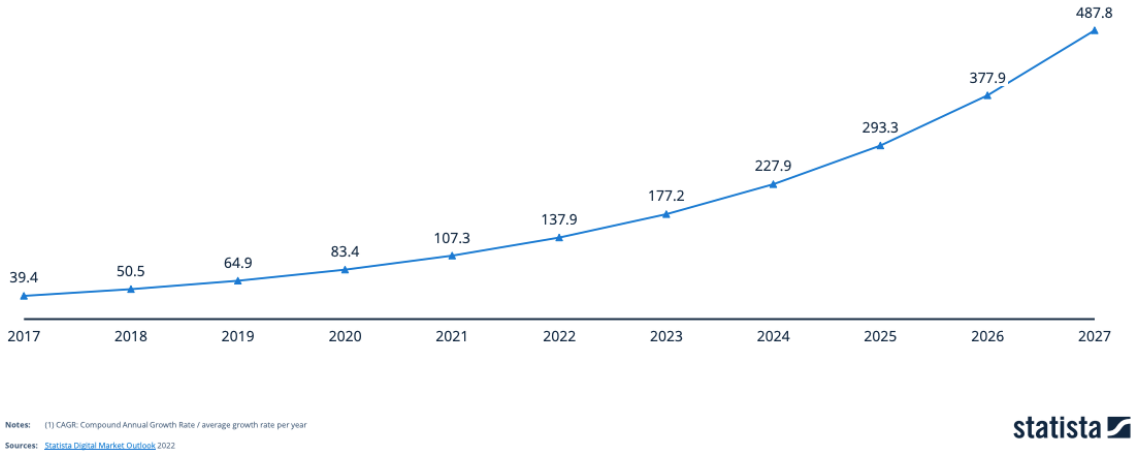

Figure 2.3: Forecast in millions: Security smart homes are estimated to increase from 2017 to 2027 (Zavialova, 2022)

less willing to spend a lot of money on security in the smart home sector by 2027 (see Figure 2.4). The value drops from US$ 158.70 in 2017 to only US$ 69.10.

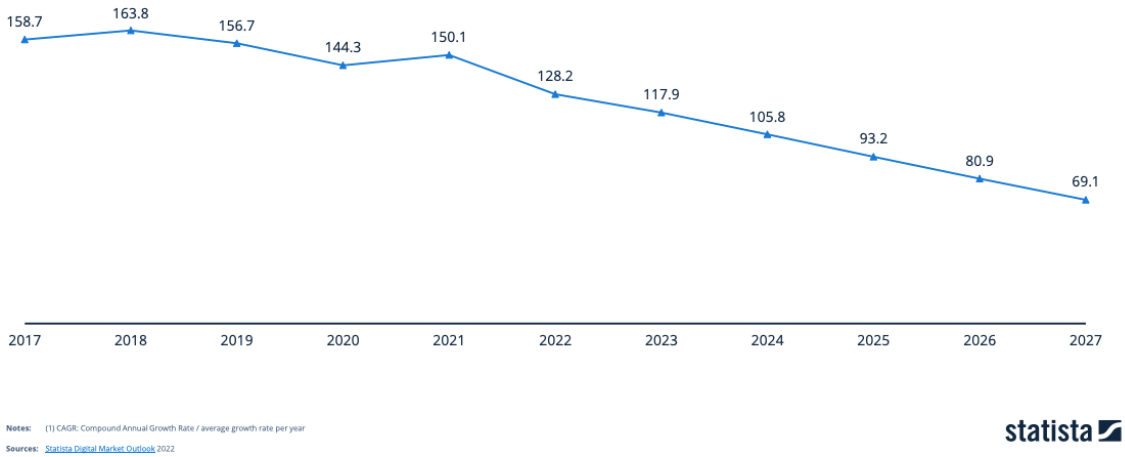

Figure 2.4: Forecast in US$: Average revenue per smart home worldwide (Zavialova, 2022)

But the adoption of AAL devices in both residential homes and other business-to-business (B2B) use cases has significant potential. This trend is likely to continue, as ageing populations in most countries create a need for caregivers that can be compensated for through automation (Zavialova, 2022).

2.4 Stakeholders for AAL

In the updated roadmap of the subsequent project of AALIANCE four main groups of stakeholders for AAL are specified (Dario and Cavallo, 2014). The needs

of each group and the disparate perspective leads to different requirements for projects in the field of AAL.

The **primary group** consists of the **person to be cared for and their informal caregivers**, e.g. direct relatives, unpaid individuals or private caretakers. Depending on the country of the EU, it is expected that approximately 80% of care is covered by informal caregivers (WeDo partnership (2012) and Ambugo et al. (2021)). Although they carry out the majority of supportive tasks for the older person, they often are not supported by the formal care system. The AALIANCE2 Roadmap suggests that this group should be supported by technological and sociological tools and care systems to provide optimal service and make informed, critical decisions in dangerous situations.

Barriers related to the primary group of stakeholder for implementing AAL projects are a certain wariness towards technology in general and the potential necessity to change known habits when introducing new technologies (Broek et al., 2010). These prejudices can be overcome by not targeting single users, but by showing the usefulness to a group of potential users and letting them explore the possibilities for improvement of daily living themselves. But according to Broek et al. (2010) sometimes this is not a viable solution as the presented technology is just not solving the right problems or the design of a solution is not considering the real needs and capabilities of the primary group of stakeholders because it was designed without asking the users, or the solution came first, and the suiting problem was found in AAL.

Apart from the wariness towards technology and the solution to the wrong problems, the third barrier for embracing AAL technology often is the economic expenses of the whole system. The purchasing power of the user sometimes is just not sufficient, and the high costs are not justifiable if the benefits are not clear (Broek et al., 2010).

Care providers constitute the **secondary group** of stakeholders. In a nursing home context, AAL technology should provide activity information to the care provider

about the older person (health conditions, carried out activities, drug taking or rehabilitative activities) and recognize dangerous situations or emergencies. But another area that could benefit from the application of AAL technology is the improvement of service for the older person by having the ability to gather all this information quickly and having more time to spend directly with the older person. In settings where professional personnel for one person in need is frequently changing, the communication between caregivers could also be improved by using an integrated information system and setting up a network between all agents related to the older person's life.

The **tertiary stakeholders** are **vendors** of AAL systems, industries and research institutes. These groups are seen as the driving force for new applications and business models for AAL. According to the Bridging Research in Ageing and ICT Development (BRAID) project (Huch, 2010) they can be listed as the following:

- application oriented research facilities that collaborate with commercial entities, work on research activities that are targeted for fast deployment and often offer access to real-world testing sites
- enterprises that produce ICT devices and develop business cases for AAL applications
- service providers that can integrate newly developed solutions
- telecommunication, cloud, transportation, etc. providers that provide the basis for these integrated services
- system providers that integrate and package alternative solutions
- distributors and vendors

The main challenge for secondary and tertiary stakeholders is that there is no clearly defined target user as each person has different needs, characteristics and skills that have to be addressed (Broek et al., 2010). Moreover, the designers of systems and services have to take in account that these demands may also vary

over time. The systems therefore have to be highly adaptable and configurable to meet the requirements of an evolving person, changed conditions and diversity in infrastructural and social environment. This leads to an involvement of other scientific disciplines such as gerontechnology, gerontology and social science to shift the primary group of stakeholders from care customers to members of a care-giving "integrated" community. On a technological point of view, there is still a lack of standards and references for domain models, open-reference architecture, solutions for unobtrusive and affordable sensing of context, adaptability of advanced user interfaces, guidelines for privacy and security of data management, and interoperability of heterogeneous components. The third main obstacle for system developers is the coverage of broadband networks: People who live in rural areas often remain isolated and cannot participate in AAL projects or use the provided systems, such as social and service networks. The quaternary stakeholders consist of public and private agencies and entities, such as the social, welfare and health care system, policymakers, standardization organizations, civil society organizations, and media (Dario and Cavallo, 2014). Besides the aforementioned heterogeneous target groups (users or buyers) and a lack of standards, there is a vast diversity of social, welfare and health care systems throughout Europe which makes large-scale funding or reimbursement policies of AAL systems impossible. On top of this, the value chains of integrated AAL solutions are invisible, leading to a lack of commitment and engagement (Broek et al., 2010).

2.5 Context in AAL

Many solutions solve problems of home automation, freedom of barriers and emergency diagnosis, as stated in Klein et al. (2007), Litz and Gross (2007) or Botia et al. (2012). But when elderly people need, for example, every day assistance, when they are suddenly mobility-disabled, there is an emerging problem of social contact depletion. Especially in rural regions, it is not simple for older people to keep up their social contacts if they are physically limited. Ordinary things like

meetings with friends, family members, or club members or going shopping aren't possible any more. This leads to loneliness, isolation and often mental health problems (National Academies of Sciences / Engineering / Medicine, 2020).

For this reason, it is absolutely necessary to adapt the user interface of all services but also the service functionality to the needs of each single user. The personalization is important because of the different combinations of impairments and capabilities, as described in section 2.4. Lauriks et al. (2007) define personalization of systems as the key functionality in supportive systems for elderly people and people with dementia.

For adaptation and personalization of a system and its services, it is necessary to integrate context awareness: To offer personal assistance in any given situation, the system must have knowledge about the users' interests, preferences, impairments, capabilities, but also about their actual situation at the present time. To define system-wide knowledge about the situation of a user, it is necessary to define the context. Context as a computing paradigm was first introduced by Schilit et al. (1994).

Definition 2. *"Three important aspects of context are: where you are, who you are with, and what resources are nearby [...]" (Schilit et al., 1994)*

This defines the location of the user and the people and resources that are surrounding the user, or in other words, two classes of information: Locality and identity. In contradiction, Dey and Abowd (1999) define context as follows:

Definition 3. *"Context is any information that can be used to characterize the situation of an entity. An entity is a person, place, or object that is considered relevant to the interaction between a user and an application, including the user and applications themselves." (Dey and Abowd, 1999)*

According to them, context information can be classified into four categories: Locality, identity, activity and time. Without the action, it is difficult to describe a situation of an entity. These four categories are defined as primary context. All

further context information that is derived from the primary context is defined as secondary context (Dey and Abowd, 1999). For reaching personalized assistance, it is essential to centralize the user's needs and include the actual user's environment. Because Dey and Abowd (1999) determine context as both, the user and his environment, this definition is chosen as a basis for this thesis.

The definition of context awareness of Dey and Abowd (1999) is also fitting the main criteria of AAL systems:

Definition 4. *"A system is context-aware if it uses context to provide relevant information and/or services to the user, where relevancy depends on the user's task." (Dey and Abowd, 1999)*

This definition includes systems that provide context-aware information and services to a user (presentation), act independently based on context (automatic execution) or tag information with context for later retrieval (tagging). These three system characterizations are also applying to modern AAL systems, and this definition of context awareness will be used in this thesis.

To build a common technological representation for context within the system, there are different possible approaches (Ehringer, 2009). Strang and Linnhoff-Popien (2004) compared different context modelling techniques: Key-value, markup-scheme (XML), graphic, object-oriented, logic-based, and ontological. They defined several requirements to compare the different approaches, e.g., the possibility of validation of context information based on the context model, the handling of erroneous or incomplete data or the applicability in existing environments. Due to their analysis, they conclude that the most promising assets for context modelling regarding the requirements can be found in the ontology category (Strang and Linnhoff-Popien, 2004).

With the use of an ontology, it is possible to model entities within a domain and the relationships (even complex relationships, like semantic relationships, inheritance, or links) between the entities. Ontologies are at an abstract level so that they are easily understandable to humans but still machine-readable. They

are particularly suitable for the exchange of data or knowledge, since they provide clear definitions of knowledge and thus exclude ambiguities (Ehringer, 2009). Many of the existing AAL systems use ontologies to represent the context for different services. However, most of them consider only the user's environment (e.g., doors, appliances, temperature, location, smoke, etc.), but do not see the user as a central element.

The Service Oriented PRogrammable smArt enviroNments for Older Europeans (SOPRANO) project (Klein et al., 2007), for example, developed an open middleware for AAL solutions. The *SOPRANO Ambient Middleware (SAM)* receives user commands or sensor data, enriches them semantically and determines an adequate system response, which is then performed by the connected actors installed in the living environment. If, for example, SAM receives the information that a window is open, it analyses the remaining context information and can inform the user about the open window, before he is leaving the house. The components communicate over semantic contracts and are based on a common domain ontology. This ontology is designed state-driven, that means that every concept (device, person, location, etc.) of the ontology is represented by its actual state.

Another example considering the environment of the user is PersonisAD (Assad et al., 2007). Some information about the user like his preferences are also part of the consideration of the PersonisAD framework, but aren't detailed enough to reach a good personalization for older people.

Within the scope of the European project VAALID (Naranjo et al., 2009), Mocholí et al. (2010) present a series of ontologies designed to enable AAL service designers in modelling and defining an AAL setting, encompassing the entities, occupants, diverse spaces, and devices involved. These ontologies encompass elements involving interactions among the various components outlined within the modelled AAL solution. These interactions are articulated in relation to the capabilities of each element, documented through the Common Accessibility Profile. The central element of the ontology is therefore the description of the interaction, which takes up a large part of the ontological representation.

The project MobileSage aims to develop a smartphone based help-on-demand service (see Skillen et al. (2012a) and Skillen et al. (2012b)). It means that the smartphone offers context aware, personalized and location aware services supporting the independence of elderly people. Such services could support the navigation, the handling of devices like ticket vending machines or household appliances or other daily tasks. The personalization and context awareness is realized by an ontology, which considers not only the environment of the user but also the user and his characteristics. It is one of the few ontologies in the field of AAL, which models a user profile and the environment of the user. The central concept of the ontology is the user, who is described by his profile. The user profile therefore is divided into sub-profiles like a preference profile, a health profile or an interest profile. But for the help-on-demand services, the focus is still on the environment of the user to offer, for example, services depending on the location of the user.

The publication by Grguric et al. (2015) describes a development method for creating an ontology in the field of AAL. The method is loosely based on parts of the *Methontology* method (Férnandez et al., 1997) that is recommended by the Foundation for Intelligent Physical Agents (FIPA), but is limited to the parts specification, knowledge acquisition, conceptualization, formalization, and integration. The basic structure follows the IEEE Suggested Upper Merged Ontology (SUMO) model (Niles and Pease, 2001), which is extended by submodels: Each data category is given its own ontology. Although this approach makes the ontology extremely flexible, it also makes it very large and complex to work with.

Silva and Alencar (2023) use ontology itself as a tool in the development process. In this study, a central ontology is introduced to facilitate the description of prerequisites within AAL systems and to standardise the integration of the elements inherent to this type of system. Utilizing ontology enables the standardization of associated terms, concurrently validating relationships between elements, thereby assisting designers during the requirement specification phase.

2.6 Conclusion

This chapter delves into the fundamental aspects of AAL by exploring various dimensions crucial to understanding its scope and relevance. It begins with a comprehensive overview of the foundational definitions surrounding AAL, shedding light on its core concepts and functionalities. The discussion then proceeds to dissect the essential components that constitute an AAL system, detailing the intricate elements that contribute to its seamless functionality.

An integral aspect covered within this chapter is the economic perspective of AAL, where an analysis of its financial landscape, market trends, and potential growth avenues is provided. Additionally, the chapter delves into the diverse stakeholders involved in the AAL ecosystem, their characterization as well as known barriers in these groups for implementing or embracing AAL systems.

Lastly, the chapter concludes by emphasizing the contextual relevance of AAL, highlighting the interconnectedness between AAL systems and their operational environments. The discussion of different approaches to context as a technological concept for AAL systems, leads to the introduction of an ontology to model the context of a user. Furthermore, in order to be able to not only adapt the system, but to really personalize it, an approach for creating user profiles and sub-profiles is presented (Skillen et al., 2012b). The thesis is oriented towards this concept in terms of adaptation and personalization.

The presented barriers for stakeholders, in conjunction with market conditions, highlight the significance of considering a PaaS approach in AAL.

Addressing the high costs for users and the risks associated with product development, efforts are needed to standardize various aspects of solutions, enabling the provision of readily available services to a broader audience (Almalki et al., 2022). This standardization can streamline production processes, a tactic already underway in existing AAL systems.

However, the rationale behind considering the migration of these services to

the cloud lies in the adaptability of resources to match the specific consumption needs on the customer's premises. This flexibility allows for a test system to remain compact while a fully operational production system can scale up significantly, eliminating the necessity of on-site equipment procurement or replacements. Nonetheless, this setup enables service providers, such as health insurance companies, to efficiently manage central billing and anticipate requirements at an early phase.

Chapter 3

Cloud Computing

In this thesis, the main ideas revolve around delivering services through the cloud and enabling locally hosted systems to be moved to the cloud. From a technological point of view, cloud computing is seen as a problem solver for scaling effects. From a financial point of view, it takes the risk of high investments in supposedly growing markets. Although these factors appear to be beneficial to all projects, there still are risks that have to be considered and may lead to a perceived loss of control for end-users (see section 8.4.1).

3.1 Cloud Characteristics

The National Institute for Standards and Technology (NIST) defines cloud computing as:

Definition 5. *"[. . .] a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable resources [...] that can be rapidly provisioned and released with minimal management effort or service provider interaction" Mell and Grance (2011).*

Cloud computing is characterized as enabling customers to provision computing capabilities automatically and on their own without requiring to interact with the service provider. The services are available via networks and accessible by

standard mechanisms by heterogeneous client platforms. The computing resources on the provider side can be served to multiple customers in a multi-tenant model and are assigned based on consumer demand. The consumer has no control or knowledge over the location of the provided resources as long as it is not defined or guaranteed by agreements. The elastic provisioning or releasing of resources (sometimes seamless and automatic) according to the appropriate demand often appears to the consumer as an unlimited resource of computing capabilities. These changing resources can be monitored, controlled, and reported to provider and customers to provide transparency of the consumed services (Mell and Grance, 2011).

There are three different service models available (Mell and Grance, 2011):

- When providing Infrastructure as a Service (IaaS) to the consumer the fundamental computing resources, like processing, storage, networks or firewalls are available and the consumer can install any software stack which suits his application. The consumer has no possibility to have an active influence on the underlying infrastructure and limited configuration options for networking devices like firewalls. The provider manages the physical processing, storage, networking, and hosting environment.

- In PaaS environments, the consumer can run their own applications based on fixed or configurable software platforms that are prepackaged stacks of software, libraries, services, and tools. Besides the configuration options of the software environment, the consumer has no influence on the underlying system and hardware stack. The provider manages the infrastructure and middleware and provides development, deployment, and administration tools.

- In the Software as a Service (SaaS) model, the consumer uses the applications that are running on a cloud infrastructure and maintained by the provider. The consumer has no influence on the underlying software stack, system or infrastructure and only limited application configuration options. The

provider manages, maintains and supports the software applications. The software application can be accessed over standard mechanisms by various thin or thick clients.

According to NIST Special Publication 800-145 (Mell and Grance, 2011) cloud environments can be deployed based on four models. A *private cloud* infrastructure is provisioned exclusively for a single organization, but may be shared between different consumers within the organization. Either the organization itself, a third party or a combination thereof may be the owner or in charge of management of the infrastructure. A *community cloud* is used by different organizations with shared concerns, and owned and operated by one or more of these organizations, a third party or a combination of them. A *public cloud* is considered to be available for open use by the public and may be owned, managed, and operated by public or private institutions or organizations and localized at the cloud provider. The *hybrid cloud* deployment model describes a combination of the aforementioned deployment models that are still distinct but bound together by standardized technology that enables portability of data and applications.

3.2 Cloud Computing Actors

According to the definition of NIST (Pritzker and Gallagher, 2013) there are five identifiable actors in the cloud computing reference architecture:

- The *cloud consumer* is a person, or organization that uses service from and therefore is in a business relationship with cloud providers. It is the ultimate stakeholder supported by the cloud computing service. As described by the service models, different usage scenarios are applicable, ranging from using the provided software application for business process operations (SaaS) to management of IT infrastructure operations (IaaS).
- The *cloud provider* is a person, organization, or entity that makes a service available to the cloud consumers. The five activities of cloud providers are

Service Deployment, *Service Orchestration*, *Cloud Service Management*, *Security*, and *Privacy*. As described earlier, a cloud infrastructure or service can be deployed as a public cloud, private cloud, community cloud, or hybrid cloud. The service orchestration is described in a stacked three layer model, with the *Service Layer* (SaaS, PaaS, IaaS) on top of a *Resource Abstraction and Control Layer* (managing access and providing the five main characteristics for cloud computing) and the *Physical Resource Layer* (including physical computing resources as well as facilities, air conditioning, heating etc.) as the base layer of this framework model. Cloud service management includes *Business Support*, *Provisioning and Configuration* capabilities, and *Portability and Interoperability* options. Security spans all layers of the reference architecture and ranges from physical security (e.g. access control to a building) to application security. Cloud providers have to protect the personal information and the personal identifiable information in the cloud system.

- A *cloud auditor* can conduct independent assessments of services, system operations, system performance, and the security of an implementation. Security controls, privacy impact, performance, and compliance with Service Level Agreement (SLA) parameters.

- A *cloud broker* negotiates relationships between providers and consumers and provides a single, consistent interface to multiple differing providers (Liu et al., 2011). Cloud brokers provide intermediation (improvement and value-added services), aggregation (integration of multiple services of multiple cloud providers) and arbitrage (interchangeability of different services with the same capability by different providers) between cloud providers and cloud consumers.

- A *cloud carrier* provides transport and connectivity of services between provider and consumer. To ensure the availability of services, a cloud provider can set up SLAs with a cloud carrier and may have special requirements such as encrypted connections or dedicated networks.

Within this thesis, the pivotal roles revolve around the cloud consumer, embodied by the primary and secondary stakeholders in AAL—specifically, the users, informal caregivers, professional caregivers including doctors and geriatric nurses. Additionally, the cloud provider assumes significance, represented by a charitable organization such as the German Red Cross, constituting the tertiary stakeholder.

3.3 State of Cloud Computing

The Public Cloud market has seen substantial growth recently due to the growing number of cloud users and applications. This growth is anticipated to continue in the future, since the full potential of cloud services has yet to be realized. The U.S., being a pioneer and influential economic power, is shaping the global Public Cloud market. Countries that adopted cloud technology early are following the transition, but with a lag of approximately two years, while late adopters are falling even further behind. As shown in Figure 3.1 the estimated total size of the public cloud computing market will grow by 22% on a yearly average between 2016 (96 billion dollars) and 2027 (835 billion dollars) (Statista, 2022b).

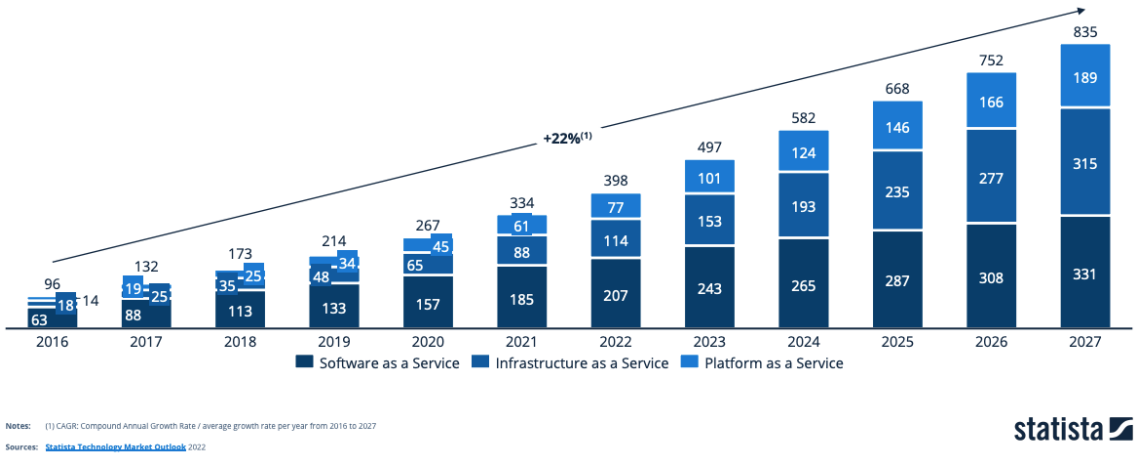

Figure 3.1: The size of the public cloud computing market from 2016 to 2027 in billion US$ (Statista, 2022b)

The largest segment of the Public Cloud market is SaaS, which accounts for over 50% of the market size. The SaaS segment has a low market concentration, as multiple companies offer a wide range of different products. IaaS is the second-largest

segment, which enables easy scaling of physical servers and data centre infrastructure. It is projected to continue growing at a high rate due to the rising demand for new technologies such as Internet of Things (IoT) and AI, which require cloud infrastructure. PaaS is the smallest segment of the global Public Cloud market but is expected to experience the highest growth in the coming years. In the combined IaaS and PaaS segment, Amazon Web Services and Microsoft account for more than 50% of global revenues, leading to a high market concentration (Statista, 2022b).

In a survey among 540 business organizations in 2020 carried out by KPMG and Bitkom Research (the research branch of Germany's digital association) (Statista, 2022a) asking "How important are the following criteria and services when choosing a cloud provider for your company?" 89% stated that "cloud performance and stability" is the most important criteria, followed by "trust in the security and compliance of the cloud provider" with 86%. The third most frequent answer with 75% has been that the "data centre [has to be situated] in the EU legal area". This effect is the result of major changes in case law in recent years: Safe Harbor (U.S. Department of Commerce, 2000)) and Privacy Shield (U.S. Department of Commerce, 2016) both tried to ease the introduction of US cloud services from a legal perspective in European companies, and were both overruled by national law (U.S. Department of Justice, 2018) in the United States. Therefore, US cloud services do not comply with the level of protection required under EU law (Publications Office of the European Union, 2021) and many companies shy away from similar problems when using cloud services from other non-European countries, although there still are foreign countries with an adequate level of data protection (Directorate-General for Communication of the European Union, 2021).

On the other hand, only 54% state that "independence or openness of the cloud provider" is a must-have, but 36% still describe it as nice-to-have. Openness for cloud services can be defined as open code (access code, right to modify and redistribute), open data (data portability, extensible formats, open Application Programming Interfaces (APIs), and open data/data privacy), and open hosting

(reproducibility using standards, no proprietary dependencies, decentralization, and federation) (OneCommons, 2022). The figures for the topic "innovative power of digital tools from the cloud" look similar: 53% of business organizations think of it as a must-have, whereas 44% think of it as a nice to have. 51% describe the "interoperability of the solution from different cloud providers" as must-have and 37% as nice-to-have (Statista, 2022a). It can be a decisive advantage for a company that services from different providers can be combined or even exchanged in order to avoid the effect of vendor lock-in: The vendor lock-in effect describes the loss of governance over one's own data and services used. If data cannot be exported from a system in a standardized exchange format, then it may be impossible to react to price increases or changes in services, for example, and one is at the mercy of the cloud solution provider (The Linux Information Project, 2006).

3.4 Benefits of Moving Healthcare-Services to the Cloud

Moving healthcare services to the cloud offers several advantages for healthcare providers (see Al-Issa et al. (2019) and Peerbits (2023)):

1. Scalability: Cloud platforms allow healthcare services to scale resources according to demand. This flexibility ensures that systems can handle fluctuating workloads, accommodating increased usage without compromising performance.

2. Accessibility and Collaboration: Cloud-based healthcare services enhance accessibility for both patients and providers. Medical records, data, and applications become readily available from anywhere, facilitating collaboration among healthcare professionals and improving patient care continuity.

3. Cost Efficiency: Cloud-based services often operate on a pay-as-you-go model, reducing the need for significant upfront investments in infrastruc-

ture. Additionally, maintenance expenses are often minimized, as the responsibility for upkeep and updates lies with the cloud service provider.

4. Security and Compliance: Cloud providers invest heavily in security measures, offering robust encryption, authentication, and compliance certifications, like HIPAA in the United States (104th Congress, 1996). This can often improve data security compared to on-premises systems, especially for smaller healthcare providers with limited resources.

5. Innovation and Integration: Cloud platforms encourage innovation by enabling the integration of new technologies and applications. Healthcare providers can leverage advancements in analytics, AI, and machine learning to improve diagnostics, treatment, and overall patient care.

6. Disaster Recovery and Backup: Cloud services offer reliable backup and disaster recovery options. Data redundancy across multiple servers ensures that critical healthcare information remains secure and accessible, even in the event of hardware failures or natural disasters.

7. Enhanced Analytics and Insights: Cloud-based healthcare systems facilitate data aggregation and analysis, allowing for comprehensive insights into patient populations, trends, and outcomes. Leveraging cloud-stored data for public health initiatives helps in designing targeted interventions and preventive measures. By accessing comprehensive healthcare information, policymakers, and health organizations can make informed decisions, allocate resources efficiently, and devise strategies to address public health challenges such as vaccination drives, health education campaigns, and community health programs.

Utilizing the potential of cloud computing, healthcare services can achieve heightened efficiency, adaptability, and innovation, all while maintaining the highest standards of security and compliance.

While all of these features also apply to centralized platforms for AAL sensors

and actors are required to be installed in the user's home and there has to be some kind of decentralized gateway for collecting and transmitting sensor data to the cloud platform, as well as triggering hardware actors (e.g. alarms, displays etc.) locally. Yet, this computing resource can remain compact and cost-effective, as the computational strength required to process data into actionable insights resides within the cloud.

3.5 Risks of Moving Healthcare-Services to the Cloud

Moving healthcare and health-related services, like, appliances or systems for AAL, to the cloud can bring numerous benefits, such as improved patient care and operational excellence (Liveri et al., 2021). Cloud service providers have the resources to continuously improve cybersecurity and data protection, making it a cost-effective solution that can cut IT expenses. A step in the cloud can also enhance cybersecurity and data protection, which is crucial since the healthcare sector is highly vulnerable to cyberattacks (Moore, 2020). The COVID-19 pandemic has further accelerated the adoption of Cloud-based technology, such as telemedicine and AI, for triaging purposes. However, this integration also raises concerns about security and data protection. Liveri et al. (2021) define five security challenges for delivering healthcare services in the cloud:

Lack of trust of cloud solutions: Stakeholders in the healthcare sector, including patients, physicians, medical staff, and healthcare organization management, have expressed a lack of trust in cloud solutions. Patients may trust their doctors more than a cloud provider to store their medical data. Meanwhile, medical staff may not be fully aware of cybersecurity and data protection, making it a challenge to raise awareness and provide training on these topics. However, it is crucial for all stakeholders to be aware of the offerings of cloud provider in terms of expertise to prevent human errors and social engineering attacks.

Lack of security and technology expertise: On-site IT staff must also deal with security aspects and new requirements when moving to the cloud. As the market for IT professionals is generally very tight, and it is often difficult to find skilled staff, this is another problem.

Cybersecurity investment is not a priority: Insufficient financial support due to limited public financing or lack of support from healthcare organization management can hinder the promotion of digitalization and impede efforts to increase cybersecurity and data protection maturity in the healthcare sector.

Proving regulatory compliance of the cloud provider: Cloud customers often struggle to determine which cloud provider is compliant with their specific legal requirements, which can limit their options for collaborating with cloud providers. Assessing a cloud provider's compliance can be difficult or require significant financial resources for the cloud customer.

Integration of Cloud with legacy systems difficulties: Integrating cloud solutions with existing healthcare infrastructure is challenging and often results in avoiding cloud services. Legacy systems in the health IT infrastructure are not supported by updates from suppliers, making integration with new technology difficult and vulnerable to cybersecurity attacks.

Another big part of the report by Liveri et al. (2021) are challenges concerning data protection in the cloud. The legal requirements of the EU GDPR (Publications Office of the European Union, 2016) have recently redefined the requirements in data protection for IT systems per se and the use of third-party systems, such as cloud computing services, in particular. In addition to encryption, the transferability of a user's data between systems (data mobility), the deletion of data after a specified period of time, and the clean management of data are requirements that cloud operators and cloud users alike must comply with. However, the most important measure and the greatest challenge for developers and cloud solution providers is the implementation of Privacy by Design (PbD) (see Section 4.6).

The Cloud Security Alliance (CSA) Top Threats Working Group maintains a well-established list of critical security and privacy problems in cloud computing for cloud consumers since 2010. They put "Insufficient Identity, Credentials, Access, and Key Management" at the top in their latest report of 2022 (Brook et al., 2022). This is because access to cloud resources is primarily based on identity. This means that identity has become the new boundary, as it is the primary way to limit access due to the large number of assets, numerous cloud accounts, and users accessing them from various locations.

According to Brook et al. (2022) the sixth item on the list is "Unsecured Third-Party Resources": This term refers to the components, such as APIs, SaaS products, and open-source code repositories, that make up a product or service. These are typically provided by external sources. It is common for digital products to include such elements. If a vulnerability is identified within the supply chain, attackers can exploit it to target all products connected to it. This is referred to as a supply chain vulnerability.

These two risks also come up again and again when talking to end users about cloud systems in general. The reason for this is often reports in the media (compare (Kedrosky, 2021) for insufficient identity management and (Graham-Cumming, 2021) for unsecure third-party resources), which remain particularly present to users and often discourage them from using cloud services without worries.

3.6 Conclusion

Starting by introducing the main cloud characteristics and benefits of delivering services through the cloud, the five cloud-computing actors (according to NIST), and the current statistics concerning the market relevance of cloud computing, were shown in this chapter. This was followed by some insights of current motivations and requirements of German companies for choosing the right cloud providers. Compliance to EU law is seen as critical, while measures against vendor lock-in scenarios and for openness and cloud interoperability are only seen as a

matter of concern by half of the respondents.

The very positive outlook for cloud-computing as technology and business opportunity leads to technological, financial, and social benefits for moving healthcare-services to the cloud.

The final part of this chapter discusses the main challenges of delivering health services through the cloud. The risks of moving healthcare services to the cloud result in requirements for the further course of this research work. Regarding the legacy systems, it should be possible to integrate existing services from the field of AAL by relying on a proven middleware standard (see section 5.1). Another primary goal is to counter the lack of trust (see section 8.4.1) through more transparency in the access control of information about the user (see chapter 9). The latter are always referred to in discussions about data breaches (Arcserve Inc., 2022) and for end users, this is one of the main concerns when discussing the use of cloud computing. A central topic here is the use of PbD strategies, as mentioned by Liveri et al. (2021).

Chapter 4

Data Protection and Privacy

As already mentioned in Section 2.4 and Section 3.5, the greatest obstacle for acceptance and a serious technical challenge for adaptable and personalized systems is the protection of data in general and in particular of PII.

In recent years legal entities, industry, and auditing institutions are implementing mechanisms and processes to build up trust in new services by implementing regulations, guidelines, seals of approval, industry standardization or certifications (EuroPriSe GmbH, 2017). In most developed countries there are already strong regulations that are applicable to all acquiring, storing, processing, or transferring of data.

In this chapter, a short overview of the most important regulations in Europe is presented. After showing approaches currently in discussion to implement this regulations in newly developed systems, special requirements and restraints for the field of AAL and cloud computing are given.

4.1 Personal Identifiable Information

In this work, the definition of personal data is used as defined by the European Data Protection Directive (Directive 95/46/EC) by the Publications Office of the European Union (1995).

Definition 6. *"Personal data shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity." Publications Office of the European Union (1995)*

The 'Article 29 Data Protection Working Party of the European Commission (EC)' further explains in Opinion 4/2007 (Article 29 Data Protection Working Party, 2007) that this definition covers any information that relates to an identifiable, living individual. The differentiation of *directly or indirectly identifiable* is best described by examples: A person's full name and address is an obvious identifier (direct identifier). But a person can also be identifiable from other information, e.g., hair-colour, shoe-size, usual activities, and combinations thereof. If there is too much apparent unspecific information, the information can possibly be combined to meaningful information and an individual can be identified. This definition is also technology neutral - it does not matter how the personal data is stored.

4.2 Legal Requirements

According to section 2.1 and section 1.1 of the German Constitutional Law (Grundgesetz) all citizens have the right to informational self-determination (Rost, 2011). For this, all data within a system must be acquired, stored, processed or transferred in compliance with the user and approved by the user himself.

The Directive 95/46/EC (Publications Office of the European Union, 1995) defines three legally binding requirements that must be implemented in national legislation by all EU member states (e.g., by the Bundesdatenschutzgesetz (BDSG) in Germany):

1. Transparency: An affected person has to be informed if his data is processed. The processing entity has to provide name and address, cause of processing, and the receiving entity of data, to ensure the fairness of processing. The

affected person has the right to access all processed data, to correct erroneous data, or to apply for correction, deletion or blocking of data.

2. Legitimate purpose: Personal data may only be used for an explicit and legitimate purpose. There may be no further processing if it is not in compliance with the original intention.

3. Proportionality: Personal data may only be processed, if they are appropriate, relevant, and not collected excessively based on the according purpose. Data have to be kept exact and if necessary up-to-date. In addition, identification of a person based on personal data should only be possible as long as it is necessary for the specified purpose.

The Organisation for Economic Co-operation and Development (OECD) published guidelines governing the protection of privacy and transborder flows of personal data (Gassmann, 1981). They describe that acquired data about a person are not property of the entity (e.g., a company) that has acquired them, but always stay property of the affected person. Therefore, the company has to request consent before processing data (if there are no different legal obligations). Consent is defined as voluntary written approval, based on an informed decision by a conscious person. In April 2016, the European Parliament, the European Council and the EC adopted the Regulation (EU) 2016/679 or short EU GDPR (Publications Office of the European Union, 2016) to strengthen and unify data protection for individuals within the European Union (EU). The EU GDPR replaced the Directive 95/46/EC and did not have to be implemented by national law, but was effective immediately by May 2018.

4.3 Data Subject Rights

A novelty of this revised regulation (Publications Office of the European Union, 2016) are data subject rights, that define the minimal information a data processor has to provide, and the basic rights of access and possibilities of intervention and

protection of the data subject.

Right of access by the data subject (EU GDPR Article 15) Information provided to the data subject should at least include the purpose, the categories of data collected as well as the recipients of the specified categories and a supervising authority to raise complaints. Additionally, a retention time for stored information, additional sources of information about the data subject and whether an automated decision-making infrastructure is in use to perform profiling tasks based on the collected data. Furthermore, the data subject must be informed about the other rights available to him or her, which are listed below.

Right to rectification (EU GDPR Article 16) The data subject must be able to correct incorrect information at any time.

Right to erasure ('right to be forgotten') (EU GDPR Article 17) Data must be erased upon request under the following circumstances: The data is no longer necessary to deliver the service, withdrawal of consent by the data subject concerning the purpose and there is no other legal ground or the legal regulations prohibit the storing of data.

Right to restriction of processing (EU GDPR Article 18) Apart from legal requirements, all processing purposes (excluding storing data) can be restricted by the data subject.

Right to data portability (EU GDPR Article 20) Collected data can be exported in a machine-readable format to migrate to another service on request of the data subject.

Right to object (EU GDPR Article 21) The data subject has the right to object to processing of personal data at any time, as long as there is no other legitimate ground or legal requirement concerned that overrides the subject's right.

These data subject rights have to be taken into consideration when developing a service and are the minimum legal requirements to all services that are based

on PII. E.g. the database of a service has to be designed for complete deletion of information about one user without interfering the functionality of others and the system operator has to have the ability to export collected data of one designated user for portability and information purposes. If the option for prearranged deletion exists, it can be executed effortlessly. However, certain instances pose challenges to deletion despite this provision. An example is systems that maintain historical data series without considering the retrospective deletion of individual data points. This limitation arises when data, like user behaviour (such as non-anonymized website visits in tracking software), should also be removable retrospectively.

4.4 Privacy by Design and by Default

This consideration in an early stage of developing services is also stressed on in the concept of 'data protection by design and by default'. According to Article 25, Section 1 "the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimization, effectively and to integrate the necessary safeguards into the processing to meet the requirements of this Regulation and protect the rights of data subjects." Publications Office of the European Union (2016)

The technical and organizational measures not only have to be present in the final product, but have to be implemented during the *design* stage of a system.

When implementing these measures, there are three constraints to be considered: The "state of the art, and the cost of implementation" (technological possibility and feasibility), the "nature, scope and purpose of processing" (purpose), and the "risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing" (risk assessment) Publications Office of the European Union (2016).

The Section 2 of Article 25 stresses that *by default* the processing of personal data is always bound to the specific purpose and only necessary data may be processed. This has also to be ensured by technical and organizational measures and is relevant throughout the whole data-lifecycle collection of data, processing, storing, as well as governing accessibility to data. "In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons." (Publications Office of the European Union, 2016)

The PbD framework originated in Canada in the 1990s (Burns, 2017). The Privacy Commissioner of Ontario, Ann Cavoukian, wanted to stop the common practice of applying fixes to privacy relevant bugs after completing a project. The framework should prevent users and developers to privacy-invasive events before they happen.

Ann Cavoukian defined seven foundation principles for PbD. According to these the PbD approach is proactive and prevents privacy infractions before they occur (Proactive not Reactive; Preventative not Remedial), personal information should be automatically protected by default (Privacy as the Default), and measures have to be embedded in the design process and not added later (Privacy Embedded into Design). PbD should not be taken as unnecessary trade-offs, but should rather accommodate legitimate interests (Full Functionality – Positive-Sum, not Zero-Sum). It continuously protects data from time of collection to the secure destruction after the process ends (End-to-End Lifecycle Protection). To assure that a system is working according to its objectives, PbD requires transparency and visibility of implemented components for establishing trust among users and providers (Visibility and Transparency). Finally, PbD protects the interest and needs of the users for managing and protecting their personal data in a privacy preserving manner (Respect for User Privacy).

Once seen as a voluntary concept by developers, the EU GDPR is stressing on PbD and developers have to adopt these foundation principles (Burns, 2017).

A well-documented example in recent years has been the "Corona-Warn-App" in Germany (Robert-Koch-Institut, 2020): Initially planned as a nationwide platform with centralised data storage of movement and encounter data, the application was fundamentally redesigned after major protests from associations and organizations (Chaos Computer Club, 2020). Based on tracking APIs provided by the two major smartphone operating system manufacturers Google and Apple (Apple Inc., 2020) for a limited period of time, the app only stores the user's encounters with other app users on their own smartphone. Keys for users are recalculated daily and only sent to a central location to warn of infection (in the event of a positive test). To warn other users individually, only known keys of individuals encountered are compared and, if necessary, a risk parameter is transferred. The decision to use a decentralised solution with pseudonymous data and the use of cryptographic keys to prevent the creation of user profiles was subsequently defined by the EU as a necessary condition for state infection protection applications (European Parliament, 2020).

In the context of this thesis, these legal obligations center around safeguarding privacy. The subsequent sections of the thesis will concentrate on the principle of privacy by design and by default. For instance, the system only allows initial viewing of the recorded data by the user, and no other service can access it without the user's intervention. Additionally, throughout a service's life cycle (from installation and updates to operation and deletion), the system guarantees that the user consistently receives information about the nature of data being transferred to the service.

4.5 Privacy Enhancing Technology

The stated example of *pseudonymisation* in Article 25, Section 1 by Publications Office of the European Union (2016) for implementing *data minimization* is a good example for supporting a relevant protection principle during design phase by an organizational concept and a commonly implemented technical solution.

These technical solutions are often referred to as Privacy Enhancing Technology (PET). John Borking defined PET as follows:

Definition 7. *"PETs are a coherent system of ICT measures that protects privacy [...] by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data; all without losing the functionality of the data system." Borking and Raab (2001)*

This technology-driven view of a system that prevents personal data by either eliminating it before processing or by protecting it against undesired processing assumes that the data is already present in a system. The measures are there to make sure that misuse is not possible. The European Commission gives a wider definition and introduces the role of PETs already in the design phase of a system:

"The use of PETs can help to design information and communication systems and services in a way that minimizes the collection and use of personal data and facilitate compliance with data protection rules. The use of PETs should result in making breaches of certain data protection rules more difficult and/or helping to detect them." European Union (2007)

Derived from the three classical protection objectives for data security *availability*, *integrity* and *confidentiality* to maintain an operational state in computing infrastructures, data protection specifies these from a users' rights point of view and adds three new protection objectives (Rost and Bock, 2011):

Transparency as a prerequisite to control or regulate technical and organizational processes, and to gain knowledge of the purpose and necessity of processing, the implementation of data minimization, and to satisfy the need for information of users.

Unlinkability to operationalize combination or separation of processes by identifying the pursued purposes and recognizing similarities or differences, as well as the necessity for data processing according to these purposes.

Intervenability as operatisation of the rights of affected users and the ability of

service providers to demonstrate that they can control (and are not controlled) by the system.

To return to the example of the Corona-Warn-App mentioned above, the three additional protection goals can be transferred as follows: Transparency was created on several levels. On the one hand, through the publication of essential parts of the application as an open-source project with the possibility of participation, and on the other hand, through the participation of various social groups. The processes were clearly separated from each other in terms of unlinkability, the data was only used for clear processes and pseudonymised for use. Control over the use of the app and participation in contact tracing was in the hands of the user at all times (intervenability).

Above all, transparency from the aforementioned definition is a key aspect that is pursued in this thesis. The aim is to clearly demonstrate the necessity of processing information and at the same time to protect all data that is not to be processed from access in accordance with the PET definition. For this purpose, a policy language will be developed that is comprehensible to the user and can be easily represented in textual and graphical form, and appropriate access mechanisms will check these policies for each access and implement their enforcement.

4.6 Design Strategies

The European Network and Information Security Agency (ENISA) defined eight technological driven strategies (Danezis et al., 2015) based on the work of Hoepman (2014) to implement PETs to support PbD. The first four presented strategies and examples of applicable design patterns are data oriented and define how data should be handled before collecting, storing, transferring, and processing.

Minimise: To limit the possible privacy impact of any data breach, the amount of PII that is stored or processed should be restricted to the minimal amount possible. This can be achieved for example by thoroughly selecting the real

relevant data for processing (select before you collect), to anonymize data before processing, or by using pseudonyms where possible.

Hide: Whenever possible, personal data, and their interrelationship, should be hidden from plain view. This unlinkability, or unobservability (Pfitzmann and Hansen, 2010) can be accomplished by encryption of data, mix networks (e.g., the TOR Project (Tor Project, 2016) or JonDonym (Jondos GmbH, 2011)), attribute-based credentials, or the use of anonymization of data and pseudonyms.

Separate: To preclude the possibility of generating a complete profile of a person, personal data should be processed distributed, or in separate compartments whenever possible. However, there are no specific design patterns to ensure this at the moment.

Aggregate: To restrict the amount of detail in the personal data of one individual, information should be aggregated over groups of attributes or groups of individuals. "[...] Personal data should be processed at the highest level of aggregation and with the least possible detail in which it is (still) useful." Danezis et al. (2015) Possible design patterns are k-anonymity (Sweeney, 2002), and differential privacy (e.g., aggregation over time as implemented in smart metering environments (Rottondi et al., 2013)).

The following four strategies are addressing process optimization techniques to further enhance transparency of the system to the affected user, control of data processing, and intervenability of systems.

Inform: Data subjects should always be informed about which information is processed, for what purpose, and by which means when using a system. This necessary information includes the ways of data protection, the overall security of a system, possible sharing of data with third parties, and personal data access rights. This strategy is supported by different policy languages, mechanisms, and frameworks, e.g., Platform for Privacy Preferences (P3P)

(Cranor et al., 2006), SecPAL for Privacy (S4P) (Becker et al., 2010), or SIMple Privacy Language (SIMPL) (le Métayer, 2009). For informing about misuse, data breach notifications are also applicable privacy design patterns.

Control: To gain user consent for processing of personal data, the user has to have agency to view, update or delete personal data at any given time. Above this, a user can control and define the data that is processed and whether to use a certain system. Design Patterns for establishing consent are a user-centric identity management, and end-to-end encryption support control. An example of intervenability is a sensor in a smart home environment that can be deactivated during a visit of friends for privacy reasons. Other examples are applications on mobile phones that ask for permission to access the camera roll or the microphone during installation (Google, 2022).

Enforce To ensure that a privacy policy is in place, there should be always one enforced by default that is compatible with legal requirements. This strategy can be implemented by access control, sticky policies (Pearson and Casassa-Mont, 2011), or privacy rights management.

Demonstrate To be able to show how the privacy policy is effectively implemented within the IT system, a data controller is required to demonstrate compliance with the privacy policy and any applicable legal requirements. This can be achieved by implementing privacy management systems, logging, and auditing frameworks.

In this thesis, the three transparency-enhancing techniques *inform*, *control*, and *enforce* are directly implemented by the description of a service (inform a priori), the system's monitoring interfaces (inform a posteriori), the newly developed policy-language and its user interface (control), and the defaults of each policy (enforce).

4.7 Characteristics of Data Protection

In a recent report titled "Rethinking Privacy Self-Management and Data Sovereignty in the Age of Big Data" by Center for Democracy and Technology (CDT) , de Mooy (2017) describes the different characteristics of data protection in the United States, Europe and Germany. Where the United States follows a sectoral approach (the context defines the legal parameters, following a self-regulatory framework with guidelines by best-practice organizations, and the Federal Trade Comission (FTC) as consumer-protection agency), data protection in the EU is built on rights and norms (protecting broader individual rights by normative standards for fair and legitimate data processing, with the core principles of Privacy by Design and Privacy by Default). The responsibilities are shared across member states and enforced in multiple jurisdictions. German laws follow these directives, but also go beyond them by coining the term informational self-determination (ISD): The value of a person being in control of their information. This constitutional guarantee of confidentiality is a technology-specific approach and directly derived from the human rights (de Mooy, 2017).

When developing a system in the field of AAL in Germany, this characteristic of data protection sets the common ground to implement privacy related tools. Every person should be defined as a self-determined user who has sovereignty over their personal data at all times. However, in the case of home care, this also creates a conflict, as it must be ensured that every user has the ability to make the necessary settings or that the system makes it so easy for every user that the system is suitable for everyone.

4.8 Digital Sovereignty

In the recent past, the term digital sovereignty (sometimes also digital self-determination) has entered the discussion on privacy. Although there is no fixed definition of the term digital sovereignty, two aspects are usually associated with it:

1. the self-determined use of digital technologies. E.g. through independence from manufacturers, data mobility concepts (State of Lower Saxony, 2020) and - in accordance with the EU GDPR - the protection of rights to one's own data

2. the competent and secure use of digital technologies; a digital know-how that has been sharpened and constantly expanded in practice, e.g. through digital education and investing in science projects (Ministerium für Wirtschaft, 2022)

Both aspects can be applied to individuals, to companies or even states and supranational institutions such as the European Union (Celeste, 2021).

Applied to the thesis, both statements are valid in relation to an individual person as a user. With regard to the second definition, however, the question remains as to how it can be possible to convey the know-how in dealing with new technologies at an advanced age or with physical or cognitive limitations and thus build trust in the technologies.

4.9 Data Privacy in Cloud Computing

The ITU-T Technology Watch Report of March 2012 (Guilloteau and Mauree, 2012) describes three main challenges to privacy in cloud computing:

Complexity of Risk Assessment: Concerning the risk assessment, there are several questions that are often hard to answer for cloud customers, including who is involved in processing and the roles and responsibilities of these entities, where the data is kept, processed and replicated, what are the relevant legal rules, and how all the expectations can be met by the service provider. By collecting data of customers, and keeping these data for an indefinite timespan, the FTC assumes that companies can introduce usage scenarios for these data in the future that are not compliant with the original purpose of the data collection (Federal Trade Commision (FTC), 2012). This can only be omitted by regulating retention periods for personal data. According to

the ITU-T the top security concerns are still data protection and regulatory compliance for chief information officers (CIOs). The main reason of concern are data breaches or disclosure of data to third parties, pursuing fraudulent, commercial or political motivations (see 3.5).

Emergence of new business models and implications for consumer privacy: Because storage offerings are getting cheaper in cloud environments, the data retention times are getting longer and some business models are working towards indefinite keeping of data. This leads to the urge to create new services based on these vast amounts of data to further lower the cost and leverage the use of data. As retention times and the pressure to build new business models often are not transparent to end-users, privacy is seen as a matter of concern. But the usage of cloud services by end is still growing nevertheless. Another lack of transparency for the user is loosely connected SaaS offerings that feel like a single application but are operated by different companies and may have different terms and conditions. (Federal Trade Commision (FTC), 2012)

Data Protection and Regulatory Compliance: The two top security concerns according to CIOs are data protection and regulatory compliance. E.g. may disclosure of data from a cloud provider to third parties have disastrous consequences for companies. Although security breaches and data theft are not cloud-specific, the benefit for an attacker is raised with the amount of data processed in cloud environments. This leads to a negative impact on the confidence of cloud offerings. Regulatory compliance can be a challenge for cloud services in two ways: Accumulated data may be used in harmful ways by an authoritarian society, on the other hand, companies often have little control where data is physically stored at a given time. Cloud providers therefore should protect data with encryption to unauthorized access. The EU imposes additional requirements on the storage and processing of data in third countries in this regard (Federal Trade Commision (FTC), 2012).

Since August 2014, the main standards of protecting PII in cloud computing are stated in ISO/IEC 27018 "Security techniques — Code of practice for controls to protect personally identifiable information processed in public cloud computing services" (Fumy et al., 2014) in combination with ISO/IEC 27002 "Code of practice for information security management" (ISO/IEC 27001, 2013): Personal data may only be processed in accordance with customer specifications. ISO 27018 requires that cloud providers offer tools that help their customers to provide, modify, delete, and correct end-user access to personal data. Cloud providers have to define processes, specify the return, transmission, transfer and deletion of personal data. The transfer of data to law enforcement authorities may only take place in the case of a legal obligation. The affected customer must be informed of the legal obligation, unless this information is legally prohibited. Personal data are not to be used for the purposes of cloud providers. Before personal data are used for marketing or advertising purposes, the customers have explicitly to give their authorization to do so. Cloud providers have to disclose the countries in which processing of personal data takes place. In case of any data security violation, cloud providers must provide cloud customers with the information needed to comply with their notification obligation, and the time, nature and consequences of the data security violation shall be documented.

All these rules have a common purpose: To restore trust in cloud computing and cloud providers, and to provide tools to enhance transparency for customers and end users in a complex cloud computing environment. As an example, the project Accountability for the Cloud (a4cloud) (a4cloud, 2016) tries to implement a Transparency Enhancing Tool (TET) based on the aforementioned regulation and standard with two goals in mind: Privacy preservation and usability. They developed design principles and showed examples for usable privacy policies for cloud environments (Fischer-Hübner et al., 2014) derived by a stakeholder workshop and legal analysis. These policies are later used in a first prototype of a TET to enable end users to track their personal data.

The same approach as for cloud providers from an industry perspective can also

be applied to AAL systems from an end user perspective. Ultimately, it is always about trust in the technology, which is hard won and can be lost quickly.

4.10 Privacy in Ambient Assisted Living

Regarding AAL, the picture is also mixed for the protection of privacy. According to Rost (2011) AAL environments can be narrowed into three different models:

(A) The user (or a familiar person) controls the sensors and evaluation of the data and makes the decisions as to when and how an action has to be triggered. The data remains exclusively in the access of the user (or the familiar person). The AAL deployment paradigm is essentially the use of an observation system to increase comfort in the sense of home automation, which attempts to adapt itself automatically to the needs of the user.

The user has full sovereignty over the system and the data.

(B) The user commissions a professional observer to provide an AAL service (e.g., a security service, a nursing service, a doctor or a hospital). The participating organizations have access to the sensor data (or even deeper access to, for example, configurations of the system generating this data) and can also initiate differentiated actions, such as calling the affected parties back, or accessing the video surveillance In the rooms of the person concerned.

The data (raw or already processed) leave the users' environment and become operationally (but not legally) the disposable mass of the professionally acting observation and evaluation authority.

(C) Professional observers who process anonymized sensor raw data, which they have captured or received by third parties according to model B, for their own purposes. The foreseeable prospective buyers of such data may be statistical offices, insurance companies, safety authorities, scientific institutes of the medical, nursing or social sciences, as well as system manufacturers for AAL components.

Mixed models from models A and B, such as the setting up of escalation stages, with the pre-examination of an alarm by a confidant of the person concerned, can then be envisaged, as well as the start-up of assistance measures by nursing service providers.

It is obvious that in model A, the specific data protection objectives transparency, unlinkability and intervenability are much easier to implement than in model B. From data protection's perspective, model A is therefore unproblematic because the affected person is fully controlling all activities and data generation. In model B, on the other hand, extensive contracts must be set up and safety precautions taken to protect data storages and data flows against unauthorized access and unintentional or unauthorized evaluations (in particular if, for example, intervention, vitality or behavioural data is transmitted). It is mandatory that only those components which meet certain interface and protocol standards, which are certified according to data protection and data security, and which have been tested and approved by a trustworthy authority are implemented.

According to Rost (2011), a particular challenge will be, which instance is assumed to have the overall responsibility of an AAL installation or how the responsibilities for individual components can be divided.

In project reports concerning already deployed AAL systems, privacy protecting mechanisms are not a thoroughly discussed subject. This could be since the existing platforms mainly belong to model A. But even complex representatives like Universal Platform for Ambient Assisted Living (UniversAAL) (Sadat et al., 2013) have little documentation about their privacy preserving efforts. The project SmartAssist (Rothenpieler et al., 2011) discusses low-level possibilities to protect sensor networks from data breaches by using common encryption techniques, noise signals to keep data safe or TETs to keep their users informed what data is transmitted to what services.

The Breathe project states in "White Paper on AAL System and Associated Privacy Issues" (BREATHE Project Consortium, 2015) that they are focusing on four factors

to enhance privacy and security in their cloud-based video monitoring platform:

1. Integrity: Verifying data transmissions (by checksums).
2. Authenticity: Proof of data source (by ID of source).
3. Confidentiality: Encryption of sensitive data.
4. Multi-Level User Control: Protection of sensitive data by user control.

They are introducing context-aware privacy levels for video capturing within a user's home by evaluating identity, appearance, location, activity and the identity of the observer and deciding which level of detail the video system is allowed to capture. The collected data can be represented for monitoring purposes by different context-aware visualization levels, and the user can always deactivate the system at will.

According to Memon et al. (2014) privacy preservation is not yet seen as a quality attribute of AAL systems. Although security (encryption and access control) is of importance for acceptability among the end-users, other major quality attributes are usability, reliability, maintainability, efficiency, safety, accuracy, and dependability.

Braun et al. (2016) show in their study that the target audience emphasize that they have a sense of shame when confronted with a video system, but are at the same time willing to accept sharing of personal data with other entities in AAL environments. In their view, this could be due to the abstract nature of the term data privacy, but the immediate feeling of shame. However, a loss of data to criminal subjects is seen as a real threat by the target audience.

van Heek et al. (2017) directly focus on data security and privacy in their study. Although the average needs for data security and privacy were on a moderate level with regard to all interviewed participants, they stated that they wanted to have control over the access of their data, see data security as an important attribute for AAL, and realize the possibility of abuse of leaked data. The own

privacy of the participants is as important to them as the privacy of others, and they want to control their own privacy.

In a study conducted by Wilkowska et al. (2022), which investigated the acceptance of sensors in people's own homes, participants emphasised that the security of their privacy was more important to them than their health. The protection of privacy should therefore be the most important priority in the development and implementation of AAL systems. On the other hand, they said they would be more willing to disclose private information about themselves to informal and professional carers if it could protect them from becoming seriously ill. A large proportion of them also stated that they would make their data transparent if they were in acute danger.

Stutz et al. (2016) define measures that have to be implemented by system developers and providers to support data protection and information security in AAL systems. Their work is based on the approach of Privacy by Design and by Default by Cavoukian (2010), that is also included as a central concept in the EU GDPR (Publications Office of the European Union, 2016). They propose a consent-based system where a user has to be informed about the data usage and no data is allowed to be transferred, stored or processed without the consent of the user.

4.11 Conclusion

Data protection and privacy is one of the most important objectives for systems which are subject to the EU GDPR, and often referred to as the major acceptance factor for broad adoption. In this chapter, the concept of Personally Identifiable Information (PII) was introduced, legal framework conditions were derived, and the primary concepts of Privacy by Design (PbD) and Privacy Enhancing Technologies (PET) were discussed. Further elaboration on the design strategies and implementation approaches will be provided as the work progresses. It concludes with a discussion of current data protection concepts in the two areas of cloud computing

and AAL. PbD, in particular, is taken up again in the further course and represents an essential aspect for the architecture of the platform and the requirement for the privacy policy. Part of the work of Wilkowska et al. (2022) is directly considered for the contextual access control system that will be implemented later: Users can set special access control rules for emergencies while maintaining privacy during normal operation of the system.

Chapter 5

State-of-the-Art in Platforms for AAL

As described in Section 2.1 the second generation of AAL introduced home sensors to recognize the user, the behaviour, and changes in daily activity patterns over a period of time. To integrate different sensors, combine sensor data into meaningful and interpretable information, and calculate according system responses, many smart home projects emerged. The second step towards platforms for AAL have been independent and extensible middleware systems.

AAL architectures are the technological successor of smart homes with interconnected sensors, actuators, computers, and other devices in the environment (Haigh and Yanco, 2002). Although nowadays, smart home is a synonym for comfort, leisure and security functions, the original focus lies on assistance and monitoring elderly people in their home environment. Due to the complexity of the first systems, the main controller was often referred to as a black box and interconnecting it with other or new systems was not possible or feasible [(Korff, 2013). Different projects try to open up or standardize the functionality of the middleware to create a common basis for future AAL projects and to provide a centralized management platform and distribution platform.

One of the first projects, that put its focus on a way to adapt to newly developed devices and integrate them into an entire system, has been the *Gator Tech Smart House* by Helal et al. (2005). In their approach, a *Programmable Pervasive Space*

can be constantly extended with new emerging technologies. Devices in the physical layer are converted to software services by the platform, that can then be programmed or merged with other services to create complex applications.

A problem according to Alam et al. (2012) is the technological limitations of early projects: The introduced technology is visible for the user and not "ambient" enough, that a user can easily forget about it and go on with his life like before. According to them, the main goal should be to optimize systems to the user requirements, but without the need for the user to adapt to the system.

Memon et al. (2014) define the role of an architecture for AAL as follows:

Definition 8. *"[...] An AAL solution is an integrated system-of-systems composed of systems, subsystems and components, providing a part of the overall AAL system and its services. The architecture defines the distribution and relationship among the AAL systems, subsystems and components." Memon et al. (2014).*

To achieve that a collection of systems, subsystems and components becomes a coherent system, the architecture needs a connecting element or a common language. In AAL systems, this connecting element is the middleware technology. This crucial component serves as the intermediary layer that enables seamless interaction between diverse devices, sensors, applications, and services within the AAL ecosystem. The middleware acts as a bridge, orchestrating data flow, managing communication protocols, and ensuring interoperability among disparate elements, thereby forming the backbone of the entire AAL framework.

5.1 Middleware in Ambient Assisted Living Systems

Many of the currently developed solutions rely on integration in a networked environment connected to a middleware, that connects and translates management operations to the different sensors, actuators, and devices. Earlier projects, such as the aforementioned Gator Tech Smart House, used specially developed middleware technologies. However, this either requires customisation when im-

plementing new functions or, in the case of very generic middleware interfaces, can mean that not all functions of a new service can be used.

The AALIANCE consortium (Dario and Cavallo, 2014) recommends using a modular and open approach for new services and software in the field of AAL. For remote management for software upgrades and installing new software to an existing platform, the OSGi (The Eclipse Foundation, 2015) is considered one of the possible solutions for middleware. The central feature of OSGi is the possibility to include, update, start and stop applications or services as bundles during runtime without the need for a restart of the whole environment or connected services. On top of this, the specification enables for automatic dependency resolution and remote bundle stores, that work as libraries of installable services. Therefore, it is adopted in different AAL architectures and many developers are delivering their applications or device-drivers as OSGi bundles with well-documented interfaces and requirements.

Different projects open up or standardize the functionality of the middleware to create a common basis for future AAL developments and to provide a centralized management platform and distribution platform. The following section describes the historical development of various projects, some of which build on each other.

5.2 Architectural Approaches

The Ambient Intelligence for the networked home environment (AMIGO) project (Janse, 2004) developed an architecture that is based on a middleware, that operates across different application domains and across different homes and environments. The Amigo architecture comprises several key layers, including a foundational middleware layer, an intelligent user services layer, Amigo-aware applications, and a programming and deployment framework. The middleware layer and user services layer cater to the specific functionalities required for a networked environment and an ambient in-home network, respectively. At the topmost tier of the architecture, Amigo-aware applications and services reside, while the

programming and deployment framework empowers developers to craft diverse applications and services. To demonstrate its potential, they developed the *Amigo Community Sharing Services (CHESS)* that uses web-services to communicate or share time together with relatives. Most of the applications are web-based and can be accessed by any device with a web-browser. The main focus of the middleware lies on automatic device and service discovery within the home network, and the architecture and the architecture is primarily aimed at device manufacturers and system integrators.

Middleware platform for eMPOWERing cognitive disabled and elderly (MPOWER) created a middleware based on OpenESB (OpenESB, 2023) with a strong focus on rapid development of applications by implementing standards-based web services in the home domain (Walderhaug et al., 2007). The system supports the interoperability between profession and institution-specific systems (e.g. Hospital Information System). It supports secure and safe social and medical information management, and addresses the need of mobile users (e.g. professional care-givers) which often change context and tools. The service is designed so that the conversion of messages into other standards is possible by providing a suitable XSL-Transformations. This allows data to be exchanged with other systems and actions to be initiated.

The Ambient Intelligence Reference Architecture (AmIRA) project by Berger et al. (2007) shows in a very abstract way how the parts of an AAL system interact and which underlying modelling is necessary for this. As shown in Figure 5.1 the main part is divided into two modules. The foundational element known as the *Perceiving and Understanding* building block relies on sensors and diverse data sources to gather information regarding the present condition of the pertinent environment. Examples of these sources include sensor systems like positioning systems and other data repositories such as timetable data. Its primary role involves the integration of this diverse data into a unified world state, a process known as world state integration. Subsequently, it utilizes this integrated perspective to identify and comprehend relevant situations, a task termed situation

understanding. The *Reasoning and Acting* building block is rooted in the Situation

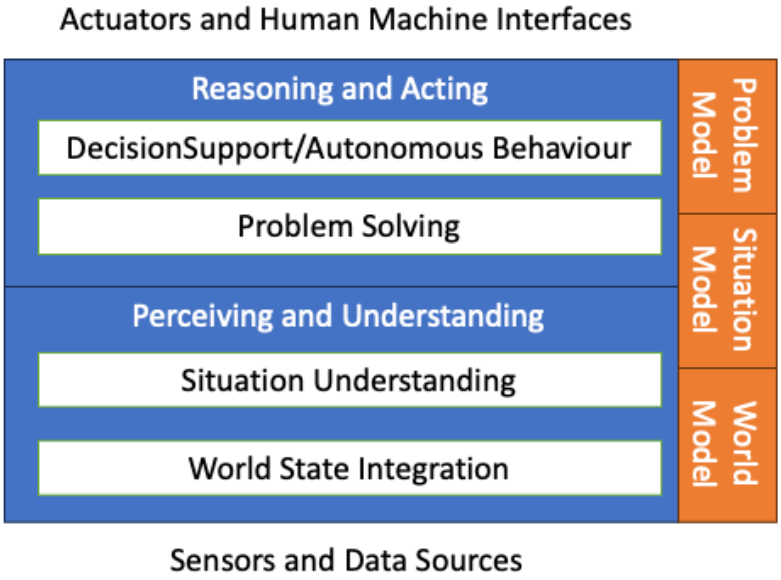

Figure 5.1: The Ambient Intelligence Reference Architecture (AmIRA) (Berger et al., 2007)

Understanding layer, which furnishes details on both current and past situations, encompassing discrepancies and discordant states. Leveraging this information, it engages in application-specific and situation-dependent problems solving. The solutions derived serve as the foundation for furnishing decision support to users and executing autonomous behaviour. To implement decision support and autonomous behaviour, human-machine interfaces and actuators play a pivotal role. All decisions depend on three models that build on each other: The world model, which describes the state of the overall system, the state model, which describes what is currently happening, and the problem model, which describes a problem to be solved.

The SOPRANO project (Balfanz et al., 2008) developed an open middleware for AAL solutions with another object of research: The *SOPRANO Ambient Middleware (SAM)* enriches user commands or sensor data semantically and determines an adequate system response, that is then performed in the living environment by the connected actuators. The middleware was introduced together with guidelines to develop new services or integrate actuators and sensors by Schmidt et al. (2009). These guidelines apply for different stake-holders that are keys to success for sys-

tems in the field of AAL: These are developers of actuators and sensors, providers of value-added services, solution developers and care providers, relatives or the users themselves. The semantic interpretation of actors, situations, and states is based on a powerful ontology, which was taken up by other platform developers in the further course of development.

The Feelgood System (Hietala et al., 2009) provides a middleware for exchange of personal health records (PHR) with different institutions and patients.

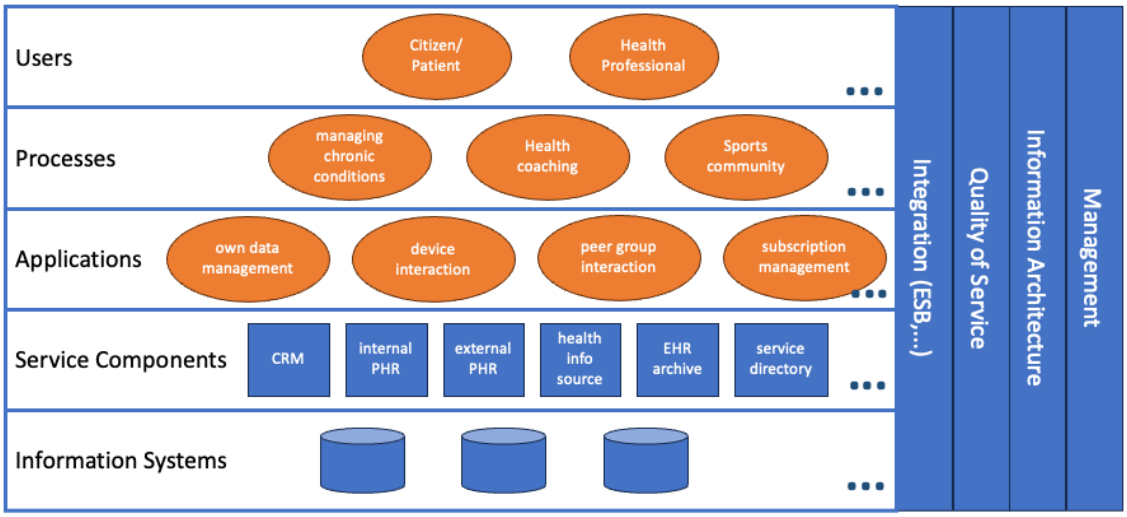

Figure 5.2: Feelgood reference architecture for PHR services (Hietala et al., 2009)

Figure 5.2 illustrates the Personal Health Record (PHR) reference architecture. At the foundational level lies the enterprise's information systems along with fundamental services. Moving up to the second layer, one finds service components that may exist both within and outside the enterprise. These service components serve as essential elements utilized by applications situated on the third layer. Applications on the fourth layer are accessed by a set of processes. Above that, the fifth layer comprises users, broadly categorized into citizens and professional users. These vertical layers are responsible for managing communication between different layers, ensuring quality of service, aligning information structures, and overseeing management services such as security management.

Realizing that AAL systems get too diverse and cannot be provided as commercial-of-the-shelf (COTS) solutions (as has also been demanded in the course of standardisation attempts by Memon et al. (2014)) the follow-up project of SOPRANO

by Balfanz et al. (2008) is OpenAAL an open middleware for AAL projects (Wolf et al., 2010). They propose easy implementation and configuration of situation-dependent and context-aware personalized AAL services and try to cope with the diversity in AAL systems. The middleware is based on OSGi and can be used to introduce loosely coupled platform services. The proposed *Business Process Execution Language* is introduced to process the captured sensor data and situation inputs in an ambient environment and provide adapted services by ontologies-based reasoning of information.

Wartena et al. (2010) developed Continua, a system that consists of:

- the Personal Area Network (PAN) Interface for communication within the proximity of an individual
- the Local Area Network (LAN) Interface for communication within a specific location or facility
- the Wide Area Network (WAN) Interface for communication from home/office/facility to backend service providers
- the Health Reporting Network (HRN) Interface for reporting to enterprise systems like hospitals or telehealth service providers

The Open architecture for Accessible Services Integration and Standardization (OASIS) project (Jaszczyk and Król, 2010) focuses on an ambient intelligent (AmI) framework with software-agents based upon an *OASIS hyper-ontology* as common language. The ontology can combine multiple ontologies in the same application domain or different domains. The *OASIS System* consists of the *AmI Framework*, based on software-agents, and a *Interaction Platform* with a user interface to combine new sensor data to new services and the ability to self-adapt to different devices.

ProSyst delivers a framework for eHealth scenarios based on OSGi to manage sensors and devices over different protocols (Petzold et al., 2013). The management software (*mBS Smart Home*) is installed at the user's home and able to be adopted

to already installed sensors or actuators. It delivers applications for predefining home automation scenarios, notification of specific events and configuring interfaces for collecting data of installed sensors. On top of this, it is possible to deploy domain-specific applications for eHealth. ProSyst offers a backend (*mPower Remote Manager*) for remote management of services and applications: These can be installed, updated, started, stopped or deleted remotely through a Software Management service in the backend. The backend is installed off-site and connected via LAN or internet over a secured connection. Developers are able to use a *Software Development Kit* for new applications in the Smart Home environment. The *mBS Smart Home* and *mPower Remote Manager* are considered to be closed source.

Another attempt is to merge promising or already successful partial solutions with different technical requirements into one big and flexible framework. The project UniversAAL (Sadat et al., 2013) tries to build up one "Consolidated European AAL platform" (Ferro et al., 2015) and integrates different software modules of other European research projects such as *Amigo* (Janse, 2008), *MPOWER* (Mikalsen, 2009), *OASIS* (Bekiaris and Bonfiglio, 2009), *SOPRANO* (Balfanz et al., 2008) and *PERSONA* (Fraunhofer AAL, 2008) into one single AAL solution.

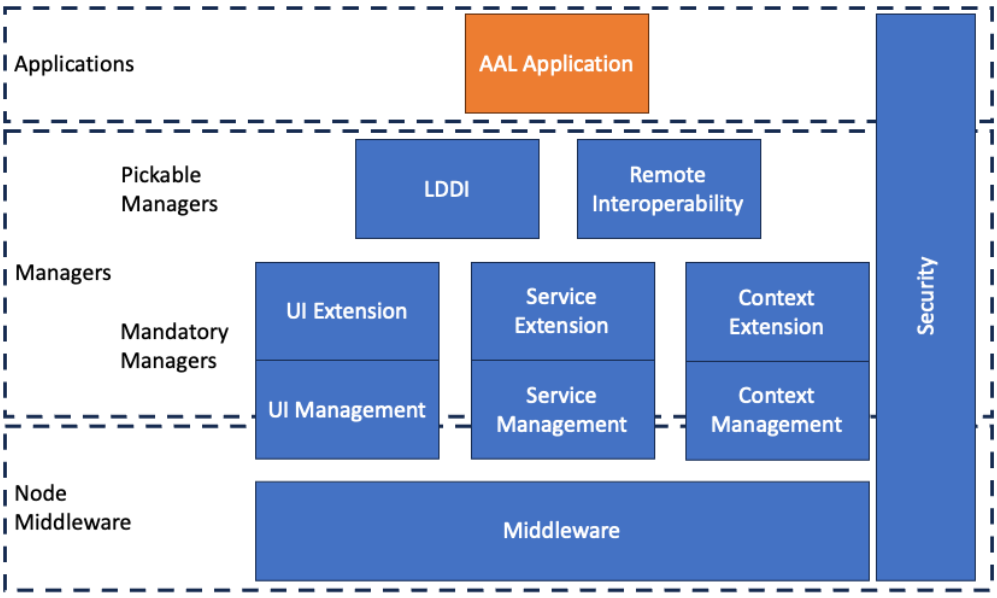

Figure 5.3: The Runtime Support Platform of universAAL (Ferro et al., 2015)

Figure 5.3 gives an overview of the universAAL building blocks:

- The **Middleware** serves as the fundamental core within any runtime platform, aiming to conceal distribution intricacies while enabling seamless connectivity among all components deployed in the AAL system. Acting as an intermediary between communicating entities, it masks the technological diversity inherent in these elements.

- **Context management** establishes the framework for effective communication between context data providers and consumers, employing both push and pull mechanisms. It ensures that data adheres to a standardized model, enabling seamless understanding and exchange among all involved parties.

- The **service management** building block streamlines service-based interoperability by overseeing service registration and functioning as an intermediary between service providers and consumers to manage service requests. For instance, it identifies alignments between incoming service requests and available service providers. Additionally, it offers capabilities for service composition and orchestration, enabling the integration and coordination of various services.

- The **UI management** building block tackles the complexities involved in the direct interaction between an AAL environment and its users. It ensures that applications remain independent of the specific input/output infrastructure present in diverse AAL spaces, which can significantly vary in occurrence. This framework establishes guidelines for capturing user input and presenting system output to human users.

- The **local device discovery and integration** component (LDDI) serves the purpose of seamlessly integrating diverse hardware devices into the UniversAAL platform. Many AAL applications demand specialized devices that arrive pre-packaged without the option for device manipulation. As a specialized building block, this component plays a crucial role in harmonizing the integration of these devices into the system, enabling their seamless incorporation despite their specialized nature.

- **Remote interoperability** oversees platform operations concerning interactions between AAL spaces and external environments. It facilitates various essential functions, including remote assistance provision by service providers, monitoring from a distance, accessing services within AAL spaces remotely, importing external services into the AAL environment, and establishing communication between different AAL spaces.

- The **security** block within UniversAAL encompasses trust establishment, privacy awareness, and access control on all layers.

This first release of UniversAAL consists of the *AAL Studio*, an integrated development environment with different Eclipse (The Eclipse Foundation, 2022) plugins, the *Runtime Support Platform (RSP)*, *UniversAAL Control Centre (uCC)*, for managing the platform, and *UniversAAL store (uStore)*, to provide one single repository for new software and services. Its goal is to make it viable for developers to create new AAL services. Interested developers are therefore provided with extensible knowledge-bases, online courses, wikis and personal training sessions. The uStore is seen as a central marketplace to distribute the developed applications based on UniversAAL.

The work on UniversAAL marks the end of the major research projects that focused on a generalised and standard-setting platform for ambient assisted living. Meanwhile, no more relevant projects have been included in the major funding programmes at EU level. Research among the European funding programmes (Publications Office of the European Union, 2023, Search terms: AAL, Platform) and in the funding line for AAL under Horizon 2020 (AAL Association, 2023) did not reveal any relevant innovations after 2017. It therefore looks as if the efforts to design a common standard platform for AAL projects have lost traction.

5.3 Cloud Computing in Ambient Assisted Living

The AAL platforms that are presented in section 5.2 mostly require an installation of the whole system in a user's environment. The needed working power can mean high costs for the initial setup of such a system. Another possibility that is currently discussed is the use of cloud systems for special services that can be accessed via web-interfaces by different systems or institutions.

Kim et al. (2012) present a platform approach to share health data in the cloud securely. The system is built around *Microsoft HealthVault* Microsoft (2016) and *DACAR* (Fan et al., 2011). The patient-centric solution provides strong security and privacy characteristics and is entirely governed by the patient. It allows sharing of health data between hospitals, trained care-personnel or relatives to indicate changes in the health conditions among different support groups of the user.

Ekonomou et al. (2011) introduced a cloud-service for maintaining an installation of an AAL solution in a home environment. They developed an extensible OSGi-based architecture for highly heterogeneous smart home systems. This architecture is focused on the integration of new devices by using a cloud-based service for discovering drivers in a manual, semi-automatic and automatic way. The user interface for the auto-discovery is displayed on a smartphone for ease-of-use.

The project Cloud-oriented Context-aware Middleware for Ambient Assisted Living (CoCaMAAL) (Forkan et al., 2014) tries to move the AAL platform to the cloud. Their focus is on the implementation of a service-oriented architecture (SOA) for unified context generation. Data of installed sensors and devices in the smart living environment is collected by a *Data Collector* on-site and transferred into the cloud. This data is combined by a *Context Aggregator* and interpreted based on classifications obtained by *Context Providers*. A *Context-aware Middleware* matches this context with services provided by a *Service Provider Cloud* and sends appropriate actions back to the *Data Collector* to activate actuators or devices. Besides this high-level architectural description, no further information or code is

provided by the authors.

El Murabet et al. (2017) introduced the concept of Platform As A Service within the context of Ambient Assisted Living for the first time.

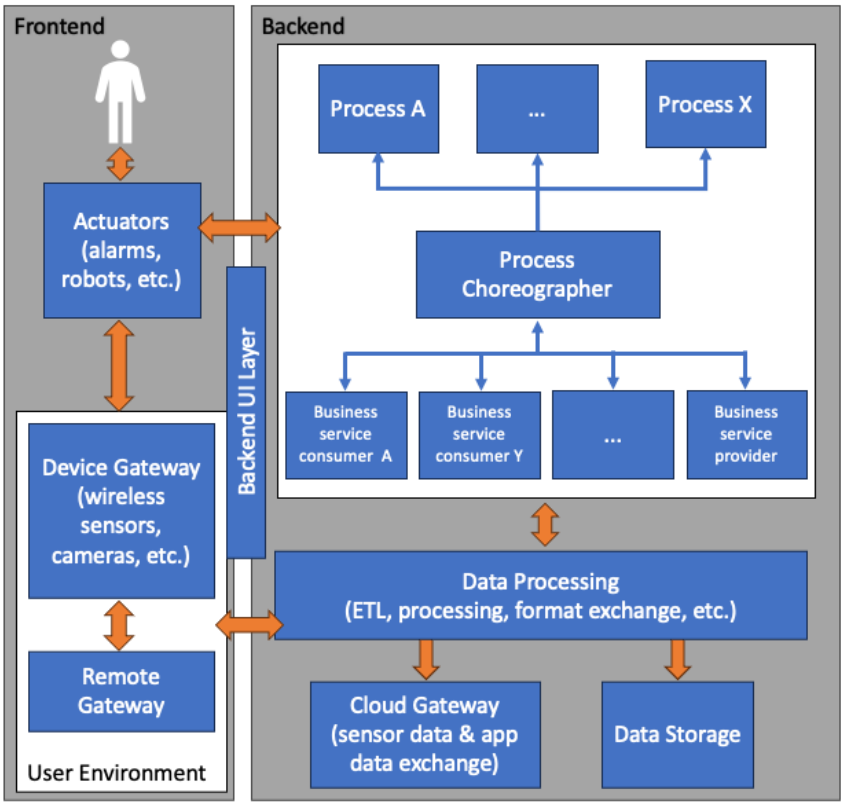

Figure 5.4: SOA-based AAL architecture (El Murabet et al., 2017)

In their approach, the architectural model relies on Service-Oriented Architecture (SOA) with loosely coupled software components based on Node.js (see Figure 5.4). The system gathers situational and environmental information about individuals, locations, and objects through an indoor sensing environment. This setup includes various devices like wireless sensors, cameras, movement detectors, etc., managed by a Device Gateway and Remote Gateway. Additionally, historical health-related data is stored in other data repositories.

To process this data, Data Processing software is utilized. This integration point facilitates the extraction, transformation, and unification of the collected data to derive meaningful insights.

Within the architectural model, services are interconnected to facilitate the exchange between service consumers and providers. A process choreographer

ensures coherence among services and defines suitable processes to be initiated by the designated actuators. Actuators, capable of executing actions toward users or their environments, are stimulated based on the knowledge derived from processed data.

Apart from this description of the individual components, no more detailed description of the composition of the platform or the used cloud infrastructure is currently available.

5.4 Reusing and Extending Existing Platforms

The two most promising platforms for research on new approaches for ambient intelligent services in the field of AAL at the time of writing are UniversAAL (Ferro et al., 2015) and CoCaMAAL (Forkan et al., 2014). UniversAAL delivers a platform that can be configured for developing applications, testing applications and test bed installations. The complexity of the platform itself and the still ongoing development makes it difficult to test and implement new mechanics in the architecture. Nevertheless, there are aspects that have to be considered when building the system architecture, like the introduction of ontologies for classification of collected data, the uStore for providing new applications or OSGi as a common basis for developed plugins. Furthermore, UniversAAL is based on local installations.

SpeciAAL tries to build up an AAL PaaS (Platform as a Service) in the cloud. The project CoCaMAAL is presenting an architecture that is cloud-based as well, but above that, no further information of the development state is provided. The same applies to the PaaS approach based on SOA from El Murabet et al. (2017). At the time of this work, no starting point could be found for the further development or adoption of technically transferable approaches.

5.5 Data Security in OSGi

The AALIANCE consortium recommends using a modular and open approach for new services and software in the context of AAL (Dario and Cavallo, 2014). For remote management for software upgrades and installing new software to an existing platform, OSGi is seen as the most adopted middleware in AAL environments (The OSGi Alliance, 2014). The central feature of OSGi is the possibility to include, update, start and stop services as modular bundles during runtime without the need for a restart of the whole environment. Existing systems based on OSGi are, among others UniversAAL (Sadat et al., 2013), OpenAAL (Wolf et al., 2010) or Soprano (Schmidt et al., 2009).

The downside to the flexible extensibility and adaptability of OSGi based systems is the vulnerability to malicious software extensions that can violate security concepts or disrupt the whole system. Huang et al. explore the security mechanisms of OSGi and divide them in three layers: The security features of the Java Virtual Machine, security mechanisms of Java (e.g. sandboxing), and the security concepts of OSGi itself (granting access of access between bundles based on the Java 2 security architecture). To further improve the security, they propose an Advanced OSGi Security Layer (AOSL) to audit bundles and detect anomalies during runtime (e.g. denial-of-service attacks by exceeding load or thread-duration) (Huang et al., 2007). A similar way of anomaly detection is presented by Wang et al. (2012): By using a Service Monitor and Java Virtual Machine (JVM) Monitor and service proxies, they keep track of the execution time and memory consumption of services to provide assistance in finding anomalies. Although the presented work does not focus on anomalies' detection, service proxies are used to intervene in the platform processes without the need of modifying the deployed bundles.

Another way of isolating components to secure the overall system is shown by Geoffray et al. (2009). They modify the Java Virtual Machine and prevent malicious components to bring down the whole OSGi system. According to them, this is necessary to compensate the original assumption of general trust between

components within an OSGi environment.

A solution of Security-by-Contract (SxC) in OSGi is presented by Gadyatskaya et al. (2012). The manifest-file of each bundle is extended by a contract that contains information about the functional requirements and the accessibility by other bundles of the OSGi environment and is evaluated during deployment by the Platform Security Policy. If the evaluation fails and contracts are incompatible with the current platform policy, the bundle will not be deployed. Putting initial requirements and further descriptive entries in the manifest-file is also of interest in the presented approach to further detail the purpose and the implications of a new installed service. Parrend et al. (2007) present a Privacy-Aware Service Integration. They propose a framework for ensuring privacy policy-compliant services and a metadata language for privacy checks in an OSGi environment. The service provider has to ensure that all offered services are secure and tested before installation, and that they provide the information needed by the platform during deployment and for privacy evaluations. Service restrictions are then realized by so called *RestrictedContext*: Bundles can only access other bundles they are allowed to discover by policy.

Due to the belief that it is not easy to control both, the service provider and the client, in a way to guarantee a sound, secure and privacy consistent platform, the presented solution has lesser necessary preparatory work and basic assumptions.

5.6 Conclusion

This overview of current projects in the field of AAL presents a classification of the chronological development of smart home environments and platforms for AAL. The core of an AAL system is always the connection of sensors, actuators and connected services. Through middleware and a central decision logic, data is combined into information that can trigger certain events (see Section 2.2).

Previous projects have each dealt with different aspects: They provide guidance

for service developers, simplify the connection to middleware by standardizing interfaces, simplify the management of eHealth services, simplify the integration of end devices by automatic recognition, develop an ontology for AAL applications, or try to consolidate and merge the existing solutions. The existing solutions of AAL systems with a cloud computing approach form a broad spectrum from simple possibilities of data exchange, to home installations with remote management extensions, to the complete shifting of reasoning tasks to the cloud. Since OSGi is a frequently used element for AAL middlewares, this chapter also deals with the data security concepts.

Parts of this chapter were published in the peer-reviewed paper "An Ambient Assisted Living Platform as a Service Architecture for Context-Aware Applications and Services" (Kuijs and Reich, 2014).

Chapter 6

Preliminary Considerations

Even though it was not possible to identify a basic architecture to reuse for this project in the previous chapter, commonalities, and trends were identified in recent architectures that should be incorporated into a new architecture. Consequently, the next segment addresses the primary requirements. Subsequently, it introduces the use cases intended for examination within the thesis, which will also function as illustrative examples throughout the remainder of the work.

6.1 System Requirements

Requirements for architecture are derived from the main concepts presented in the last chapter:

- OSGi can be considered the basic technology for middleware. This gives the system access to already established implementations and secures the connection to legacy systems (see Sadat et al. (2013) and Wolf et al. (2010)).
- The functionalities are accessed via web interfaces. On the one hand, this can be done via web interfaces or web services and thus offers flexibility to connect end devices that are adapted to the users (see Berger et al. (2007), Kim et al. (2012), and Ekonomou et al. (2011)).
- New functions can be installed via a bundle repository. This creates a central

marketplace that can be used for updates in addition to the presentation and installation of new functions (see Sadat et al. (2013)).

Regarding access management, the following requirements arise:

- OSGi services that are new or updated must undergo monitoring at every stage of their lifecycle to detect anomalies (see Huang et al. (2007) and Wang et al. (2012)).
- The manifest-file of OSGi bundles can be extended by meta-informations for access policy creation purposes (see Gadyatskaya et al. (2012) and Parrend et al. (2007)).

6.2 Use Cases

The success of a system for AAL depends on customizing its services to meet the varying needs of users in specific usage contexts. Adjusting service functionality based on the user's environment, needs, and profile through context-based service adaptation is key. Because of the data minimization principle mentioned in Article 5(1)(c) of the EU GDPR (Publications Office of the European Union, 2016) and Article 4(1)(c) of Regulation (EU) 2018/1725 (Publications Office of the European Union, 2018), not every service gets all the information. For example, the communication service providing audio and video telephone calls, should not get information about the health condition of the user. It gets access to information about the volume, the contacts and possible colours or font sizes for the user interface.

For this reason, information is grouped into categories for which independent release permissions can be granted. Subsequently, within the thesis, these categories form the basis of the underlying ontology.

Adaptation of services in SpeciAAL is founded on the context of the user. The following sections describe the use cases and the information that is used for

adapting the services. First, a brief description of the user is given, showing his current situation.

User description:

Mr. F. is a 73-year-old widower, has two children and lives alone on a big farm outside a small rural town. One of his children lives abroad, the other in a city far away, so they rarely can visit their father. Mr. F. is a member of a model railway club in the city about 30 km away. Once a week, he used to attend the club meetings. Recently, he broke his leg after he slipped on an icy surface and therefore has mobility limitations and cannot leave the house very often. His children are worried because his friends and also his club mates from the model railway club don't have much time to visit Mr. F. personally.

Information Items	**Information Category**
Children	Contacts
Model Railway Club	Interests
Club members	Contacts
Clubhouse 30 km away	Environment
Winter/Icy surface	Environment
Broken leg	Health

Table 6.1: The relationship between items of information about the user and information categories

To support Mr. F. in his daily tasks, the SpeciAAL platform assists him in communication, information acquisition and learning. With this platform, he can stay socially integrated. Especially his children can feel more comfortable, by contacting him more easily during this convalescence period.

Use Case 1: Communication Assistance

Each contact in Mr. F.'s address list has specified several communication channels, like telephone, email, video chat, SMS, etc. Additionally, each contact has defined information

about the availability of the different communication channels based on the contact person's daily habits or appointments. It is assumed that there is always at least one communication channel, where the contact can be reached in an urgent situation. Suppose Mr. F. wants to communicate with one of his children. All he has to do, is to select the names of his children from his address list. After this, the SpeciAAL platform automatically selects the communication channel based on the aforementioned schedule and preferred communication channel (e.g., SMS because his son is busy).

The communication app itself is just a simple client service, getting only the information needed to interact with the user. Therefore, the main context information is about the contacts saved as individuals of the class *Contact*. For the communication app, information about the system preferences of the user are used to adapt the GUI. Most of the settings can automatically be derived from the health condition of the user (information category: *HealthCondition*). For example, if the user has a red-green colour blindness, these colours should be excluded from possible system settings or if the user has a hearing deficiency, the volume should not be set under a minimum level. This information can be saved in the class *SystemPreferences*. Other information must be collected manually, like information about existing accounts.

Use Case 2: Information Acquisition Assistance

Another application on the platform helps Mr. F. find assistance from other people in the countryside. Although he stopped active farming, there are many things to be done on his farm. He has to feed his bunny, do lawn mowing, go shopping, repair things once in a while, clean the house, etc. All this is very difficult or impossible for a mobile restricted person. If he needs help, he should be supported by a SpeciAAL service. Because the platform knows the user's health condition, it offers an "search-and-offer" service automatically. This could be used to search for assistance in the aforementioned daily or weekly tasks, but also for special occasions. For instance, if there is a social meeting with the model railway club, he would like to participate in, the system will automatically help him to get a lift or special transportation. If his health condition gets worse, and he cannot

attend the meeting, the lift will be cancelled by the system. Because the system also knows about the environment, e.g., the weather condition, it can automatically organize help, for example, to clear the snow.

Information Items	**Information Category**
Appointment with model railway club	Environment (Time)
Tasks	Activities

Table 6.2: Additional Information for Use Case 2

For the application which assists the user in organizing information acquisition, primarily knowledge about the health condition (information category: *HealthCondition*) and environment (information category: *Environment*)of the user is helpful. The main advantage of this app is that it asks if it should organize assistance in something, depending on the actual context. Context could be, for example, the condition of the user, his impairments, the weather, the time, the sensors in the house, etc. Due to the information given by the information categories, the system can decide if there is a need for a special service or not. But for not deciding absolute autonomously, the user is always asked if he really needs help.

Due to the acquisition of the interests, activities and personal preferences of the user, it is possible to offer the user with the "search-and-offer" service assistance of finding all kinds of support. Since the user in our use cases has a broken leg, he could get a snow shovelling offer automatically, during winter time. The model railway passion of Mr. F. can be supported by helping him to get a lift for the weekly meetings by the "search-and-offer" service. It uses the information saved in the instances of the classes *Interest* and *Activity* for providing personalized functions.

Use Case 3: Learning Assistance

Every day, Mr. F. uses the SpeciAAL platform's fitness service. The fitness service guides Mr. F. through his every-day exercises like arm circles, arm curls or leg straightening.

Because of the new change in health condition, the service automatically skips exercises which are not suitable for a broken leg and adds some arm movement exercises to reach the same fitness level. As he recovers slowly from his leg fracture, the system can include specific exercises for his legs to restore his mobility.

The fitness status of Mr. F. can be gathered by the *Education* class. If he reaches a new level of fitness by doing all the required exercises, the level can be saved in this class. Through the *History* class, it is possible to consider the whole progress of fitness condition. If there are steps backwards, the exercises could be adapted accordingly. The health condition information makes it possible to automatically offer only the exercises that are feasible for the user with his current impairment.

6.3 Conclusion

This chapter describes the main requirements for the thesis in the two areas of architecture, with a starting focus on the middleware and interfaces to be used, as well as on the design of access rights. These elements were recognised as commonalities and trends from the previous literature research.

In addition, various use cases were presented to illustrate the practical application scenarios and emphasise the adaptability of the system in different contexts. These preliminary considerations serve as a cornerstone for the subsequent development phases to ensure a well-defined system that is in line with the defined objectives and user needs.

Chapter 7

The Architecture of SpeciAAL

The first part of this research focuses on delivering cloud-based services for AAL. Cloud computing enables service providers (e.g., caregivers or day care facilities) to deliver services without the need for investing in expensive technical equipment in advance. By delivering services through the cloud, the high start-up costs can be reduced significantly, and it will be feasible for service providers and users to try out new or innovative services without the need of a high investment. This extensibility can be provided by a customizable PaaS that is run by the service provider. The PaaS is considered to run in a private cloud, as adaptation of the system to the user's need is heavily based on personal user data. But as described in chapter 3 this setting has the downside, that it will not scale beyond the boundaries of the physical hardware that is used for running the private cloud. For this, the private cloud is extended by services that may run in the public cloud (e.g., third-party cloud providers).

7.1 Acknowledgement

At the beginning of development for the architecture in the context of this thesis, some of the technologies now in use for providing scalable services in the cloud were not yet available. This thesis therefore uses virtual machines as working nodes and presents PaaS management for scaling on a VM basis. If this architecture

were to be developed again from today's perspective, the much more lightweight container technology based on Docker (Docker Inc., 2023) or Kubernetes (The Kubernetes Authors, 2023) would be used. Containers represent specialised runtime environments that are much less generalised, can be used both stateless and stateful, and can therefore be put together to form an overall system in a very similar way to bundles in OSGi.

Nevertheless, basic mechanics such as the basic structure of the management system, the provisioning of a dOSGi layer, centralised access to data storage and the redistribution of resources can also be transferred to the new technology.

7.2 SpeciAAL and Cloud Computing

SpeciAAL is based on OSGi (The Eclipse Foundation, 2015): OSGi supports installing, starting and stopping software bundles during runtime. By introducing tools for managing and resolving of dependencies between bundles, the application can be extended or updated during runtime without the need to restart the whole environment. OSGi has also been chosen, since it is a seen as a standard technology for Smart Home environments and AAL platforms (OSGi Alliance, 2016).

The main idea of the presented architectural approach is to provide a platform for OSGi applications in the cloud. When leveraging services to the cloud, it is often required to have the ability to scale resources according to the computational demand.

At an IaaS provider, scaling can be achieved by providing bigger or smaller Virtual Machines (VMs) in terms of computational power or memory resources, by providing bigger or smaller storage nodes or by load balancing network traffic among different VMs or with different priority.

At the SaaS level, scaling is often achieved by load balancing requests between more or fewer nodes of the same application. For this the application has to be

either stateless, has to provide synchronized states among all instances of the application or has to store its current state on client side (which is often done in web-application sessions).

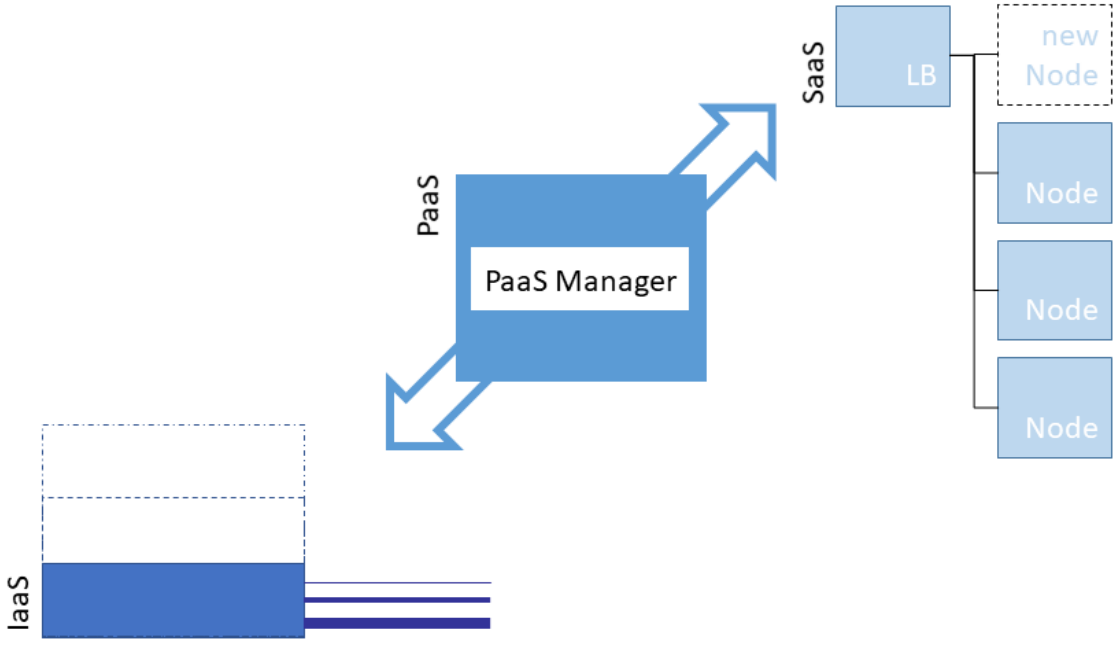

Figure 7.1: Scaling at SaaS and IaaS level by PaaS management

PaaS management organizes scaling on the IaaS (vertically) and SaaS level (horizontally) and is often used to automate the scaling process (see Fig. 7.1). The AAL service developer wants to use the scaling service from the PaaS to develop and provide an AAL service to the customer.

Strictly speaking, PaaS just provides platforms for development or deployment (Mell and Grance, 2011). One scaling scenario would be to request a bigger platform to test or run an application. This would translate to a bigger VM on the IaaS level. To address user load, a scaling scenario would be to start new nodes of the same application behind a load balancing infrastructure on high demand or to stop the nodes when there is a decline of demand for the application. This would trigger the SaaS scaling like explained before and also be coordinated by the PaaS management environment.

The focus of this approach lies on the demand of a growing modular application on the computational resources itself. By adding more functionality to the modular

application, the provided environment on one platform node can get too small regarding memory or CPU power. The presented research supports this scenario by scaling out horizontally to being able to put the new module on a new node in a distributed OSGi platform (see Fig. 7.2).

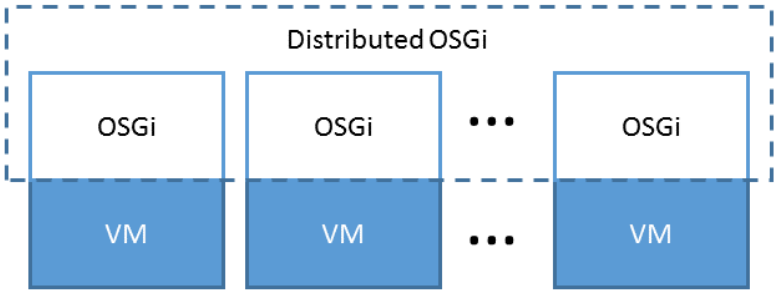

Figure 7.2: Horizontal Scaling with dOSGi

In a dOSGi environment, different OSGi VMs and their running bundles are connected to each other to compose one big OSGi environment by imports and exports of endpoints. Communication between the different nodes is usually done by calling HTTP interfaces. The OSGi Core Specification 4.3 (OSGI Alliance, 2011) introduces the main concept of dOSGi, but does not recommend a specific way of implementation for the required components and functionality.

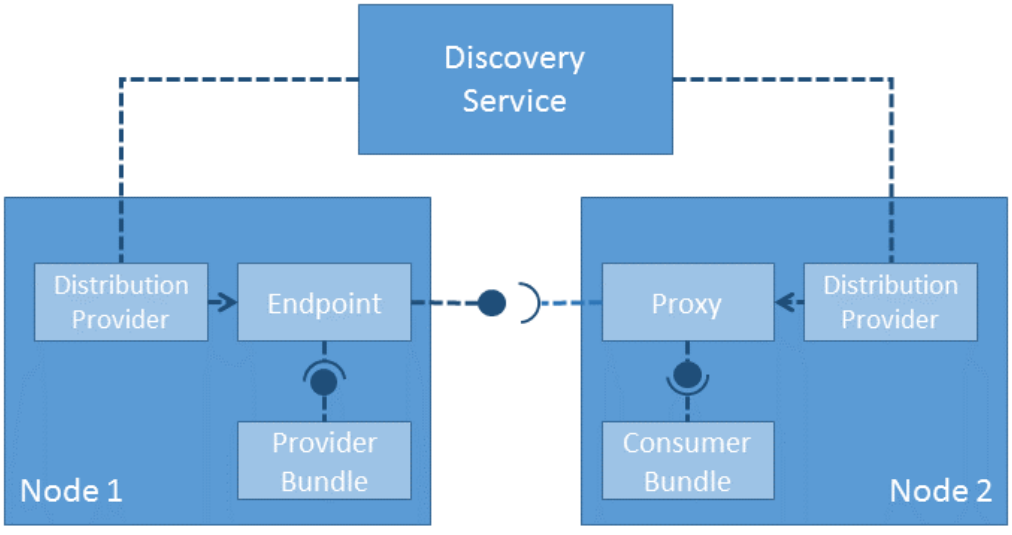

Figure 7.3: Basic Functionality of dOSGi (based on Apache Software Foundation (2015c))

As shown in figure 7.3, a *Provider Bundle* in *Node 1* exports an OSGi service as an interface by using additional service properties (e.g., which interface is accessible

remotely). This interface is registered at the *Distribution Provider* within the node and an *Endpoint* for a remote call of the service is created. Through a *Discovery Service*, this existing *Endpoint* is announced at the *Distribution Provider* of the remote node, where the *Distribution Provider* creates a *Proxy* for the remote service. This *Proxy* can be imported by a *Consumer Bundle*, like a locally deployed bundle. The *Proxy* and *Endpoint* provide the implementation for remote message exchange.

The OSGi Compendium (OSGi Alliance, 2012, Specification 4.3) splits the *Distribution Provider* into several modules, to make it possible to enhance or exchange parts of the *Distribution Provider*. The *Discovery* module notifies *Endpoint Listeners* upon detection of available *Remote Endpoints*. The *Topology Manager* uses also an *Endpoint Listener* to monitor remote OSGi services and can monitor locally available OSGi services. The creation and destruction of *Endpoints* and *Proxies* is delegated to the *Remote Service Admin* module.

The project Apache CXF (Apache Software Foundation, 2015c) has implemented these components in a framework to support dOSGi in several specification compliant OSGi platforms (e.g., Equinox, FELIX or Knopflerfish). The *Discovery* module is implemented with an Apache Zookeeper server (Apache Software Foundation, 2015b), to discover and announce endpoints in a highly dynamic environment.

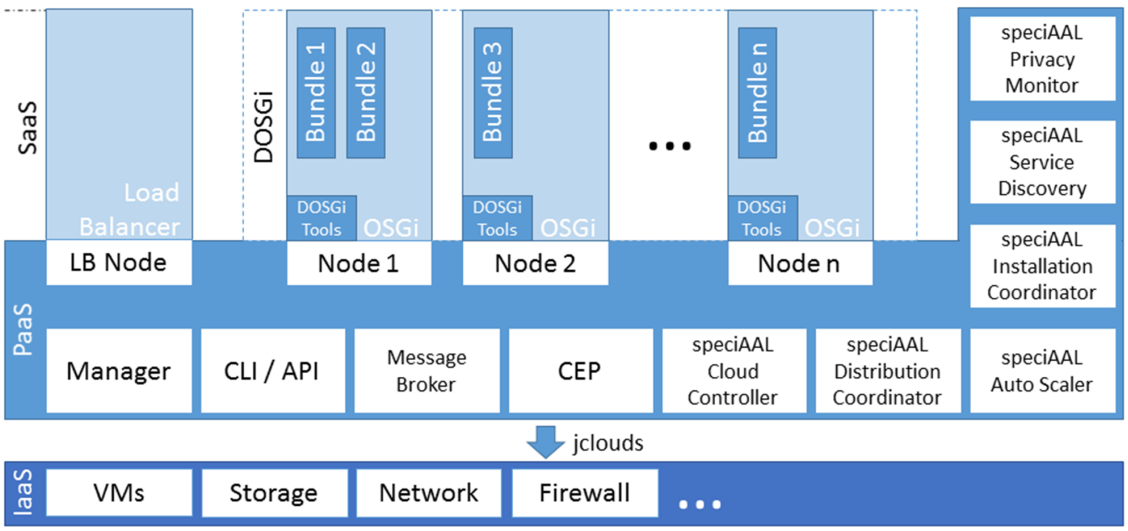

Figure 7.4: dOSGi PaaS for SpeciAAL

7.3 Overview of the SpeciAAL Architecture

Figure 7.4 shows an overview of the SpeciAAL architecture. The architecture is divided into three layers: The IaaS layer, the PaaS layer including the PaaS Manager and the SaaS layer. Heavily modified or newly introduced modules are marked by SpeciAAL. To explain the details of each layer, the different components are described in the following subsections.

7.3.1 IaaS Layer

The IaaS can be implemented in either a private cloud (e.g., an OpenStack installation hosted at the institution) or a public cloud (e.g., Amazon AWS, Rackspace). IaaS providers support starting and stopping virtual machines based on specified VM templates (compute power and storage services), network routing services, database and persistent datastore services, accounting services and monitoring.

The IaaS layer is controllable through command line tools (Amazon Web Services, 2022) or API calls (The OpenStack project, 2015) to manage nodes based on decisions made in the PaaS layer. To be able to control different APIs of different IaaS providers, there are tools, that wrap the system specific or vendor-specific API for being able to exchange the IaaS infrastructure based on different service requirements. jClouds (Apache Software Foundation, 2015d) or BOSH (Cloud Foundry, 2023) try to standardize the usage of Cloud infrastructure APIs.

7.3.2 PaaS Layer

Open PaaS management systems simplify the provisioning of developed applications. Examples are Apache Stratos (Apache Software Foundation, 2015a) and Cloud Foundry (Linux Foundation Collaborative Projects, 2015). It reduces deployment time of a platform or a framework needed to run an application. For this, the PaaS management systems can be configured to certain environments

(e.g., PHP, JVM, Ruby, OSGi) that are ready to be started and used by application developers. This can reduce deployment time for the developer or the system operator, and therefore also cost for the company they work in. Open PaaS management should be IaaS provider independent to enable provisioning of platforms on different IaaS environments like OpenStack, Open Nebula or Amazon AWS. The presented PaaS layer architecture is based on the works of Apache Stratos (Apache Software Foundation, 2015a) and customized with components needed to provide horizontal scaling of dOSGi.

The *Manager* (see Fig. 7.4) is the central component for interacting with the PaaS environment. The *Manager* provides a user interface (UI) or command-line interface (CLI) for registered PaaS users. It holds information for available platform environments, scaling and deployment policies and is the central component to deploy environments or load balancers. The *Manager* provides tools for multi-tenancy: virtual computing resources and platform environments can be administered and shared among PaaS users, for deploying the applications, but also divided to provide specialized platforms or set different resource limits to various developer groups.

The *Cloud Controller* component communicates with the IaaS infrastructure and holds all the topology information of the PaaS system. The communication with the IaaS layer is done through an implementation layer and can be provided by the aforementioned jClouds. This makes the API of the IaaS layer accessible to the PaaS layer and allows management of different VMs or other service functionality (e.g., network routing) of the IaaS provider. All information retrieved from the IaaS is stored in the topology configuration at the *Cloud Controller* and can be published to other components that need to be aware of changes in the topology of the PaaS system. Examples of components where topology data is crucial information to work properly are the *Load Balancer* or the *Distribution Coordinator* component.

The *Distribution Coordinator* holds a set of deployable artefacts to update the deployed platforms. This component can also be used to automate the deployment process for the complete application on all subscribed running nodes. The artefacts

are usually received from a connected repository service and deployed based on deployment policies, by events triggering the deployment or by manual commands to the *Manager* component. The *Distribution Coordinator* is triggered on start-up of a new node and is considered to hold all nodes of the same type at the same deployment state by the concept of deployment synchronization.

To take advantage of the possibility to add and remove computational resources to or from an application or distributed environment, the *Auto Scaler* component evaluates load and health information of the *Complex Event Processor* based upon policies (e.g., deployment policies or scaling policies). This evaluation is executed by a rule engine and applied according to the current topology retrieved from the *Cloud Controller* component. The information exchange between components is realized by a *Message Broker* component and a message bus based on a publish/subscribe pattern. This pattern enables the PaaS layer to add or remove components (e.g., load balancers) dynamically by preserving the information exchange between components.

The *Nodes* (or *Cartridges*) are the actual environment in which the application is running. They are started, stopped and registered by the *Cloud Controller* module. In modern PaaS Management systems, the focus lies on fast deployment of a completed application to a cloud node. For this purpose, the *Distribution Coordinator* can provision the whole application out of its repository into a new node and to keep existing nodes up to date. In the presented approach, this task is reduced to deploying just the environment and the minimum required components for setting up the initial bundles of the application in a dOSGi environment. The deployment of new functionalities is later triggered by functionality in the SaaS layer. This leads to a flexible and extendible application that can interact with the PaaS layer.

The *Service Discovery* is integrated in the PaaS layer but directly connected to the SaaS layer to translate the currently active application topology to coordinated actions in the PaaS layer. It is further described in section 7.4.

The *Installation Coordinator* is a new concept for the SpeciAAL architecture. It can receive installation requests out of the SaaS layer and evaluate the best place for installing a new functionality in the distributed environment of the application. Its main characteristics are detailed in section 7.4 and the process of installation is explained in section 7.5.

The *Privacy Monitoring Module* can collect log-data of actions within the SaaS layer and generate reports according to privacy policies and data access policies. This component will be of main interest in a later stage of the research.

7.3.3 SaaS Layer

In the presented approach, the SaaS layer provides services for the platform SpeciAAL in a dOSGi environment. All running bundles are added up to one adapted application for the user, with the functionalities configured to his needs. It consists of system bundles, core bundles and configurable application bundles.

The system bundles are part of the environment and provide general services for distribution (e.g., DOSGi bundles for Apache CXF), discovery (e.g., bundles for communication with Apache Zookeeper) and monitoring.

The core bundles are part of the application and provide core functionalities, like a Web-Interface, an Address Book, Communication bundles for Smart-Home Control and Sensors or a Customizing bundle.

The configurable application bundles are individually chosen by the user and installed via a Bundle Store. These bundles can be installed and configured during runtime and also have the ability to adapt to user behaviour (Fredrich et al., 2014). They can be compared to apps on a smartphone, that can be installed, tested and also deleted if they do not provide a desired functionality.

7.4 Load Balancing in SpeciAAL

In figure 7.4 some components are marked as "SpeciAAL" components: The *Cloud Controller*, *Distribution Coordinator*, *Auto Scaler*, *Installation Coordinator* and *Service Discovery*. These components have to be adopted to support the required functionality to provide the distributed load balancing approach for SpeciAAL as described in section 7.2.

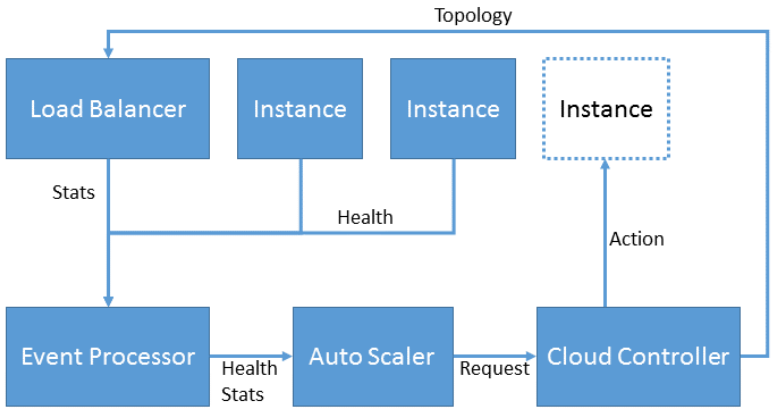

Figure 7.5: Auto Scaling in Apache Stratos

In Apache Stratos, scaling is achieved by creating or destroying instances (so-called cartridge instances) of an application (Fig. 7.5): A real-time event processor receives statistical information (e.g., requests or failed requests) of the *Load Balancer* component and the health status (e.g., load average, memory consumption or request count) of the running cartridge instances. This data is evaluated, summarized and published to a *Health Statistics* topic in the *Message Broker*. The *Auto Scaler* receives this information and decides, backed by a *Rule Engine*, whether new nodes are needed or existing nodes are expendable. The *Auto Scaler* then sends a request to the *Cloud Controller* to create or destroy instances. After the performed action, the altered topology information is published to the *Message Broker* and the *Load Balancer* is updated with the new topology.

One simple solution to provide horizontal scaling for a dOSGi environment would be, to work with small nodes and put each new part of the application on a single node. On installation of a new functionality, the environment would be extended

by a node and the corresponding bundles would be deployed on the started node. It would then be easy to delete the functionality by simply destroying the node. However, this would lead to a fragmented environment and unbalanced resource use across the application. The presented approach is focusing on making use of the available computational resources of one node before extending the environment by adding another node.

For SpeciAAL the *Distribution Coordinator*, *Service Discovery* and *Installation Coordinator* have to be added to the workflow of auto-scaling (see Fig. 7.6):

Analogous to the *Cloud Controller* holding the topology of VMs and network interfaces on the PaaS and IaaS layer, the *Service Discovery* holds the topology for all the distributed services in the SaaS layer. On creation of a new node for the dOSGi environment, it is getting contacted by a previously configured startup script and the new node and further installed services will be updated in the topology and service registry.

Furthermore, the *Service Discovery* is also monitoring the availability of the registered remote services on the node: If the node is deleted, it will also de-register the node and all formerly running remote services on this missing node.

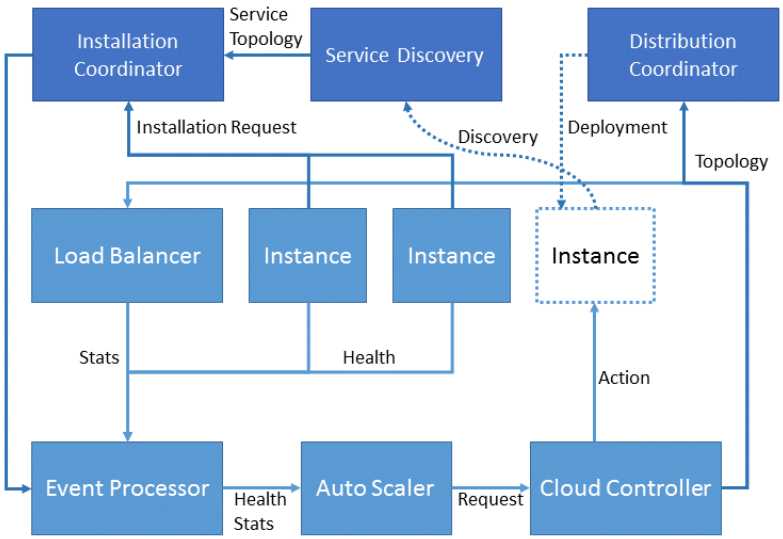

Figure 7.6: Auto Scaling in SpeciAAL

The *Distribution Coordinator* has to configure and set up a new node after starting to provide the required services to integrate the node in the distributed environment.

As described before, it has the capability to keep the nodes on the same patch-level (distribution synchronization) and can push configuration updates as well (e.g., on what address or port a node can contact the *Service Discovery*). For SpeciAAL the *Distribution Coordinator* is used to set up the initial environment with all services that are needed for the application for configuration by the end user (e.g. authentication bundle, database access agent bundle, web interface bundle and an installation wizard bundle). Later, the *Distribution Coordinator* provides additional nodes that are stripped down to only provide the minimal configuration for extending the platform as a dOSGi environment.

The *Installation Coordinator* plays a central role in this setup, as it enables for detailed decisions where to install a new service. Before the bundle installation is performed, load information on the nodes is evaluated and based on this different actions are executed: If the nodes can run another service, it receives the information where (on which node) to install the new bundle in the distributed environment. If the nodes are on a load limit, it triggers the extension of the environment by a new node and receives the information to install the bundle on the newly provisioned node.

To further broaden the basis for these decisions, the *Complex Event Processor* has to be extended to collect information from inside the dOSGi environment (e.g., request/response time between servers and services) as well as from the *Service Discovery* component (e.g., registration or de-registration of services and nodes).

7.4.1 Simulation of Resource Redistribution in DOSGi

To put the main components for resource redistribution in a dOSGi environment in action, a simplified setup is used, and a specified test plan is carried out to gather some first performance data. The test plan combines the two scenarios described above 7.5.2 Installing a new Service and 7.5.4 High Load. This first simulation assumes that the environment is running and the PaaS-Management has already deployed two nodes. Both nodes have low load but are not empty. The strategy

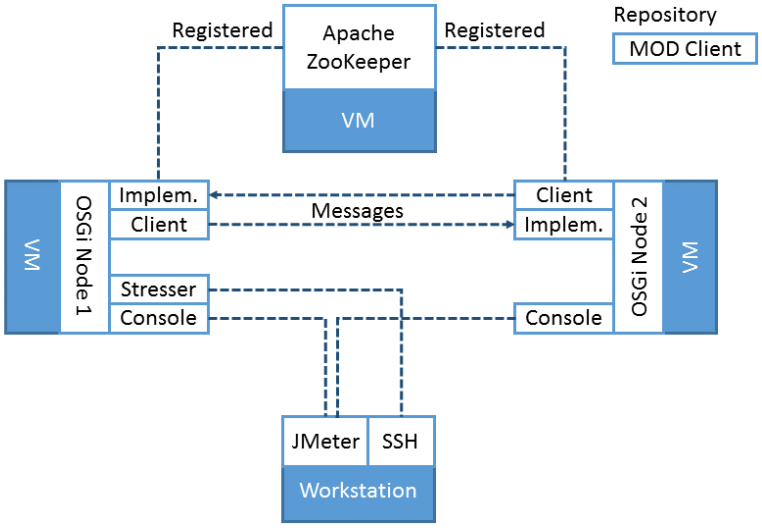

Figure 7.7: Overview of the simulation setup

employed for load balancing during high load involves migrating bundles that are not causing the load, while retaining the critical bundle on the original node.

The simulation environment consists out of three virtual machines and a workstation. The virtual machines are running in a private cloud of Furtwangen University (Meier et al., 2016), based on OpenStack. The workstation is running on the same campus as the virtual machines. Figure 7.7 shows an overview of the setup for the simulation.

The three virtual machines are of the same size and running the same operating system:

- 1 virtual CPU, 512 MB RAM, 5 GB disk space
- Debian Server 8

Two of the virtual machines are set up as OSGi Nodes by using OpenJDK IcedTea 2.6.6 (Oracle Corporation, 2016) and Apache Felix Framework 5.4.0 (Apache Software Foundation, 2016c). On this standard installation, the Apache Felix Web Management Console based on Jetty is added and started to show the actual bundle configuration on a website. For enabling the distributed environment, Apache CXF dOSGi Software Single-Bundle Distribution (Apache Software Foundation, 2016a) is installed and configured to communicate with the third virtual machine where only Apache ZooKeeper is running.

On both OSGi Nodes, a *Sample Interface Bundle*, a *Sample Implementation Bundle* and a *Sample Client Bundle* are running. The *Implementation* and *Client Bundle* are sending and receiving messages through the *Sample Interface Bundle* between nodes every five seconds (see Apache Software Foundation (2016b)).

A *Modified Client Bundle* is placed on another web server and accessible to both OSGi Nodes. This bundle is based on the *Sample Client Bundle* but executes a for-loop every 500 milliseconds, sends the duration to the listening nodes and writes the duration in a file to the disk.

OSGi node 1 is running a *OSGi-Stressor Bundle* (Delacretaz, 2012) that can be configured and activated by issuing telnet commands. This bundle was developed to simulate high load on an OSGi platform by performing random maintenance tasks, like starting and stopping a bundle, refreshing a bundle or updating a bundle. These actions are only performed on one Node and do not interfere with the whole distributed environment.

The Workstation runs JMeter 3.0 (Apache Software Foundation, 2016d), SSH-connections to the OSGi Nodes and a telnet connection to the *Stressor Bundle* on OSGi Node 1.

7.4.2 Description of the Test Plan

The simulation lasts 120 seconds and shows the following sequence:

0 s: The environment is performing normal operations - the *Sample Bundles* are communicating with each other. The web-console on both nodes is accessible.

20 s: A new service is downloaded from the repository, installed and started on Node 1. This is the *Modified Bundle* that is communicating with the already present *Implementation Bundles*.

40 s: Another bundle is started on Node 1. This *Stressor Bundle* leads to high CPU load and influences the other running services.

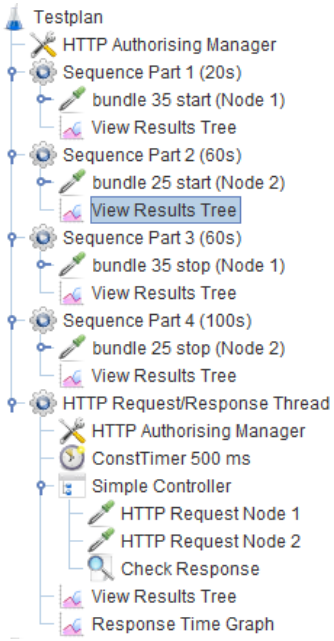

Figure 7.8: JMeter Test Plan (Screenshot of Apache Software Foundation (2016d))

60 s: The *Modified Bundle* is migrated to Node 2 (deployed on Node 2 and uninstalled on Node 1) and continues communication with the *Implementation Bundles*, the *Stressor Bundle* is still present and active on Node 1.

100 s: The *Modified Bundle* is stopped, the *Stressor Bundle* continues operation on Node 1.

120 s: End of simulation.

This is automated in the following parts: A JMeter Test Plan controlling the environment and the running state of the *Sample Bundles*, JMeter request-/response measurements to gain an outside view at the environment and a command to start the *Stressor Bundle* on Node 1 after 40 seconds. The JMeter Test Plan is shown in Figure 7.8.

Sequence Part 1 to 4 define the starting and stopping points of the bundles described above. Each bundle start is timed accordingly.

HTTP Request/Response Thread measures the request/response time of HTTP requests to the web consoles on each node. This is done every 500 ms.

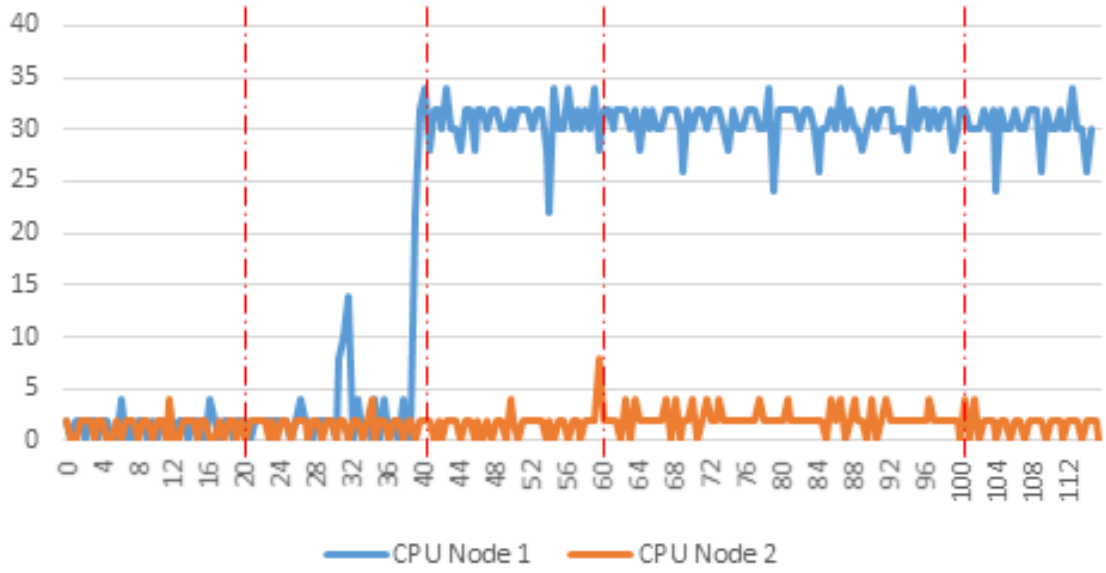

Figure 7.9: CPU Load during the simulation (120 sec)

Response Time Graph is used to plot the response times at the end of the simulation.

After 40 seconds, the *Stressor Bundle* is started by a command via telnet. An otherwise inactive bundle is updated constantly, which leads to a high resource usage.

7.4.3 Results

The simulation is run twenty times in a row to make sure that the shown results represent a constant behaviour of the presented approach. After each run of the simulation, the gathered logs and measurements are processed and evaluated the same way. All results are comparable and deliver nearly the same graphs. The following graphs are an example for the gathered results.

Figure 7.9 shows the CPU Load during the simulation. After the *Modified Bundle* is started, the CPU Load of Node 1 is slightly increased, but after the *Stressor Bundle* is activated, the CPU Load of Node 1 raises significantly. After migrating the *Modified Bundle* to Node 2 the CPU Load of Node 2 is also increased until the bundle is stopped again.

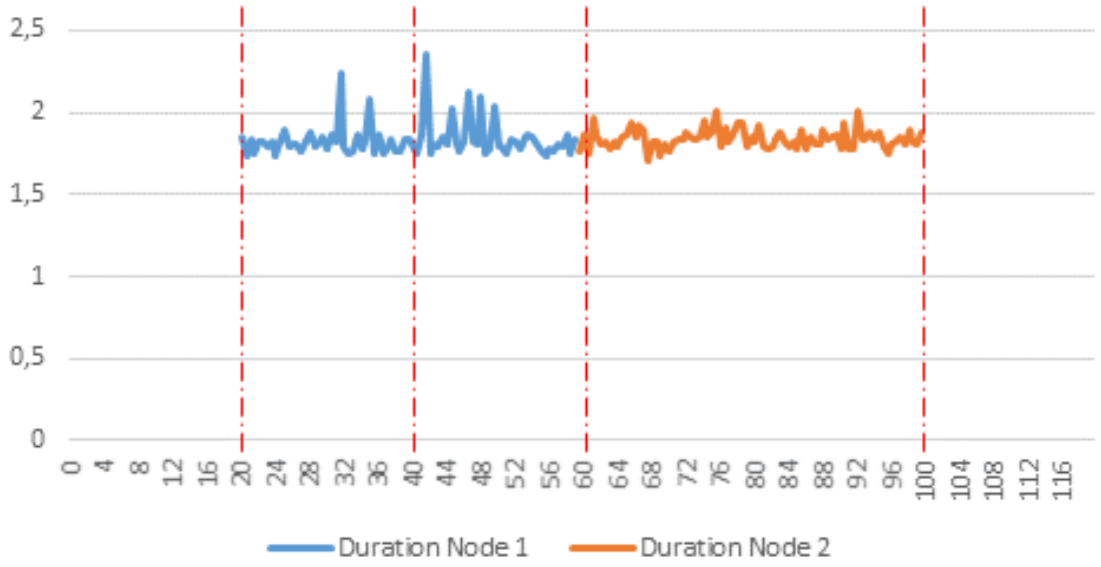

Figure 7.10: Execution time during the simulation (120 sec)

Figure 7.10 shows that the execution time for the function inside the *Modified Bundle* raises after the *Stressor Bundle* is started. After migrating the *Modified Bundle*, the execution time remains fairly low and constant on Node 2. The decline of execution time after 50 seconds could be due to higher prioritization of the Java process/higher CPU scheduling on the virtual machine or allocation of more physical resources in the OpenStack environment.

The response times of both nodes show an according behaviour (see Figure 7.11). Node 1 has an increased average response time after the *Stressor Bundle* is started.

The graphs show, that although it is one distributed environment, it is possible to monitor each node on its own and implement strategies for resource redistribution and distributing services across nodes. The inside view of the execution time by the *Modified Bundle* shows, that besides freeing up needed resources on Node 1 the performance of the bundle is increased on Node 2. This effect could also lead to new strategies when doing resource redistribution during deployment time.

Although these simulated results of resource redistribution in a dOSGi environment are just examples, it indicates that it is possible and can lead to better resource utilization or higher performance and an improved user experience.

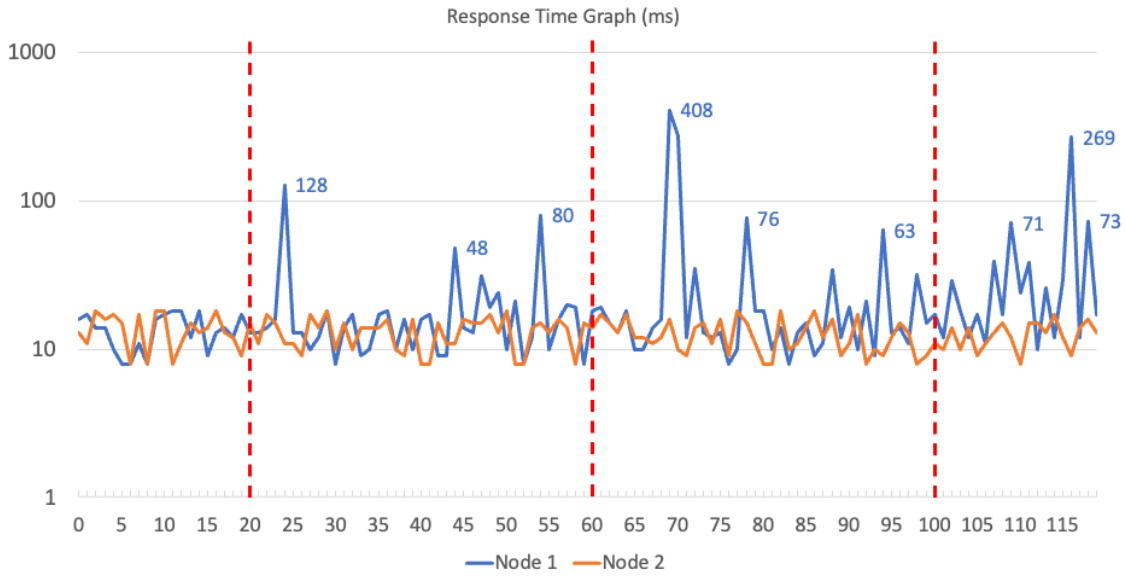

Figure 7.11: Response Time Graph (120 sec)

7.5 Scenario-Based Evaluation

The auto-scaling during operation is influenced by two main aspects: User triggered events or monitoring events. If a user adds a new functionality to the platform or deletes an existing functionality from the platform, the *Auto Scaler* component has to decide whether a rebalancing of nodes has to be performed. Besides this, monitoring events, like high load, low load or health issues, are gathered at the *Complex Event Processor* and can lead to a re-evaluation at the *Auto Scaler* component. In addition, there is load balancing during deployment time as well.

Flexibility of the system is demonstrated by outlining the initial situation, events as they occur, and the system's involved components.

7.5.1 Setup of Application

If a new end-user wants to use SpeciAAL, a new PaaS environment is created. This means that the basis template is deployed by the *Deployment Coordinator* to a newly created VM by the *Cloud Controller*. This action is triggered by the *Manager* and the node will be already enabled for the distributed environment. Although

there is just one node in the beginning, the *Service Discovery* has to be active and the node has to be registered for being able to access remote services later on. The new environment is created with the goal to give each user (e.g., an elderly person) an isolated, customizable and adoptable environment.

7.5.2 Provisioning a New Service

When the user wants to add a new service to the application, the installation request is sent to the *Installation Coordinator*. The *Installation Coordinator* informs the *Complex Events Processor*, which combines the request with the current health and load information of the nodes and triggers the evaluation process of the *Auto Scaler* (see Figure 7.12). Based on the rules engine, the decision-making can lead to

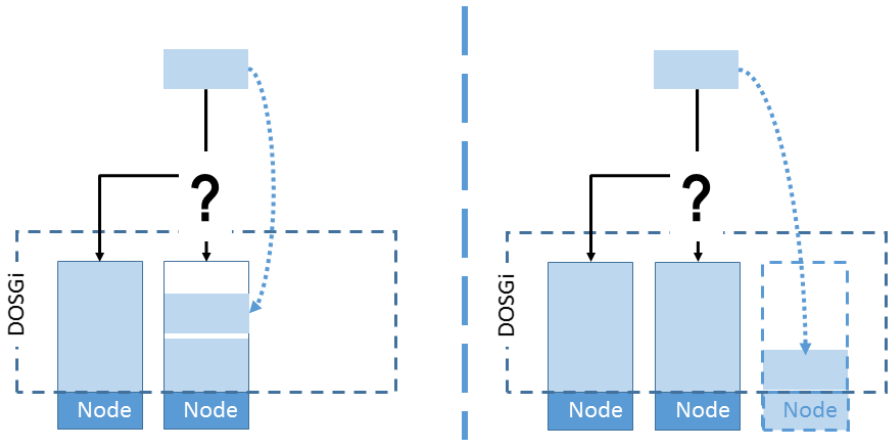

Figure 7.12: Adding a service

one of the two results:

- There are still resources available on a specific node. This information is sent back to the *Installation Coordinator* and the bundle installation is performed on the specified node. On start of the new bundle, exported services are registered by the *Service Discovery* and can be used by other services or the end-user.
- All nodes are exceeding a defined threshold and the new functionality is likely to exceed the computational resources of a node. The *Auto Scaler* requests an additional node (VM) at the *Cloud Controller*. After the node is

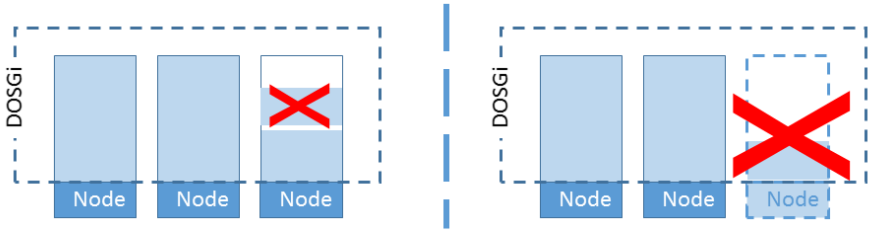

Figure 7.13: Removing a Service

started, the *Deployment Coordinator* gets an updated topology information and deploys the extension template to the new node. The new node is registered at the *Service Discovery*, the *Installation Coordinator* is updated to install the requested bundle on the new node. After deploying and starting the bundle, the exported services are registered by the *Service Discovery* and can be used by other services or the end-user.

7.5.3 Removing an Existing Service

If an end-user decides to remove a certain functionality out of his application, the associated bundles that are no longer needed by other services are stopped and removed. This triggers the de-registration in the *Service Discovery* and the exported remote services are no longer present in the system (see Figure 7.13) (see Figure 7.13).

One special case to this scenario is when the last exported remote service on a node is deleted. This may indicate an orphaned node that might as well be deleted. To verify this sufficient condition, the current set of bundles on the node has to be compared to the set of bundles of a node extension template with only the vital services for distribution.

- If the set is the same, the node is removed from the distributed environment by simply deleting the VM on the IaaS level by the *Cloud Controller*.

- Otherwise, no further actions are required at this phase and the node will be re-evaluated in the scenario “Low Load”.

7.5.4 High Load

At first, this scenario does not differ from the auto-scaling mechanism of Apache Stratos (see section 7.4). One node is monitored as having high CPU load, memory swapping or long-running requests. The *Auto Scaler* triggers the creation of a new node at the *Cloud Controller*, and it is deployed as an extension node by the *Deployment Coordinator*. As Apache CXF has the ability to monitor request/response times on a service level inside the OSGi environment, this is used in a second step to get an estimation, what bundles are causing the overload this time.

As the new node is started up and registered bundles are "moved" to the new node. This is realized by duplicating bundles at first on the new node and deleting the bundles on the busy node afterwards to make sure that a remote service to handle the requests is always available in the environment.

There are two conceivable strategies to move services from a node with high load:

- Moving the service that is detected as causing the high load. This can mean that the long-running requests are prohibiting the service from stopping and the moving scenario will take longer than expected.

- Freeing up resources on the node by moving other services that are not causing the high load. This will leave the problematic service untouched and running, but is not helpful if the service is crashed and producing the high load (e.g., by continuously looping).

7.5.5 Low Load

The opposite situation is too much idle time for one node in the environment. The environment can then be consolidated to fewer nodes. Before a node can be deleted, a method must be established to ensure that all necessary services have been migrated for reassurance: As the *Service Discovery* knows what remote services are running on a specific node, the according OSGi bundles have to be

started on a different node before stopping the services on the node that is to be deleted.

The other information that is crucial is, from which node to which other node the migration of services is applied. There are different requirements that have to be considered for the migration of services:

- For the migration scenario, there have to be at least two nodes with low load. If it is just one node and the services are consolidated on another node with medium load, this can lead to a higher than expected load on the target. In this case, the "High Load" scenario would be triggered, and this would lead to another migration in the opposite direction.

- The definition of threshold for low load should be set low enough, that it is viable to consolidate the two nodes into one.

If the *Complex Event Processor* gets notice of two nodes with low load, it triggers the consolidation process on the *Installation Coordinator*. This is applied the same way as in the High Load scenario: The corresponding bundles have to be started on the target node, before the bundles can be stopped and uninstalled on the source node. After the last remote service is de-registered from the *Service Discovery*, the node is ready for deletion and can be shut down and removed by the *Cloud Coordinator*.

7.6 Conclusion

This chapter presents the architecture of SpeciAAL: The main objective relates to the possibility of scaling computing resources on demand in cloud computing. After presenting the principles of dOSGi, the complete 3-tier architecture based on Apache Stratos, CXF and ZooKeeper is explained. This PaaS layer enables elasticity for OSGi based applications and platforms like SpeciAAL. The IaaS interface with jClouds can control resources in hybrid cloud environments and may even offer cloud bursting strategies for times of high demand.

The detailed description of the scaling module of SpeciAAL is followed by a technical simulation and a scenario-based evaluation for the different main scenarios.

The PaaS presented combines existing solutions with current possibilities by combining important concepts, such as the use of the commonly used middleware based on OSGi (with the possibility to install, start, update and delete components during runtime, an integrateable repository of installable bundles, and the characteristic of being lightweight, as introduced in section 5.1), with the flexibility, interoperability and scalability of cloud computing (see chapter 3). In doing so, deliberate attention was paid to the versatility (also across IaaS provider boundaries) but also to the large existing market of system providers that can be docked onto the new solution as a COTS.

The first part of this chapter was published in the peer-reviewed paper "A Scalable Architecture for Distributed OSGi in the Cloud" (Kuijs et al., 2016).

Chapter 8

Field-Test: Service Adaptation

Based on the use cases presented in Section 6.2, an ontology is being developed to model the user's context, forming the basis for service adaptation. Using ontologies to represent entities in a system for AAL is not a novel approach, as described in Section 2.5. As adaptability of services stands as one of the key acceptance factors in AAL systems, it constitutes a central element for further work. To model the user's profile and environment, the dedicated SpeciAAL ontology is utilized. This ontology contains all the necessary information about the user and their relevant personal environment to modify SpeciAAL services and applications accordingly, such as their impairments, interests, and hobbies. The stored profile of the user can be accessed by the SpeciAAL platform through an access control mechanism, deciding which service is getting what kind of information about the user.

8.1 SpeciAAL Ontology

For an optimal personalization of the SpeciAAL system, the user context must be modelled, the information should be semantically connected to each other and there should be rules describing the usage of the single information. As a result, the context information is modelled in form of the SpeciAAL ontology, which enables the description of information relationships and to deduce or uplift new

data out of existing information. For example, if the system knows about the health condition of a user, capabilities, and impairments could be deduced out of it.

The procedure of the ontology design for the SpeciAAL platform is based on the approach of (Noy and McGuinness, 2001) and the ontology is developed iteratively and adjustments of the ontology are possible in the whole life cycle of SpeciAAL. The core idea within the ontology revolves around the user, characterized by their profile. This concept was taken directly from the project MobileSage (Skillen et al., 2012b), as described in the Section 2.5. The main user profile encompasses various sub-profiles such as preferences, health, or interests. The SpeciAAL ontology is the base for saving, classifying and interpreting context information. Automatic updates of the concepts or just the individuals of the ontology must be possible. It specifies the way of describing the user, his properties, and his environment for all components of the SpeciAAL platform, particularly for the personalized services. The ontology describes primarily the user and his properties, but additionally the user's environment like weather, time, date, devices/sensors, etc. In Figure 8.1 an overview of the basic concepts of the ontology are shown.

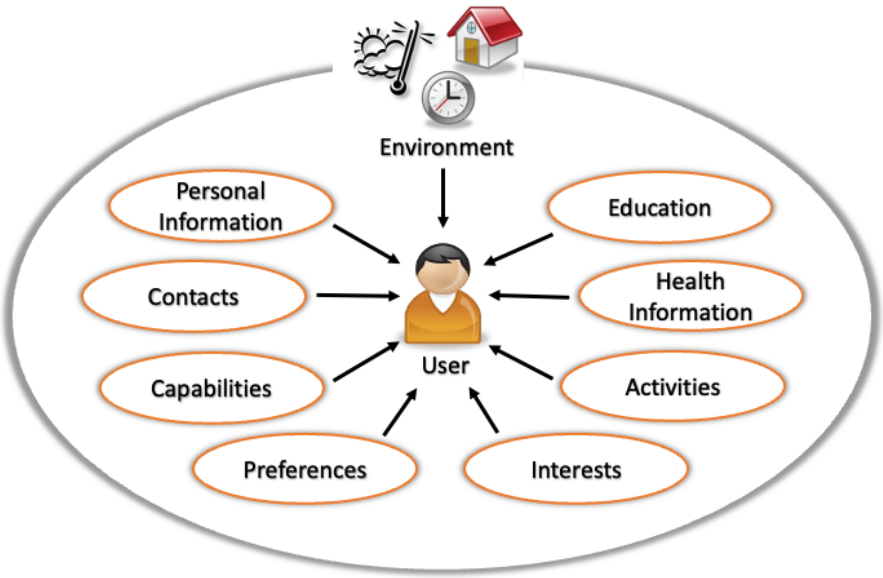

Figure 8.1: Overview of the basic concepts of the SpeciAAL ontology

In addition to the mandatory user data like the personal information (name, address, date of birth, contact information, etc.) there are some more specific and

more complex concepts like the interests, preferences, capabilities, or the health condition. Many of the ontology classes are fixed defined classes, defining the properties an individual of this class must have. This leads to a better consistency of data. The central role of the user is reflected in the class User, as shown in Figure 8.1. It is connected via properties to almost every other main class of the ontology.

The needs, interests, health condition, etc. are gathered in several ways. On the one hand, there is a manual acquisition of user data during the initialization of the system by the user or a personal assistant and on the other hand, there is a continuous analysis of context data through e.g. sensors resulting in the adaption of user and environment data. The environment information is collected in a non-personalized system database.

In order to keep the ontology up to date, a central instance is needed to ensure that any suggestions for changes can be received from users and developers, to check whether these changes are relevant and to ensure that they are implemented in a future version of the ontology. This central role can be assumed by the platform operator (see Section 2.4), for example, or alternatively by a consortium of operators of the same infrastructure.

8.2 Advantages of Adaptation Based on Ontology

There are several advantages of the SpeciAAL ontology. These advantages may be summarized as follows:

1. Context awareness is a mandatory requirement for optimal assistance for elderly people. It is also important not to consider only the environment of assisted persons, but especially the assisted persons themselves and their needs. The SpeciAAL ontology offers a **centralized user view**. Therefore, useful information about the user can be applied to offer personalized services.

2. All **services are adaptable to the user's needs**. They can use information

about the capabilities, impairments, interests, etc. of the person and can tailor their user interface and also their functionality to the abilities of the user. For example, they can control the volume, the font size or the colours depending on the condition of the ears or the eyes of the user.

3. Due to the **historical view** integrated into the ontology, it is also possible to react to changes of the user profile. The services can, for example, repeat helpful information if the user begins to suffer from dementia.

4. The ontology is used within the SpeciAAL platform as a common understanding of the user profile data. It is used to semantically interpret the user context in the different use cases.

5. Another benefit of the ontology is its facilitated **expandability**. This is because of the centralized concept *User*, where it is easy to add new properties to expand the user profile. Other reasons are the hierarchical structure and the reuse of concepts by many classes. Only currently useful information is saved in the ontology for a better data privacy. Concepts which turn out to be relevant in the future can be easily integrated into the ontology.

Now that the groundwork has been laid for the implementation of the entire system, an initial field test is being planned. For this purpose, prototypes are being developed so that the test users can operate the created use cases themselves and provide direct feedback on the system.

8.3 Developing a Prototype for Proof of Concept

An Android app for tablets was developed to better present the mechanics presented (see 8.2). The app accesses a server based on OSGi in the background and can manipulate data as well as be graphically adapted to the needs of the user (for example, regarding the font, the font size or a higher contrast). In the server application, it is possible to change ad-hoc settings, create events and change certain types of context via a web front-end. For example, in the events or information

app, it is possible to change the time and date to simulate the system behaviour concerning upcoming events (see Fig. 8.3). Other examples are the state of health of the user, or the current weather situation.

This preparatory work was not only necessary for presentation at conferences, but could also be used in the further course of user tests and group discussions.

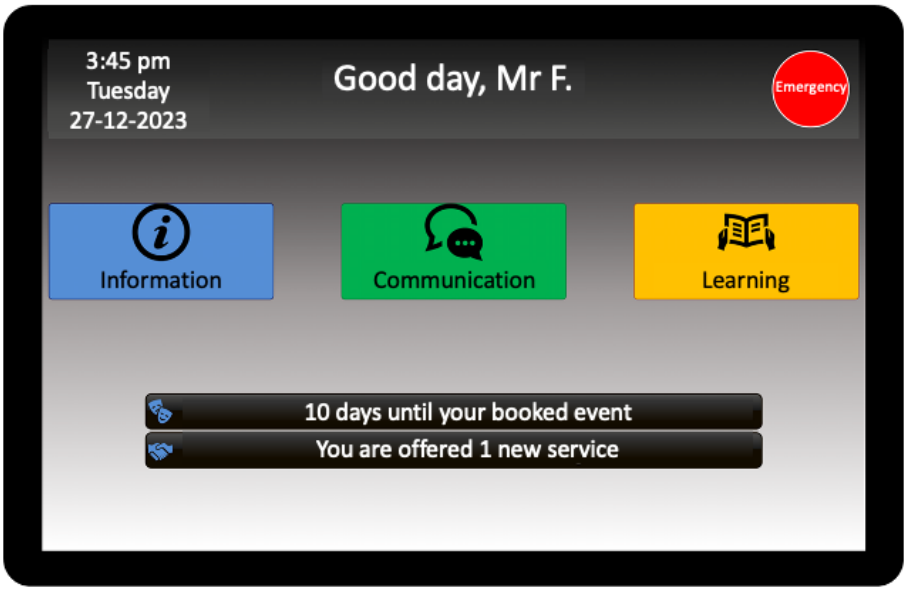

Figure 8.2: Welcome dialogue of the SpeciAAL prototype

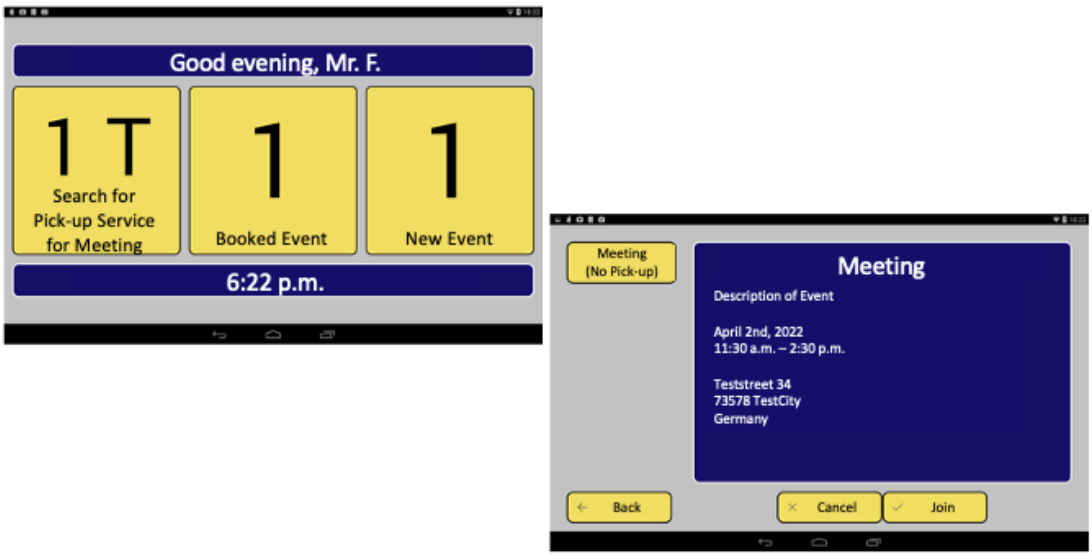

Figure 8.3: Screenshots of the SpeciAAL prototype events and information app

8.4 Field Testing

After defining the use cases and designing the SaaS architecture of SpeciAAL there was the possibility to conduct a group discussion and a first field test together with sociologists and gerontologists of Hochschule Ravensburg Weingarten (HRW). HRW is also a university for applied research, but is very well networked in the field of ageing research and geriatric care. They were able to recruit test persons for the group discussion. The scenarios, use-cases, technological background, the prototypes as well as the presentation of the platform were part of this thesis. The partners of HRW recorded the discussions, recorded and coded the given answers given by the participants for later analysation. All results from this field test were published in a joint project and compiled by the author of this thesis.

8.4.1 Group Discussion

Based on the described use cases (see Section 6.2), a group discussion with individuals out of our target group was organized together with HRW. Based on inclusion and exclusion criteria (e.g., age, technical affinity) suitable and interested subjects could be found in regional senior citizens' organizations. The group discussion was conducted in three rounds with a total of thirteen people aged between 67 and 79. Of the participants, nine are female and four male, eight live alone and five lived in two-person households. Overall, the subjects have a predominantly higher level of education.

After a brief presentation of the basic usage scenarios backed by flow sketches (see Appendix A), the use readiness, suspected chances and risks and the applications of the system were discussed. Although the target group members were not situated in a rural region but inhabitants of an urban environment, many analogies to our original considerations for support scenarios in communication or information retrieval support could be identified.

The main discussion was guided by a list of questions towards prospective user

reviews concerning the relevance, completeness, application, and the chances or risks of the system. The key questions that were asked are:

1. In your experience, what are the biggest barriers to or in the use of existing technologies, such as PCs, tablets, smartphones, etc., especially for older people?
2. To what extent do you believe that the technology presented can be useful (especially for people with less technical experience) to facilitate access to different **communication channels**?
3. To what extent do you think that the technology presented can be useful (especially for people with less technical experience) to facilitate the search for different **types of information**?
4. Where do you see the opportunities of the technology presented?
5. Where do you see the risks of the technology presented?

The main results of this discussion were:

- Based on the view of the elderly individuals, the technical system was difficult to understand but could be clarified during the discussion.
- Contemporary technical products are generally considered not elderly friendly or easy to use by elderly individuals (e.g., font-size, contrasts, or vocabulary)
- Based on the latter, they welcome a simpler application for communication and information retrieval.
- Based on the proposed use cases, additional use cases are introduced by the participants, such as mechanics services, shopping services, and commercial services.
- Data protection and the financing of the proposed system, as well as questions concerning the individual support services for introducing such a system, were critically discussed.

- The selection of potential users based on their cognitive abilities or financial possibilities was considered a major risk.

- Another danger is seen in promoting isolation, making the user stay in his own home, or weakening mental capabilities by simplifying complex tasks too much.

These findings were also discussed at the European Nursing Informatics Congress (ENI) in 2015 (Rosencrantz et al., 2015). The last point is also backed by the work of (Wilkowska et al., 2022): Especially for the primary group of stakeholders in, AAL it is important to offer perfect transparency (What is the system able to do?), make the user the master (How can the system be controlled or deactivated?), and to fight laziness (Keep the user active and activated).

8.4.2 Setting

To carry out a first field test, the use cases (see Section 6.2) were further refined to show different system reactions to the test subjects. These were also used as a basis for our use case tests to verify that the prototype was working correctly in slightly modified scenarios. A web interface was introduced to change and vividly demonstrate the initial situation during our tests. With this interface, it is possible to mock the state of the user to present the responsiveness and adaptability of the system. Depending on the desired state changes, the modifications are directly carried out in the ontology backed database of the test user.

The main prototype for the evaluation was developed on a 10-inch Android tablet (see Figure 8.2). The use cases for communication and information retrieval are merged into one application to gain a uniform user interface.

To communicate with a contact from the user's address list, he just has to choose the contact (see Figure 8.4). The system automatically identifies the prioritized channel for a given time (e.g., mobile phone, landline, office phone, short message) and directly connects the user. The sometimes difficult task to choose the right

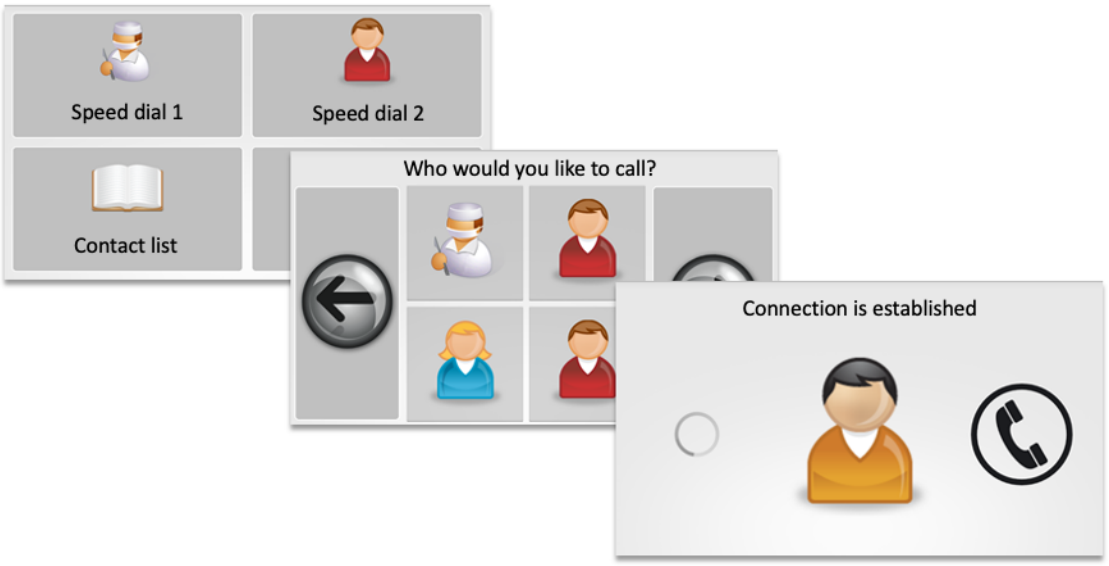

Figure 8.4: Screenshots of the SpeciAAL prototype communication app

channel is taken from the user and directly carried out by the system (see Figure 8.5).

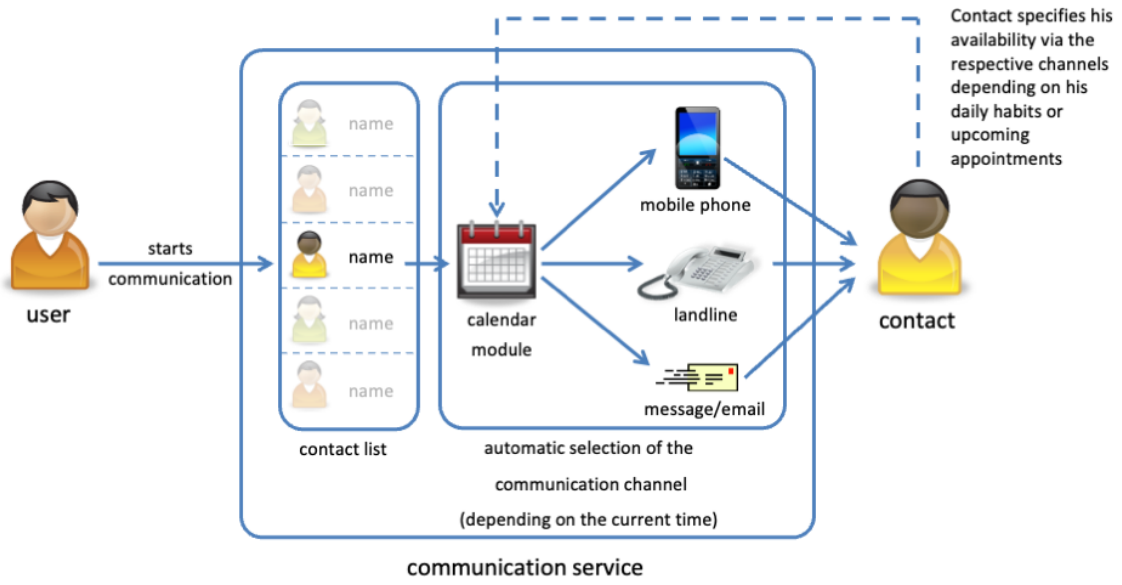

Figure 8.5: Use case for adapted communication

In the second presented use case (see Figure 8.6) the user is supported in attending events and organizing household help. The user is only presented items of a local calendar of events that match his stored interests, and can then decide whether he wants to attend them or not. Once a day, the user is asked about his general state of health. In case of health deterioration, the system can search for a lift to the event or to cancel the participation. To demonstrate the household help scenario

within the prototype, two additional global states were introduced: Snow weather conditions and an empty fridge. Upon detection of these conditions, the system automatically provides services to ask for someone to help with shovelling snow or to organize shopping help.

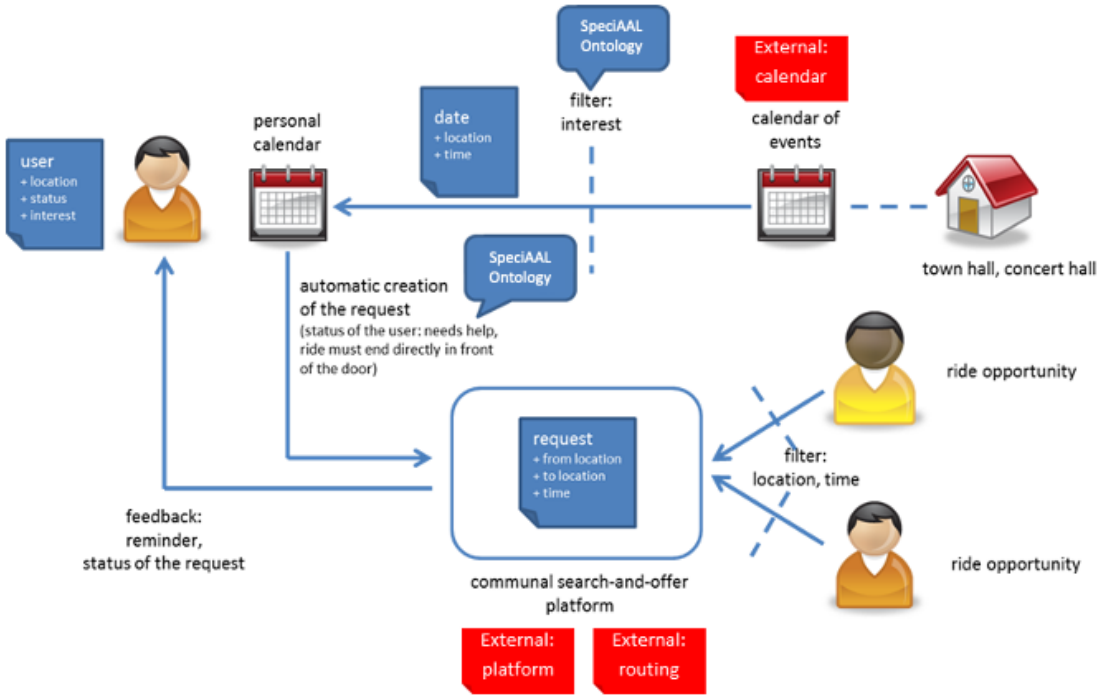

Figure 8.6: Use case for adapted information retrieval

8.4.3 Procedure

To be able to easily demonstrate the personalization functions to our test subjects, a fictive user with his characteristics (health, interests, social environment and housing environment) was presented. The different functions of the prototype could be tested, and the adaptability of the platform was demonstrated through various tasks that the subjects were supposed to solve on the tablet. Following the presentation of example scenarios, the test participants were able to independently explore the prototype system. Because the field tests were carried out in three separate groups, the team of HRW collected field notes. These could be used to document unplanned changes in the demonstration process or technical difficulties to be later considered when evaluating the results.

Figure 8.7: Introduction of scenarios

Following the prototype tests, AttrakDiff (User Interface Design GmbH, 2008), a standardized questionnaire regarding the user experience (see Appendix B), as well as individual interviews were carried out. The standardized questionnaire assesses the subjective perception of the user regarding the operation and appearance of an interactive product. 28 opposing pairs of words (e.g., simple vs. complicated; see Appendix B) are given to the test subjects with which they are to classify the product. The assessment of interactive products is a significant activity within user-centred design. Questionnaires typically serve as an evaluation technique, primarily focusing on the usability or "user-friendliness" of a product. However, there's ongoing discussion regarding additional quality aspects known as "hedonic" qualities. These are rooted in human needs for stimulation and identity, while pragmatic quality addresses the need for controlled manipulation of the environment (User Interface Design GmbH, 2008).

After filling out the questionnaire, individual interviews were carried out according to previously prepared guiding questions. Besides questions concerning the overall usability of the system by the elderly people, the main interest was the presumable benefit a system like this could offer elderly people (based on the demonstrated use cases) and the assessment of support to enable elderly people to stay in their known environment for as long as possible.

Figure 8.8: Test subjects solving tasks on tablets

8.4.4 Results

During the evaluation of the system, smaller usability problems (e.g., unclear text-buttons) could be identified and fixed directly after the evaluation. Recurring questions could be recognized as a process problem during the interaction. Most of them could be mitigated by changing textual feedback in the dialogue boxes.

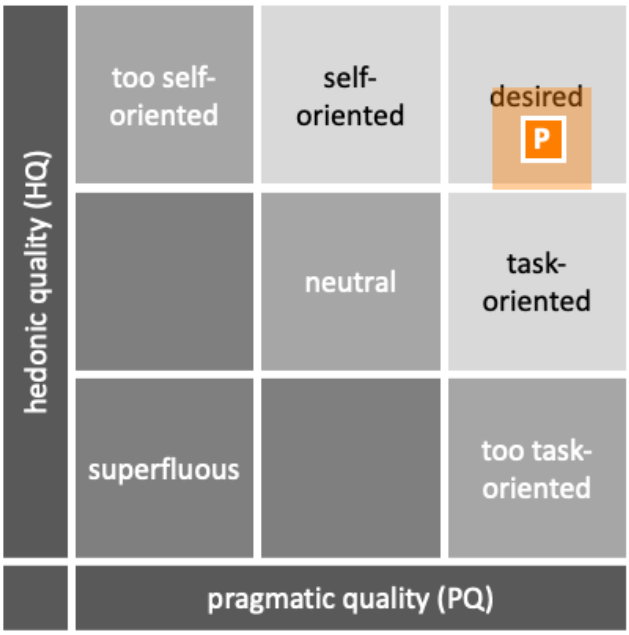

Figure 8.9: Average expression of the dimensions pragmatic and hedonic quality and the confidence rectangle (User Interface Design GmbH, 2008)

The AttrakDiff (User Interface Design GmbH, 2008) questionnaires of the thirteen

test subjects were evaluated with the according web evaluation tool. The user-interface is unambiguously classified as desirable. In Figure 8.9, the result of the survey is marked with a "P" on the two axes "pragmatic quality (PQ)" and "hedonic quality (HQ)". The semi-transparent orange area represents the so-called confidence interval. The smaller the area, the more uniform the answers given. The prototype is pragmatic and supports the user optimally. The subjects can identify with the product and get stimulated and motivated (hedonic quality). Optimal results are achieved in the areas of attractiveness and identity, only small optimizations could be achieved in the area of motivation. For a detailed view of the results for the different word pairs see Appendix B and Figure B.1.

Figure 8.10: Evaluation of the prototype

After structuring and summarizing the audio files of the individual interviews, a qualitative content analysis was carried out. Central findings show a fundamentally positive attitude towards the prototype and the system. However, the test subjects see themselves as healthy, active and sufficiently independent to master everyday life without the support of technical systems. In their point of view, later generations will be more open-minded and there will be more demand for technical support systems, due to earlier and larger technical experiences during their lives.

An early approach to and with the technology is rated as positive, and a surplus value is recognized in integrating the system into everyday life. As a prerequisite

for the application of the system, it is pointed out that it should already be learned and used in the healthy state, to be able to handle it in difficult situations. This contradicts the assessment that the technique is not necessary or helpful for the current life phase. It should also be noted that people from a generation who have been faced very late with technical innovations can see the program and its benefits, but do not want to suddenly replace their own everyday routine with an innovative system.

Basically, it is stated that this system is already self-explanatory to people without technical affinity and the risk of mistakes seems almost excluded. The use of the SpeciAAL system as a whole is very uncomplicated. This evaluation was made by the participants independently of their previous experience and skills in ICT. An introduction and start-up aid seems necessary for some participants to overcome the first scepticism about this system and to avoid (alleged) hurdles with it. It was emphasized that the presence of support services is important, which could be connected with the application of the system (e.g., introduction, consulting, technical support). For social participation, no compulsory added value is per se shown by the system, but it could provide impulses for an activity by adapting the system to the personal profile, displaying information about individual interests. The physical and mental capabilities of an elderly person were described as a prerequisite for participation.

Based on all individual interviews, it can be pointed out that the respondents emphasized the intuitive usability of the prototype and at the same time separated themselves from people in need of assistance and support. This is especially due to a good to very good health condition, a high level of personal activity and a social involvement of the subjects at the time of the field test (selection effects for the sample of participants) and there was only a limited desire or ability to put themselves into the scenarios presented. Nevertheless, there is an awareness that personal health may change or deteriorate in the future and the need for technical assistance in terms of communication support and information search will increase.

As already described in Section 8.4.1 the preservation of privacy and the question about which entities in a system to AAL have access to what PII has been an important aspect for the test subjects. When asked about the acceptance level for introducing a service platform like this, some of the subjects were aware that many free existing services are paid by user data input, and that transparency in data usage is key for the user and the introduction of new services.

Some subjects had doubted that the financial support of the health insurance alone would suffice for such a service. With recent news in mind, about data leaks and personal information disclosures, they were expressing their fear about a system that they cannot control and that would even turn against them.

8.5 Conclusion

In this chapter, an ontology for storing and semantically structuring context for service adaptation in the SpeciAAL platform is presented, and the main functionalities are described. The subsequent field interviews were conducted with a previously developed prototype. The tasks carried out as part of the thesis included finalising the prototype, dynamising the server backend (to simulate rapid context changes such as different times of day, different health conditions or weather changes), outlining the key questions for the user survey and developing the use cases, including the creation of graphics and posters. In addition, the AttrakDiff questionnaire (User Interface Design GmbH, 2008) was used as a standard measurement tool to provide additional feedback on the user experience of the prototype. During the implementation, the author of this thesis guided through the programme, presented the prototype using the posters and addressed questions during the discussion.

The findings of this discussion and foremost the concerns about privacy preservation in SpeciAAL lead to the second part of the thesis, in which I try to address the privacy concerns of the test individuals.

This work was done during the research project ZAFH-AAL (Kunze and Renyi, 2015)[1]. The findings of the field test were published in the peer-reviewed paper "Entwicklung einer Informations- und Kommunikationsplattform für ältere Menschen." (Rosencrantz et al., 2015).

[1]The project ZAFH-AAL ("Zentrum für Angewandte Forschung an Hochschulen für Ambient Assisted Living") is funded by the Ministry of Science, Research and the Arts of Baden-Württemberg, Germany. The funding program for the universities of applied science is called: Zukunftsoffensive IV "Innovation und Exzellenz" (ZO IV).

Chapter 9

Context-Aware Access Control in SpeciAAL

As outlined in Section 8.4.4, a crucial factor for acceptance revolves around safeguarding personal data within the system. Users within the target demographic prioritize transparency and trustworthiness in the system provider, while also emphasizing the reliability of its technical implementation. Consequently, ensuring secure access to personal data stands as a paramount concern addressed within this chapter.

To protect privacy, design strategies can be used when designing a system from scratch. In general, a design strategy describes an abstract approach to achieving a particular design goal. A listing of eight different strategies is presented by the ENISA (Danezis et al., 2015). In addition, each strategy identifies design patterns for implementation. The presented approach mainly centres around the three strategies (see Section 4.6):

- **Inform:** Data subjects should always be informed about which information is processed, for what purpose, and by which means when using a system.
- **Control:** To gain user consent for processing of personal data, the user has to have agency to view, update or delete personal data at any given time. Above this, a user can control and define the data that is processed and

whether to use a certain system.

- **Enforce:** To ensure that a privacy policy is in place, there should always be one enforced by default that is compatible with legal requirements.

With these principles as goals and following the guidelines of Cavoukian (2010), this chapter describes the basic structure of the SpeciAAL Privacy Monitor (see Fig. 7.4).

The architecture Privacy Monitor can be divided into two main components.

- **A Monitoring Component:** An OSGi monitor component that enables the user to be **informed** of the personal data in use.

- **An Access Control Component:** On top of these, a policy language is developed that can be enriched with context-aware conditions to support the special needs of users in AAL environments. A SpeciAAL access control system, that is based on that defined policy, enables the user to **be in control** of the overall system and **enforces** rulesets to the collected personal data.

9.1 Requirements

The goal is to introduce a central control authority for the regulation of access in SpeciAAL. The novelty is seen in the possibility to define access-rules based on context information, that is used as an additional attribute in access patterns. This approach provides finely granular access rules with greater flexibility and precision in controlling access to sensitive data or resources based on specific attributes or conditions. But this can lead to authorization policies that can be complex and difficult to manage. To ensure that policies are effective, they must be easy to understand, update, and enforce.

To meet the previous requirement of the SpeciAAL platform, the system has to be able to provide a unified integration of variable data sources. The provided

solution has to be interoperable, lightweight and extensible to meet subsequently formulated requirements.

9.2 Monitoring Component in SpeciAAL

To protect the potentially personal data inside the platform in SpeciAAL, monitoring has to be initially implemented at all trust boundaries.

Definition 9. *"The distinguishing feature of a trust boundary is that the system's owner is trusting every system (sentient or automaton) that lies within the trust boundary." Thomborson (2010).*

Trust boundaries are defined at the interface of OSGi modules that have different groups based on user access privileges. This analyses the flow of data and is used to show the user which services can access which data (design strategy "inform", see Danezis et al. (2015)). In Figure 9.1 all relevant spots for monitoring are illustrated: It must take place between installed bundles, between bundles and the database, but also at interfaces to other parts of the AAL system (e.g., web-interfaces or interfaces to external services).

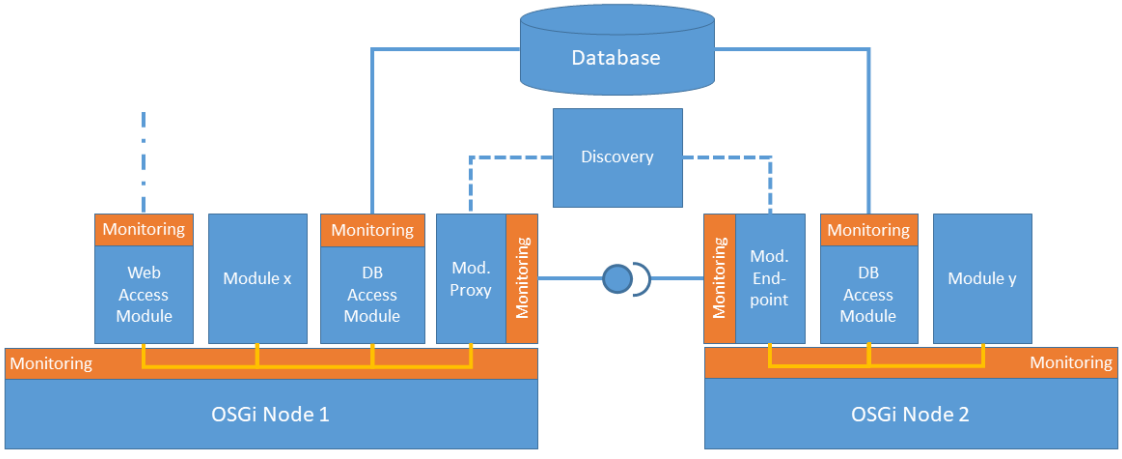

Figure 9.1: Monitoring in SpeciAAL

In this approach it is realized by a central protection bundle, that automatically creates a proxy service during the deployment of a bundle in OSGi that mirrors the original bundle with all its methods. By injecting logging facilities inside the

proxied bundles, it is possible to log access to the data source of the service but also indirect access between bundles and to external interfaces. The gathered information of the logging implementation can then be stored and presented to the user in a simplified and non-technical way. In a second step, these proxies can be extended by decision logic to allow or deny communication with other services within the platform. This enables us to have detailed control over the data flows inside the environment SpeciAAL without the need to have full control of all installed bundles before deployment or doing security checks and code inspections of all bundles to whitelist them for use in the AAL environment.

The OSGi-Core specification describes an Event Listener Hook, to respond to events in the Service Registry (The OSGi Alliance, 2014, Chapter 55.4). This hook is used to inject program code in the service registration process. The automatic generation of the proxy is triggered and using Java Reflection (Glen McCluskey, 1998) a proxy class is generated that acts on behalf of the actual class and accepts their calls. It offers the same methods as the original class and can be extended by code functionality to log its activities and control its behaviour. To ensure that the proxy and not the original bundle is called by other bundles in the OSGi environment, the proxy is prioritized higher in the Service Registry of OSGi (The OSGi Alliance, 2014).

The call of the OSGi hook is realized by implementing a *Component Protection Bundle* within the OSGi environment and allows us to apply the generated access rules to the system. Figure 9.2 shows the sequence diagram of the access between a caller bundle and the service bundle through the presented proxy mechanism. In this example, the requested *name* is only accessible if the access is authorized inside the *Proxy Service*.

9.3 Access Control Component in SpeciAAL

To realize the design strategies "control" and "enforce" (Danezis et al., 2015) the presented approach is an access control system based on the established XACML

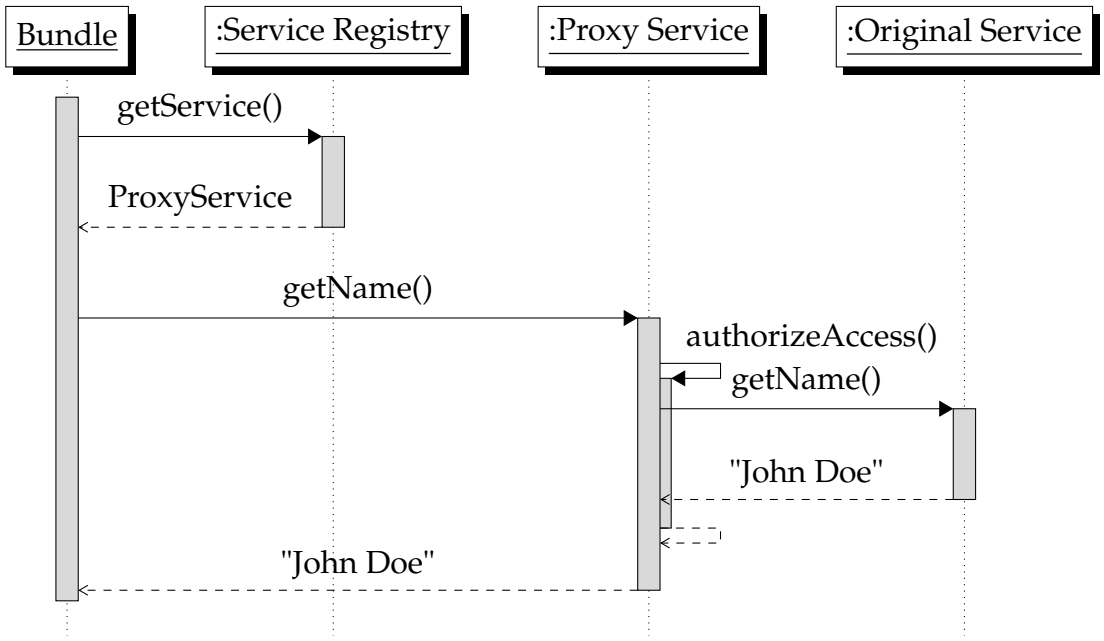

Figure 9.2: Sequence diagram for access control

reference architecture by Kafura (2004).

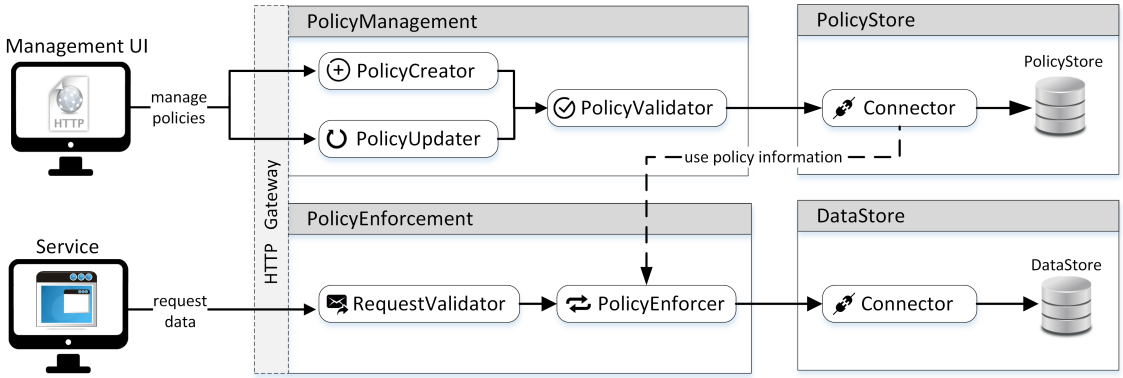

Figure 9.3: Architecture overview of the SpeciAAL access control system

The system's structure, illustrated in Figure 9.3, is divided into two key areas: the creation and administration of authorization policies, and the safeguarding of access patterns during data retrieval requests. A particular focus of the developed platform was to ensure the highest possible interoperability for the integration of many individual services. To keep it simple to operate for the target audience, the system also has a central user interface for administering the policies. The purpose of the user interface is to provide the user with the highest possible level of transparency and comprehensive control over the granted authorizations, while abstracting the technical details. Thus, the user can always manipulate existing

permissions, remove them when deactivating a service or grant new permissions.

The *PolicyManagement* module contains the subcomponents for creating and managing authorization policies. The creation of a policy can be done via user-friendly input forms within the user interface or by importing pre-defined XML files. In the case of form-based authoring, the information about the authorizations to be granted is provided via HTTP endpoints of the subcomponent *PolicyCreator*. Using the subcomponent *PolicyValidator*, these are first checked for their semantic correctness and then a corresponding XML file is generated. However, a particular focus of the implementation of this component is the ability to integrate pre-defined authorization policies by allowing services to provide them directly to the user during service deployment. To preserve transparency and control for the user, the access rules defined within the XML files are initially interpreted by the platform and presented in a readable form within the user interface. Therefore, the user has the choice to effortlessly deactivate specific rules or modify them according to their preferences. One characteristic of the user interface is the possibility of adding context to the access rules, that may permit the access of data or functionality only at a special time, a special location or in special occasions. If new policies are inserted in this way as an XML file, an additional review of syntactic correctness will take place.

The created policies are stored within the *PolicyStore*, in which the contents of the authorization policies are transferred to a relational data model for high-performance and targeted querying. Due to the defined interfaces, the platform supports both local and remote database systems, which can be used individually depending on the desired form of the platform. Since the allowed access patterns can also change over time, an additional option for manipulating existing policies has been integrated into the platform. This is done via the component *PolicyUpdater*. Manipulating existing policies is equivalent to creating them by updating existing information, either through user interface forms or directly within the corresponding XML files. Such a case has relevance both in the delivery of a new version of the service concerned and in the need for manual adaptation of the rules

by the user. The associated component also provides this functionality via HTTP endpoints, which, after successful completion, result in an update of *PolicyStore* data. Because of the resulting interfaces, it is also possible to integrate this functionality into higher-level applications, such as a central instance for managing all permissions within a given domain.

The depicted lower part of the Access Control Component (see Fig. 9.3) is responsible for the enforcement of the created authorization policies within the module *PolicyEnforcement*. An entity attempts to access the stored and protected data within the *DataStore* by specifying its own identity, the desired resource and the respective access pattern by calling the defined HTTP endpoints of the *RequestValidator*. The indication of the identity has particular relevance to counteract possible abuse. For this, a certificate-based matching of the identities within the *RequestValidator* takes place. If the given identity can be confirmed, the request is forwarded to the *PolicyEnforcer* component. Using the stored policies, this component checks whether the requested access corresponds to the defined authorizations and, if positive, responds with the requested data. In the negative case, access to the data is denied. The verification of the permitted access patterns is done similarly to a conventional firewall systems in decreasing granularity. As soon as a corresponding rule has been found, access is immediately permitted or denied. This allows for efficient processing of data access by considering only a subset of all rules. If the data access is permitted, the data can be queried by use of the connector component of the respective persistence media.

9.4 Privacy Policy in SpeciAAL

To integrate the crucial contextual aspects, pivotal in AAL use cases, into the formulation of access rules, an initial extension to the current privacy policies is imperative. Furthermore, it's essential to ensure that the formulated rules not only fulfill the necessary criteria but also cater to older individuals and those without technical expertise, ensuring clarity and comprehensibility for diverse user groups.

This inclusivity aims to make the rules easily accessible and understandable, fostering usability across a broad spectrum of users with varying levels of technical proficiency.

The privacy policies that are currently discussed, are the P3P (Cranor et al., 2006), S4P (Becker et al., 2010), and SIMPL (le Métayer, 2009). P3Pdescribes privacy information of websites, such as editor information, collected data, dispute scenarios and retention time of data. S4P, on the other hand, is used for privacy descriptions of services and what personal information is used for what purpose. SIMPL is used to specify preferences and policies with a small subset of English. Only a small part is already specified for future use, and it is not easy to comprehend for humans. To keep the policies in a natural language and easy to understand for

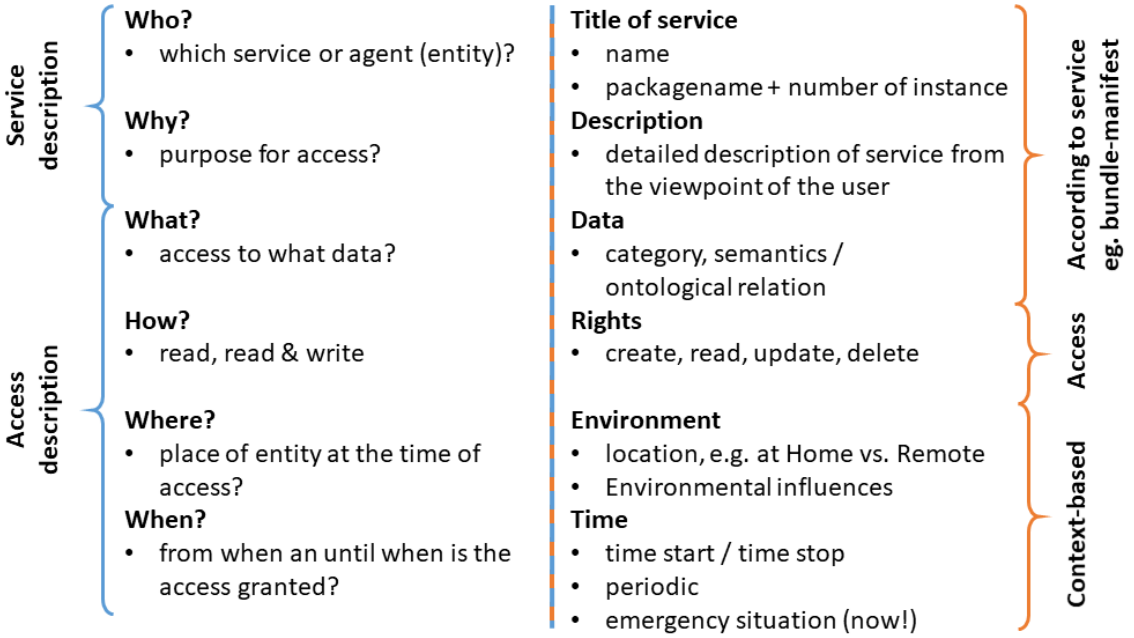

Figure 9.4: Proposed privacy policy based on 5W1H questions

the target group of AAL, the approach is to give answers to the 5W1H questions (shown in Figure 9.4). On the left side, the questions are listed (each followed by a corresponding example), divided in a service description and access description part. On the right side, the technical implementations and corresponding configuration options are shown. *Title* and *Description* can be found in the manifest-file of a bundle, data defines the accessed data category of the information to be processed by the service, and the Access-Rights are based on the CRUD acronym. Special

to the use case in AAL is the possibility to add context to each policy. In this early stage, environment based and temporal context is supported, where the environment considers the location of the user, external influences, or emergencies. Temporal context-based access could be periodic, e.g. during working hours on week-days, to preserver the user's privacy during night and on weekends.

To put it in natural language:
An entity is provided access to data for some defined task, if the particular context applies - otherwise access is forbidden.

This flexibility leads to very fine granular access control mechanisms that can be applied by applying the policy language.

The basis of the proposed access control system is the definition of the authorization policy. The chosen structure of the policy is based on the lightweight representation of the eXtensible Access Control Markup Language (XACML) by Kafura (2004). XACML is a declarative, attribute-based markup language for the presentation of authorization policies and is characterized in particular by its high interoperability, extensibility and the resulting general validity. The main aspect of the definition of an authorization policy are the data to be protected, which vary depending on the specific application scenario, the sensitivity and purpose. To efficiently map this variability, the definition of an authorization policy is based on the requesting entity. This design choice results in increased flexibility, in which new services can be added, or their privileges can be revoked or manipulated without global impact.

```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <policy PolicyID="HeartRatePolicy">
3     <Subjects>
4         <Subject>NursingService</Subject>
5     </Subjects>
6     <Rule RuleID="ReadHeartRate" Effect="Permit">
7         <Resources>
```

```
            <Resource>HealthData</Resource>
        </Resources>
        <Categories>
            <Category>General</Category>
        </Categories>
        <Actions>
            <ActionMatch MatchId="
    HeartRatePolicy:HealthData:General:Read">
                <AttributeValue>Read</AttributeValue>
            </ActionMatch>
        </Actions>
        <Context ContextID="onlyInternal">
            <Apply FunctionID="Location (internal)" />
        </Context>
    </Rule>
</policy>
```

Listing 9.1: XML example for the proposed authorization policy

This is depicted by the attribute *Subjects* shown in listing 9.1. In addition to defining the services involved, a policy includes a variable set of rules that are used to determine the desired access permissions. A rule always refers to a concrete resource that can be further restricted by specifying a *Category* for fine granular authorization assignment. In a first attempt to categorize the data, the main concepts of the implemented ontology are used (Fredrich et al., 2014): Personal information, contacts, capabilities, preferences, interests, activities, health information, education and environment. The heart of such a defined rule is the attribute *Actions*. Within this, the permitted access patterns can be defined (according to the CRUD acronym).

To ensure context-sensitive access authorizations, the defined rules can be supplemented with additional conditions through the *Context* attribute. The available conditions are defined by the Privacy Policy and include, for example, mapping

time- or location-dependent access patterns. In the presented, authorization policy includes a location restriction of the permitted accesses.

The default behaviour of the developed solution prevents any data access without an appropriate policy, which is why all access patterns of a service must be defined within a corresponding rule. The individual rules are interpreted sequentially and therefore have to be defined in descending access granularity. The described structure of an authorization policy can be arbitrarily extended to represent more complex access authorizations and has the possibility to be converted into a format conforming to the XACML specification that provides complete interoperability with deviating implementations.

9.5 Examples for Application of Policy

To illustrate the newly added possibilities, illustrative examples are described below that function based on the privacy policy. The first example is an online medication plan that is connected with a drug dispenser. The three information that are accessible for this service are: the *schedule* for the drug ingestion, the information whether the drugs have been *taken*, and the *reason* for the medication. The user always has the full access to his own data. Informal caregivers (e.g. a neighbour) may have access to the schedule (name and time to take the drug), professional caregivers (e.g. nurses or doctors) also know the reason for the medication and are allowed to control the taking of the drugs, but only (context-awareness) if they are visiting the patient. Figure 9.5 shows the example and the granularity of access rights, where the "if..." icon is indicating the described context-based attribute to the access policy. In the second example, a nursing service has the right to access all *values* of a heart rate sensor only when accessing the system from within the user's home (e.g. at the user's own terminal during a daily visit). Otherwise, the access rights only permit the access of *average* values. The informal caregiver has no rights to access the data, but this can be overridden by critical values. In this case, the contextual portion of the access right could be

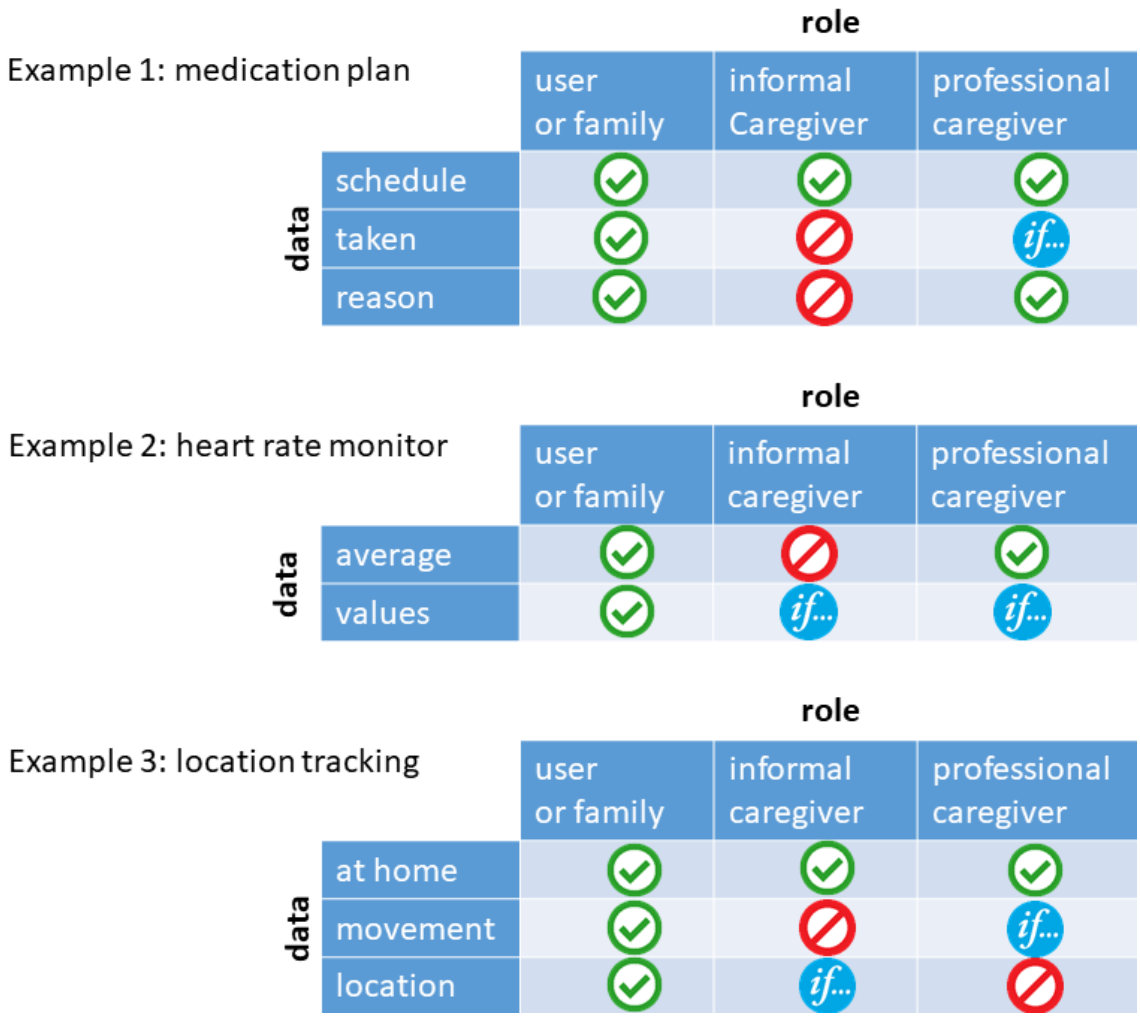

Figure 9.5: Examples for policies based on three groups of stakeholders

set to *in emergencies* (see Figure 9.5).

Our third example is based on a location tracking service, that can indicate, if the user is *at home*, *moving* inside his home, and can show his *location*. in this example, all stakeholders have the right to see if the user is at home, professional caregivers are allowed to know if the user is moving during weekdays, and informal caregivers are allowed to access the location of the user in case of an emergency.

These brief examples show the flexibility of our developed data access policy language.

9.6 SpeciAAL Access Control: Compliance with Requirements

The SpeciAAL Access Control component can meet the aforementioned (see section 9.1) functional (F1 - F5) and non-functional requirements (NF1- NF3) that are briefly described below:

F1 **Introduction of a central control authority for the regulation of access:** The main focus of the development of the access control system is the possibility to control all access to the stored data of the user. To make this possible, the platform is extended by a unit to control all data access. Since the accesses are made exclusively via the defined interfaces of the system, the data stores and data sources can be completely decoupled from the serving services. The central access control authority does not have full access to the stored data itself, but authorises data access after checking the access rules.

F2 **Unified Integration of variable data sources:** The variety of possible data sources, such as health gauges or recording the user's temporary environmental conditions, requires the definition of common interfaces for the persistence of the information. Thus, the data sources may use the functionality of the platform to store their recorded data, regardless of the persistence technology used. In addition to increased interoperability, this enables a flexible exchange of technologies

F3 **Possibility of finely granular definition of the permitted access patterns:** Since the access management based on the data categories often has no satisfactory granularity, it is necessary to subdivide these further. Thus, the defined policy language always offers the possibility of assigning individual subcategories.

F4 **Definition of context-aware allowed accesses:** The allowed data accesses can vary greatly depending on the service in their requirements. The high

flexibility of the authorization policies used to regulate the access allows an individual definition of specific access rules, which go far beyond the usual CRUD operations in this environment.

F5 **User-friendly definition and manipulation of authorization Policies:** According to the target group of the developed system, the simple usage is another requirement. Since the used structure of the authorization policies is primarily optimized for efficient machine readability, the system is extended by a natural language definition of the permitted access patterns.

NF1 **Lightweight:** When operating on resource-poor hardware, it must not be restricted in its functionality. This requirement is fulfilled by the streamlined structure of the authorization policies, as well as a lightweight and individual implementation for machine processing.

NF2 **Interoperability:** The SpeciAAL Access Control component enables the integration of versatile data sources and intelligent systems, as well as the consistent use of the platform by the requesting services. The services can access the platform via defined HTTP endpoints, creating a variety of integration options, such as the use of mobile device applications or web applications.

NF3 **Extensibility:** Due to the generic structure of the platform, a variety of application areas are possible. To meet the specific requirements of the respective domains, the implementation is based on a modular structure. This provides clear interfaces between the modules, which can thus be extended by adaptation or additional modules.

The requirements can be met with the presented solution. Whether the requirements for usability and simplicity of implementation (F5) can actually be met will be examined in detail in chapter 10.

9.7 The Impact of Privacy Enhancing Data Access Control to the Architecture

To simplify the scenarios, the final evaluation in chapter 10 deliberately refrains from defining more complex access rights. Especially in an extensible system in the cloud, it is very likely that processed information from one service will not only be accessed by another stake-holder, but will also be consumed by another service. This means that the services must be constantly monitored, and the access rights must be re-requested if necessary. The complexity further increases when considering additional scenarios in the hybrid cloud approach. In SpeciAAL this is handled by the *Privacy Module*.

To demonstrate the principle of operation of the *Privacy Module*, the installation process of a new service is described. As a simple case, it is assumed that the new service has to be run in the Public Cloud of our Hybrid Cloud approach for SpeciAAL. For privacy reasons and with the threads of Section 3.5 (e.g. Insufficient Identity Management, and Unsecured Third-Party Resources) in mind, this Public Cloud is considered as a third party with a low level of confidence.

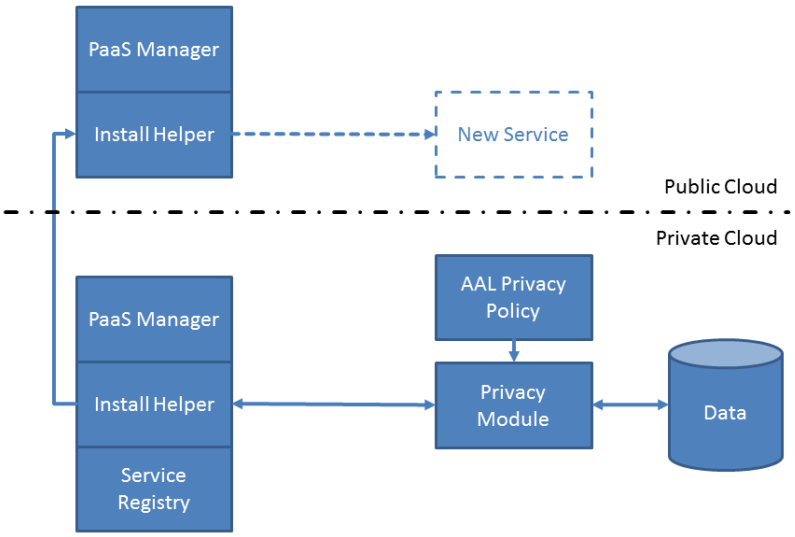

Figure 9.6: AAL Privacy Policy and Privacy Module

Figure 9.6 gives an overview of an installation process for a new service in the Public Cloud. It is assumed that the user has triggered the installation process

and by some requirements (e.g., shortage of resources or cost efficiency) the new service has to be started in the Public Cloud. The *Install Helper* then requests the needed data for the initial configuration and adaptation of the service. The Privacy Module checks the AAL Privacy Policy whether there are policy breaches in the requested information (e.g. by querying information categories that have not been released for the service or for which no rules yet exist). In this scenario, no breaches exist and therefore the data may be passed to the *Install Helper* which then passes it over to the *Install Helper* in the Public Cloud to install the New Service.

If the policy check fails, the *Install Helper* has to request new resources from the PaaS Manager to be able to install the service in the Private Cloud. One exception to this policy-driven decision-making could be, that the user actively enforces a service to get data beyond these policies, as shown in section 9.7.2.

9.7.1 Reevaluating data access

Besides installation and initial configuration, user data is also requested for adapting and reconfiguring a service during run-time. This reconfiguration is triggered by changes in user data that are reasoned by agents and combined in events. An example would be a fitness service with video-trainings that is reconfigured to exclude trainings for feet after the user has sprained his ankle. The service is registered in the service registry (as shown in figure 9.6) together with the documentation of the needed data for configuration. With this information, the *Privacy Module* can reevaluate if the policies are still met and the updated information is allowed to be passed in the Public Cloud.

This reevaluation is needed because a change in user data can mean that information that was not defined during installation of a service now has some value and is considered a breach of privacy. In the fitness example of section 6.2, the service was used with no restriction before the sprained ankle and after the information of the sprained ankle has to be passed as change in context for service adaptation. If the sprained ankle is defined as personal information (see chapter 4)

the reconfiguration requires the service to be shifted to the Private Cloud.

9.7.2 Transparency

One feasible solution for compliance when transferring user data to third parties is transparency. As a legal requirement, a user has to be informed about PII that is passed to third parties. This information can be used to 'override' the policies that are evaluated automatically in the Privacy Module.

In Google Android, the user is informed when installing a new application about what sensitive information will be used by the application (e.g. contact details or the whole address book) and the user has to decide whether the application is allowed to access the data or not (Google, 2023). Sometimes this decision results in not being able to use the application at all. This consequence is not seen as the desired behaviour for services on a Platform for AAL.

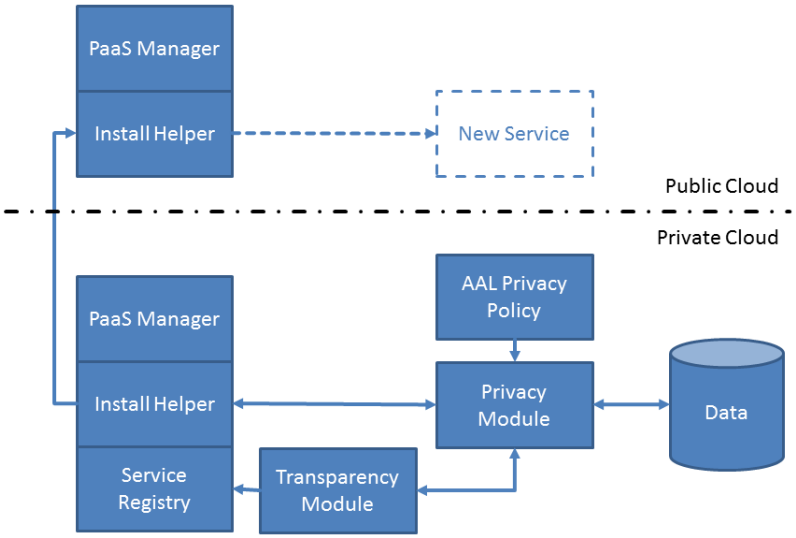

Figure 9.7: Privacy Module and Transparency Module

Figure 9.7 shows the same scenario as Figure 9.6 except this time there is a privacy policy violation and a malicious service tries to access additional data for which there is no policy. A Transparency Module is triggered about the violation and the user is informed about the personal information that will be passed to the service. In this scenario the user complies with the data transmission, the decision is saved in the Service Registry and the New Service is installed and started in the Public

Cloud. If the user disagrees, the service cannot be started in the Public Cloud.

9.8 Conclusion

This chapter presents the three main parts of monitoring, access control, and enforcement of privacy data in the platform for AAL: A) An OSGi mechanism to intervene in the communication process of bundles and has the ability to monitor and control data flows on service level (inform), B) an access control system to manage access rights based on rules, and C) a policy language to define these rules (control, enforce). The privacy policy language is extended by context awareness to better suit the requirements of AAL use cases.

By examining functional and non-functional requirements, it is shown that they can be met with the solution presented. Furthermore, the next chapter will clarify whether the basic assumptions of this solution (granular release of information, standard protection of data, context awareness) are also understood by users.

In the last section, the impacts of the solution on the architecture of the PaaS are shown. In particular, it focuses on where the policy may need to be reevaluated, or service migration prevented to maintain function.

Through this extension of the overall system, general access rights can be assigned, but also special context-dependent access rights can be created. These can be adapted directly to a particular situation or an event that occurs. Of course, this not only expands the possibilities of the system, but also increases the complexity for the users. The extent to which the added value outweighs this increase in complexity is to be found out in a final study.

Parts of this chapter were published in the peer-reviewed papers "Architektur zum Schutz der Privatsphäre in AAL-Systemen" (translated: Architecture for the protection of privacy in AAL systems) (Reich et al., 2017) and "Privacy enhancing data access control for ambient assisted living" (Kuijs et al., 2019).

Chapter 10

Evaluation of Context-Aware Access Control

The access control system that enables users to define what data can be accessed by what other user or service has been developed. These access rules can be defined during installation and changed to the user's liking during runtime. Special about this access control mechanism is the fact, that it can be adapted to the actual context (time, location, situation, etc.) of a user (see chapter 9). The basis of the evaluation of the experience with access rules is a user questionnaire (user survey). In this survey, participants of all ages were asked if access-rules, allowing to specify data access in detail, and rules that are explicitly in place for emergencies, represent an added value to the overall system.

10.1 Design Principles of the Survey

Due to the relative complexity of the issue of access rights for outsiders, the first idea for the evaluation was a series of expert interviews. In numerous discussions with experts in the field at Furtwangen University, contact was made with various facilities for older people. Unfortunately, due to the onset of the pandemic and the additional need for protection of older people, as well as care facilities, it was no longer possible to include them in the survey. Expert interviews with professional

staff were also not possible at times due to the rules in force in Germany.

Therefore, the evaluation was changed to an interactive experiment followed by a questionnaire and evaluation was generally opened to other groups of people without a specific AAL background. The survey could be carried out online by using SoSciSurvey (SoSci Survey GmbH, 2022), a survey platform that adheres to the strict requirements of German data privacy laws, is mainly used for scientific surveys, and can be programmed and extended by standardized APIs.

10.2 Structure of the Survey

The survey is divided into an experiment with a) subsequent check of understanding of the presented solution, b) a review of the underlying hypotheses, c) assessment of the PbD principles and d) demographic questions.

10.2.1 Hypotheses

The hypotheses are based on the assumption that people are more willing to share personal information with other people in dangerous situations. This use case was chosen because it represents a very comprehensible context change in relation to AAL and users can easily empathise with it. Similar hypotheses were made in relation to the protection of privacy in the study by Wilkowska et al. (2022).

The following three hypotheses of this Thesis are to be tested in this study:

1. **In emergencies, people are more willing to share personal information with third parties.**
   The option to make context-dependent changes to the access rules for stored data is viewed positively by users.

2. **The possibility to create different access rights for emergencies is an added value within the AAL platform.**
   In deviation from normal operation, special rules for accessing data can be

defined for special situations. This functionality represents added value, especially for emergencies.

3. **The detailed control of access rights based on the collected data of a service increases the perceived effort.**
   Although the additional functionality is considered an advantage, the increased effort is an additional barrier to easy access to the system.

10.2.2 Introducing the Access-Control Concepts to the Participants

The first part is a scenario-based experiment presenting the management solution for access control in the SpeciAAL platform. The participant is given a fictitious but realistic scenario to carry out the survey.

The survey participants are introduced to third parties that he can provide access to collected data of a heart-rate monitor and a drug dispenser in an according user-interface. As introduced in section 2.4, the third parties are oriented towards the groups of stakeholders for ambient assisted living. The two devices represent different classes of AAL systems: Sensing and reasoning systems in the case of the medication dispenser, respectively sensing and interaction systems in the case of the heart rate monitor (see section 2.2).

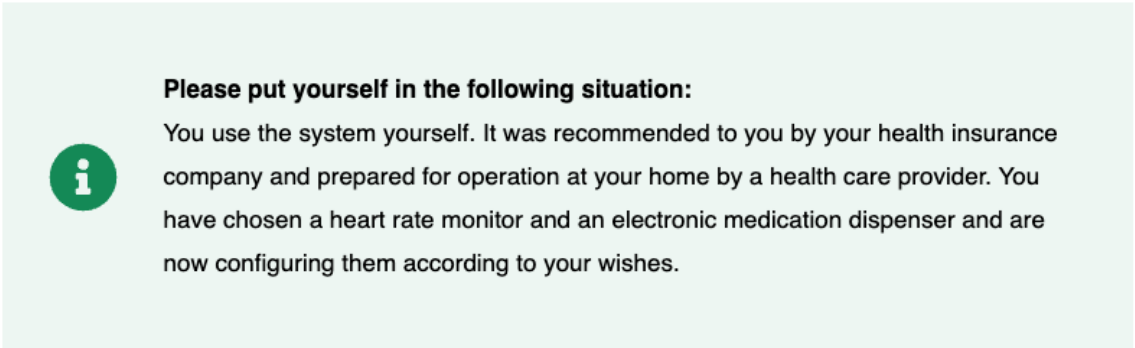

Figure 10.1: Questionnaire: Introducing the Scenario

The participant is introduced to three possible levels of granting access to private data via the system: 1. For a whole device (basic access), 2. for specific data

that is collected by the device (detailed access), or 3. for specific data during a state of emergency (situation-based access). The different modes are presented by describing changes in the scenario and giving the participant updated input possibilities to make their decisions (see Fig. 10.2).

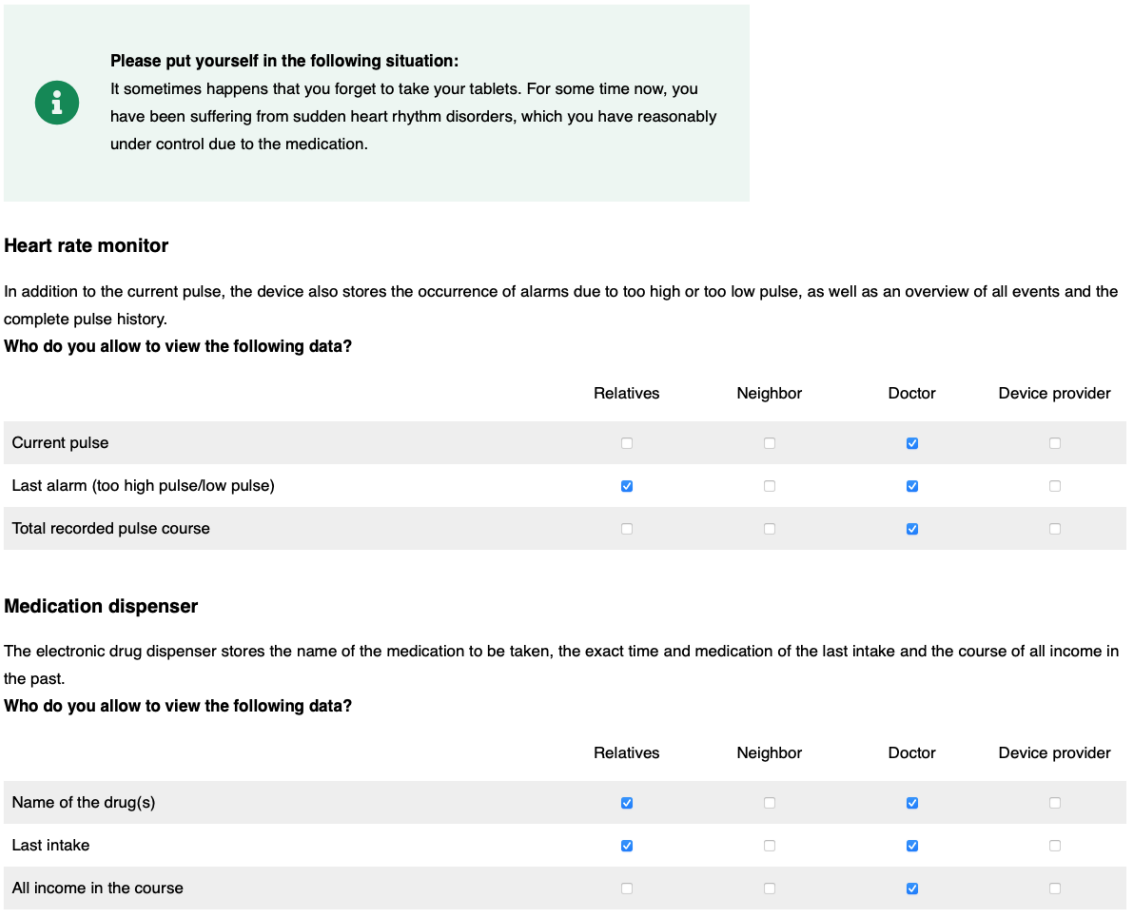

Figure 10.2: Questionnaire: Detailed access control for types of data

The lead questions for the three parts are:

1. **Basic:** *Who do you allow viewing this data?* The participant can then tick *Relative*, *Neighbour*, *Doctor*, *Device Provider* to allow them to access data of his heart-rate monitor and his drug dispenser (two independent questions).

2. **Detailed:** *Who do you allow viewing the following data?* The description of collected data by the two devises is specified in more detail. There is one item with information about the latest interaction, one item with information about alarms, and one general item with all data collected (that resembles complete device access in the basic scenario). The access for this data can be

again granted to the aforementioned third parties by ticking the boxes.

3. **Situation-based:** *Who do you allow in case of emergency to see the following data?* In this third block of the experiment, the UI stays the same, but the scenario is switched to an emergency. This situation implicitly enables an override for the previously set access rights (see Fig. 10.3).

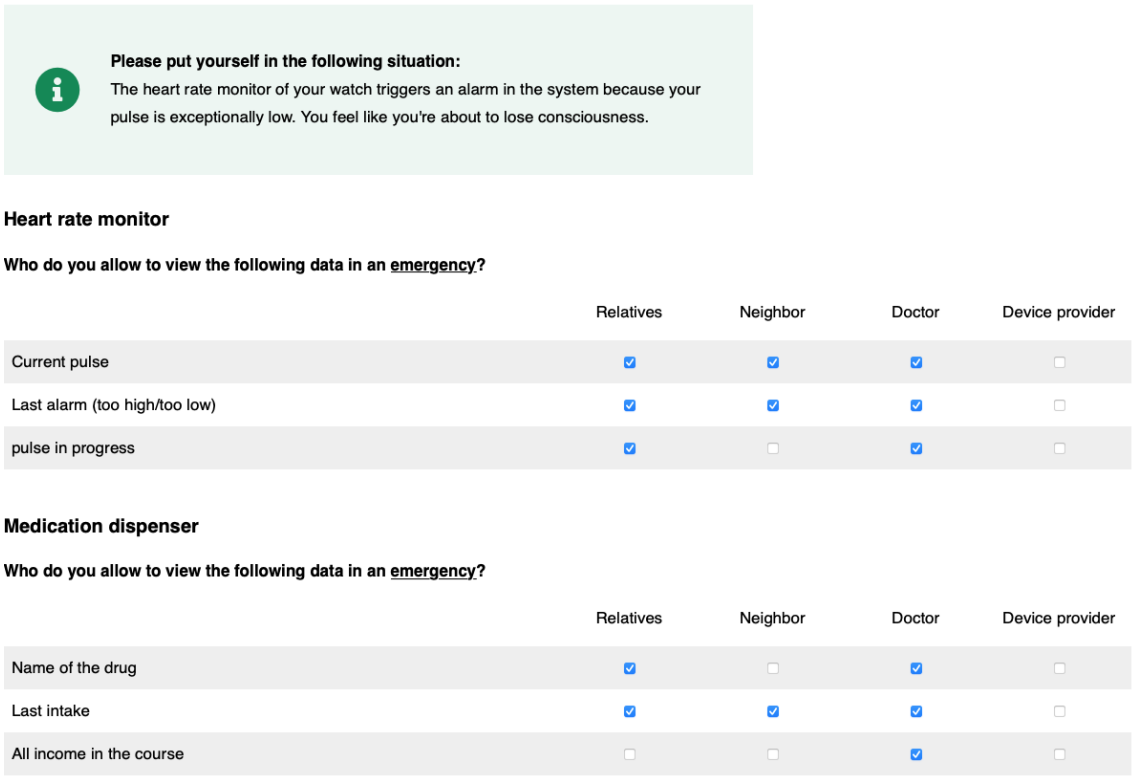

Figure 10.3: Questionnaire: Detailed access control in an emergency situation

10.2.3 Conformity with Expectations

In the previous part of the questionnaire, the participants are asked to decide what third party can access their data in the presented scenarios. To additionally check whether the desired effect corresponds to the selected options and at the same time to test whether the concept of situation-based release of user data was generally understood by the participants, a system feedback is used in this part. The selected options of the experiment are translated into natural language sentences and presented to the participant (see Fig. 10.4 - The sentences are according to the ticked boxes in the two previous figures).

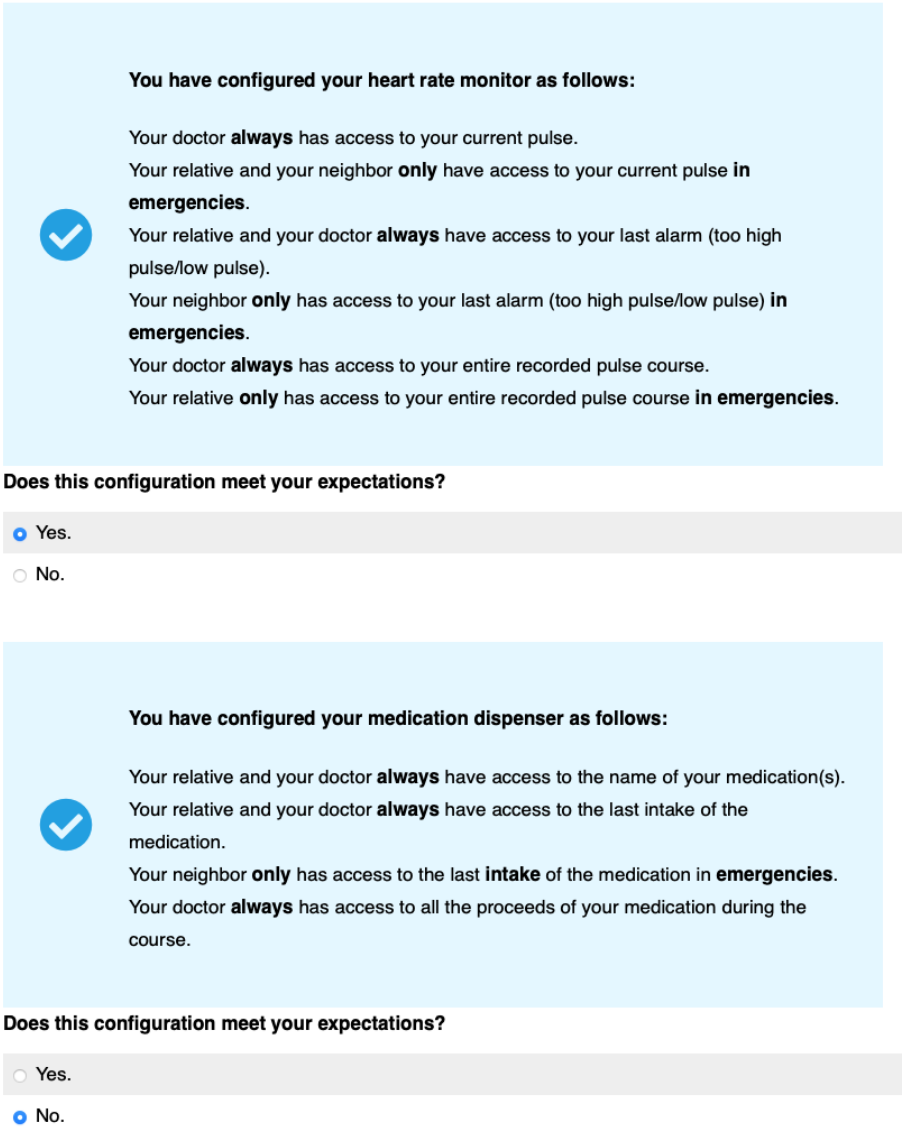

Figure 10.4: Questionnaire: Conformity of expectations

A ticked box in the first scenario (no emergency) corresponds to "[third party] always has access to [type of data]". A ticked box in just the second scenario (emergency) is interpreted as "[third party] only has access to [type of data] in emergencies". In this case, "always" overwrites "only in emergencies", thus avoiding duplications. In addition, the same rules for a data type for different third parties are combined into one sentence. An inline PHP: Hypertext Preprocessor (PHP) script was used for the programming. Access to the required variables from the questionnaire was provided directly via the survey platform.

If the result does not correspond to the expected settings for the release of private data to third parties, the participant is asked to explain in writing why it does not

apply (see Fig. 10.5).

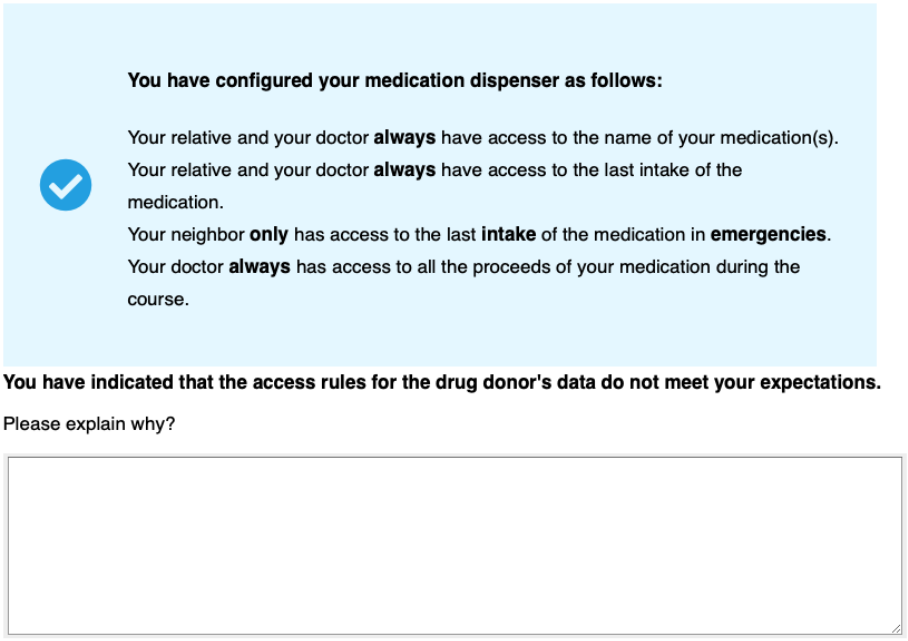

Figure 10.5: Question about the selected options during the scenarios: Why do the access rules not match your expectation?

This part is provided to give a direct feedback from the experiment to the participant, as well as a possibility for him to correct unexpected behaviour of the system and to understand what the expectation has been in the first place.

10.2.4 Verification of the Hypotheses

For the third part of the questionnaire, a five point Likert scale (*I fully agree - I disagree*) is used. The respondents have to give a self-assessment based on two times six statements. The first six statements refer to the experiment, and relate to one of the three PbD strategies (see section 4.6). For each design strategy, there are two statements following the lead question "Which statement applies to your data in the cases described?":

- **Inform:**
  - "I now know who can see my data in everyday life and in emergencies."
  - "I have to make these decisions because otherwise I don't know what happens to my data."

- **Control:**
  - "I can control the protection of my data with my decisions."
  - "I am aware that the system can be used by me even without these decisions."
- **Enforce:**
  - "If I don't decide, other people can see my data."
  - "My data is protected in the system from unwanted access."

In the second part of the statements, the participant is asked to give an assessment of the system as a whole. The overarching question for this part is: "How do you evaluate the presented setting of access rights?":

- **Questions asking about the ease of use:**
  - "I would have someone help me with the configuration."
  - "The setting of access rights is complicated."
- **Questions asking about the personal relation to the system:**
  - "I would use the system myself."
  - "I would recommend the system to other people in my environment."
- **Questions asking about the hypotheses of the survey:**
  - "The distinction between everyday life and emergency is an added value."
  - "The possibility to share only certain data of a device with others is helpful."

10.2.5 Demography and Self-Assessment

Finally, the participant is asked for information about himself, his immediate environment, and his affinity for technology. In the final questions, they are asked

whether they see themselves as technically gifted and as a help to others, or as needing help themselves.

10.3 Discussion of Survey Results

The survey was held out in autumn of 2021. Of the 82 participants, 29 were female and 53 male. The age distribution (see Fig. 10.6) ranged from younger than 20 years old (1 participant), over 20-39 years old (40 participants) and 40-59 years old (36 participants) to 60-79 years old (5 participants).

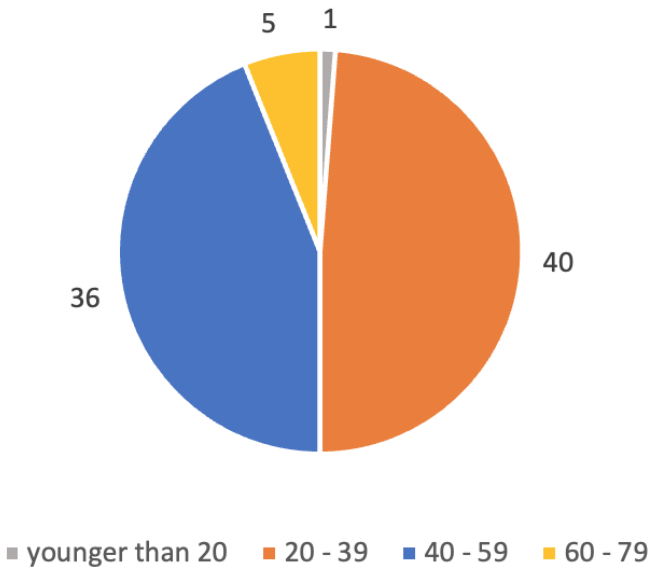

Figure 10.6: Age distribution among participants

When asked about other persons living in the participants' household, 13 participants state that they are living alone, the main part of the participants (63) live together with one to three people, only six participants live together with four or five people in the same household.

The majority of participants (66) are stating that they have 6 or more different ICT-devices at home. When the participants are asked about their personal assessment of their understanding of technology, the majority of them are more likely to help others to set up equipment than to be helped by others (see Fig. 10.7).

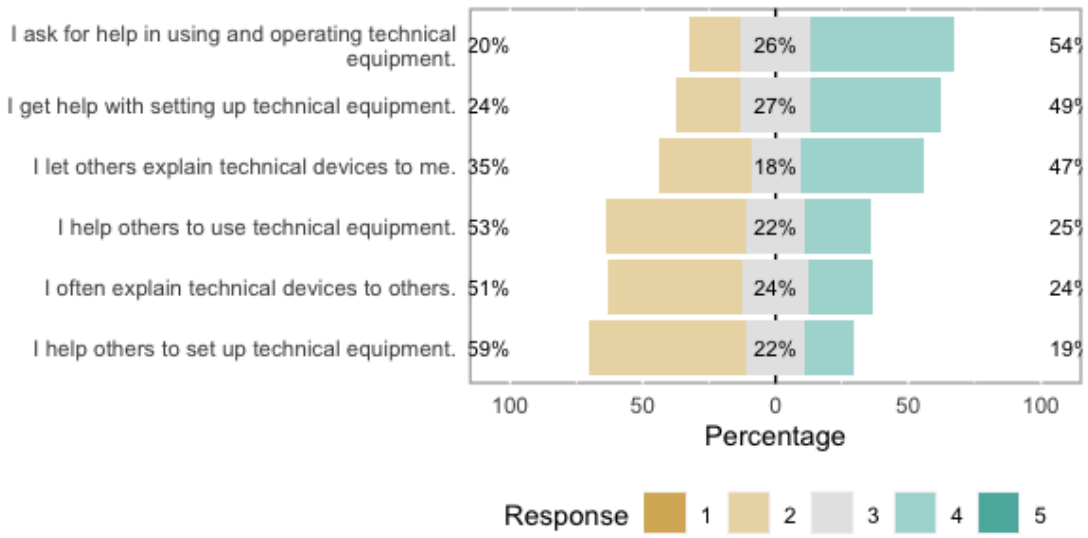

Figure 10.7: Personal assessment of understanding of technology (1 = I fully agree / 5 = I disagree)

10.3.1 Scenario Part of the Survey

In the scenario part of the survey, the participants assigned access rights in three gradations. To better illustrate the differences in the individual scenarios, the change per application item (drug dispenser and heart rate monitor) is shown below.

Scenario: Heart Rate Monitor

When asked about access to all data collected by the device, participants indicated that they would share the data with the responsible doctor (76.8%) and relatives (70.7%) in the majority, but with neighbours (7.3%) and the device provider (7.3%) only to a small percentage (see Fig. 10.8).

When given the possibility of granting access in more detail due to a finer granularity in access-rights (current pulse, last alarm, all pulse data), the participants showed a similar behaviour over all three data categories. It is noticeable that, in relation to the doctor, the acceptance of the release of the complete data set is still increasing (79.3%), while to the relatives, there is only an increase (64.4%) for the alarm (and thus a potential emergency - even if it may have happened a while

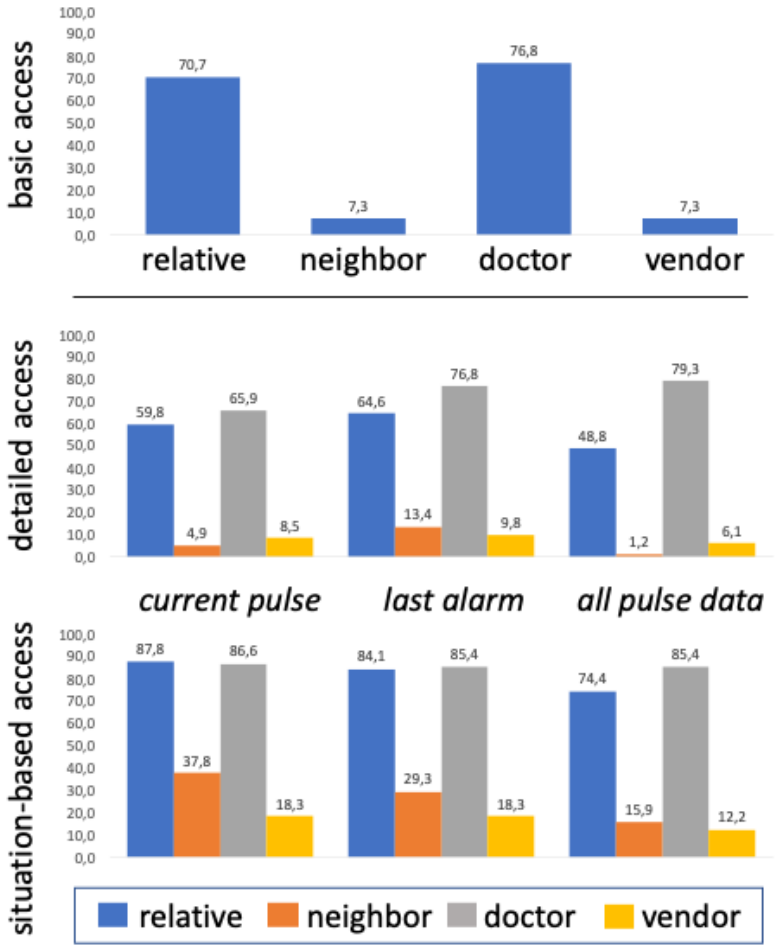

Figure 10.8: Granted access rights related to the heart rate monitor (Percentage)

ago) and full access is less accepted (48.8%). The other two user groups remain in the single-digit percentage range, even though the last alarm experiences an increase to 13.4% for access by neighbours.

All values increase significantly for the third scenario and the occurrence of an emergency, with an acceptance of around 80% for data release to relatives and professional help personnel and also an increase for release to neighbours. Even the release to the system providers experiences an increase, and this without any apparent reason how the latter could intervene helpfully in an emergency.

To calculate statistical significance, a McNemar's χ^2 test (McNemar, 1947) is used with a significance level of 5% and a critical value of $\chi^2_{1;0.95} = 3.84$. Since the values are greater than the critical value with two exceptions (cf. Table 10.1), the null hypothesis is invalidated. This means for the given case and the present

χ^2	**relative**	**neighbour**	**doctor**	**vendor**
current pulse	21.043	23.310	15.059	4.900
last alarm	14.062	6.857	4.000	4.000
all pulse data	17.391	8.643	3.200	2.286

Table 10.1: χ^2 of McNemar's Test for change between detailed and situation-based access control settings for heart rate monitor. (Null-hypothesis falsified with $\chi^2 > 3.84$)

experiment that there is a significant change for the granting of access rights. The two aforementioned exceptions represent the marginal increase for data release of all pulse data for doctors, that has been high for detailed access rights and stays on a high level for emergency access rights (which leads to a ceiling-effect for McNemar's χ^2 test), and a light increase for data access through the device vendor in a case of emergency.

Scenario: Drug Dispenser

A similar pattern is observed in the context of the drug dispenser, wherein once again, it is apparent that general access is more likely to be permitted for relatives (64.6%) and professional carers (62.2%) than for the group of neighbours (secondary carers - 2.4%) and equipment providers (3.7% - see Fig. 10.9). In the detailed access scenario, the values remain very similar on average. Only access for the Doctor is allowed significantly more often for all three data groups. In comparison, the willingness of all third parties to access data increases significantly for the emergency situation.

χ^2	**relative**	**neighbour**	**doctor**	**vendor**
medicine name	14.450	19.048	5.143	2.500
last intake	13.474	18.050	9.091	0.571
all intake	20.045	11.077	7.111	2.286

Table 10.2: χ^2 of McNemar's Test for change between detailed and situation-based access control settings for drug dispenser. (Null-hypothesis falsified with $\chi^2 > 3.84$)

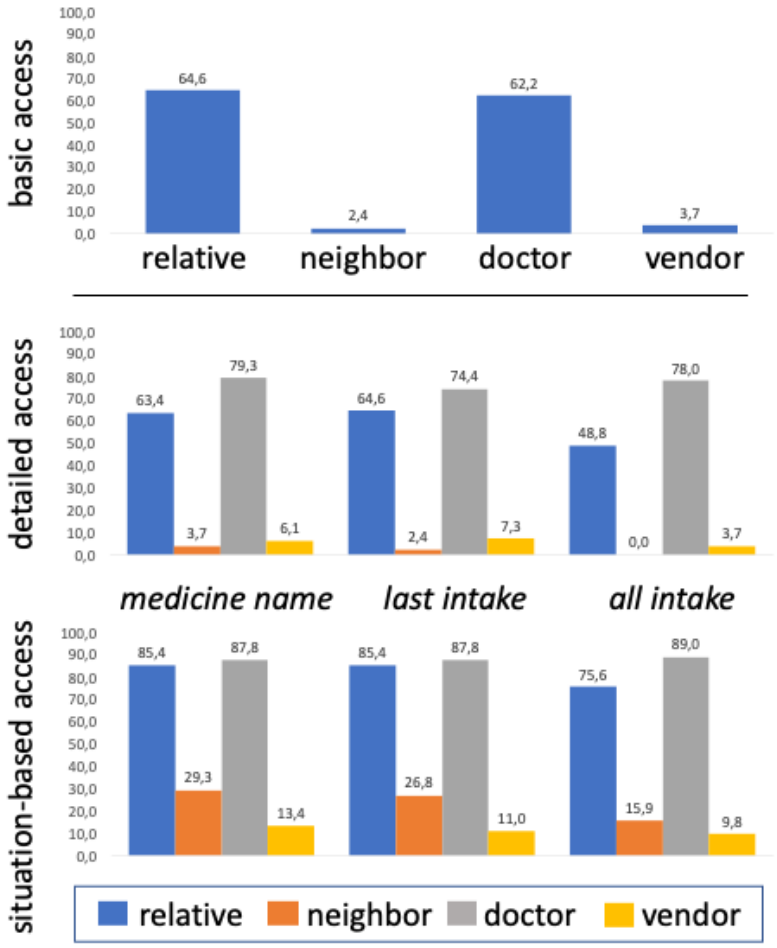

Figure 10.9: Granted access rights related to the drug dispenser (Percentage)

This effect is again evident in McNemar's test, which attests to significant changes in acceptance for all given access-rights between detailed access and the emergency (see Table 10.2).

10.3.2 Conformity with Expectations

In the direct comparison with the third-party access options clicked on in the scenarios in natural language, 96.3% said they agreed with the statements for the heart rate monitor and drug dispenser. For the 3.7% who did not agree with the statement sentences, the reasons were also asked: With one exception, where additional data was to be released for the relative, the users who did not find themselves in the statement sentences indicated that too much data would be passed on to third parties with the settings previously made. One respondent

stated that he only wanted third parties to have access to the data if he explicitly allowed it in the actual situation.

10.3.3 PbD Principles

The statement related to the PbD principles was answered by the test persons as follows After the presentation of the system and the information in the questionnaire, the majority of the test persons feel *informed* about the access rights they have set in the system (see Fig. 10.10, row three). Nevertheless, they think

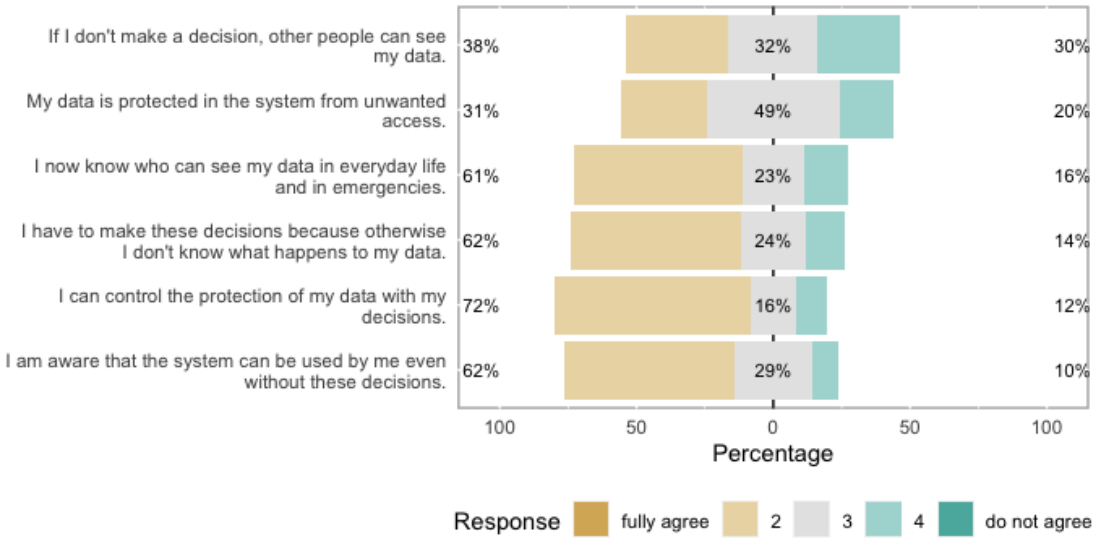

Figure 10.10: Likert Scale: Statements referring to Privacy by Default Principles

that they have to actively set the access rights to know about the current status of data access by third parties (62%, row four). The user are well aware that they can *control* the system with their decisions (72% agreement) and understand in the vast majority (62% agreement) that they do not need to perform this control to use the system (row five and six). The *enforce* strategy (basic data protection setting always protects the user's data) is viewed sceptically by the test persons, as they are not sure whether their data in the system is generally protected against unwanted access (31% approval and 49% undecided, see row two) and at the same time they have the feeling that they have to set access rights to protect their data. This is, although they were informed during the experiment that only they have access to their data if they do not decide (38% approval, see row one).

10.3.4 Feedback to the System

In terms of the ease of use of the system presented, the picture is balanced, with no one finding the system overly complicated, but also no one who would describe it as easy to use (see the first two rows of Fig. 10.11). The majority of respondents state that setting up special access rights for emergencies adds value to the system, and that a fine-grained release of access rights is an advantage (row four and six). Again, there is no extreme agreement or disagreement with the statements presented. Regarding the use by the test persons themselves or the recommendation to persons in their circle of acquaintances, the picture is also positive for the solution presented: the majority state that they can definitely imagine using the system themselves and recommending it to others (row three and five).

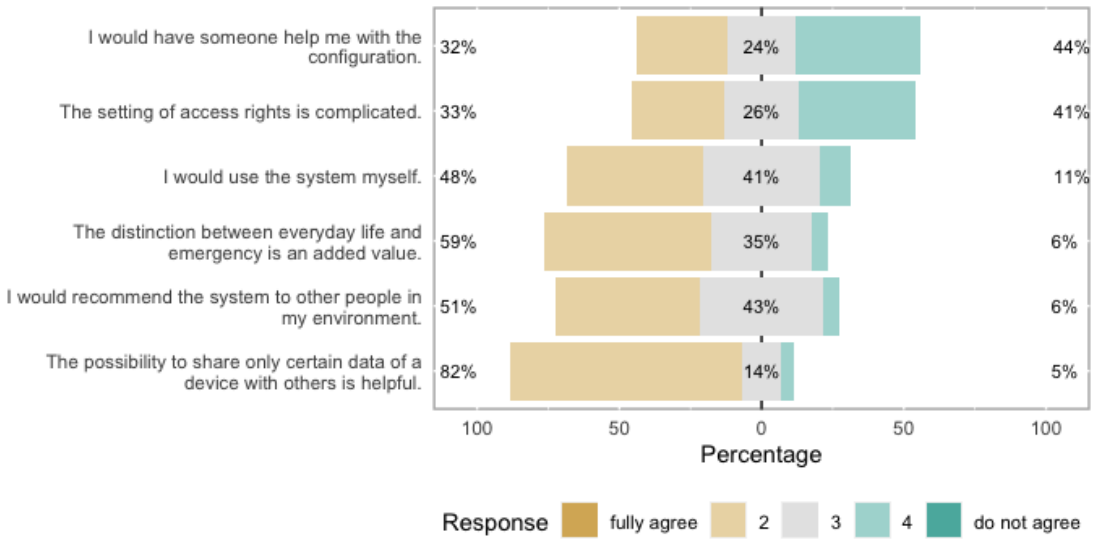

Figure 10.11: Likert Scale: Statements about the presented access-control system

10.4 Crowd-Sourcing for Recommended Settings

Another aspect of collected data is that over time the aforementioned complexity to initially set access rules can be supported with collected data per service. In our experiment, for example, the frequencies of access rights granted can be directly transferred into recommendations for new users. To comply with the requirements

of the EU GDPR and the PbD, these settings must not be set from the outset, but are, for example, colour-coded in a prototypical implementation. This can reduce the complexity of the system and further increase the benefit and use of the system.

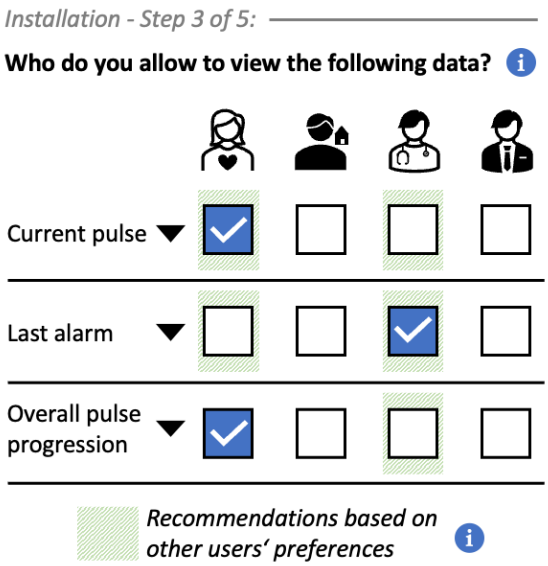

Figure 10.12: UI Prototype of Crowd-Sourced User Recommendations

This approach is graphically illustrated in the UI prototype shown in figure 10.12. In this example, recommendations were made based on simple majorities of over 50% using the data previously outlined. The verification of this hypothesis, however, is not part of the presented study among the test persons.

10.5 Conclusion

With the presented survey, it could be shown that people are more willing to share personal information about themselves with third parties in a case of an emergency. This was not only the result of the direct questioning, but also emerged from the collected data of the empirical study as a statistically significant increase in permission to access data for other key actors in AAL systems during an emergency. This is also underpinned by the fact that the majority of respondents said that the possibility of creating different access rights for normal operation and emergencies was an added value.

Due to the increased perceived effort of the creation of access rights, optimization

regarding the user interface will be the next step for improvement. Considering that emergencies are only a very illustrative example of user context, many more context-based access right scenarios (possibly depending on location or time) can be developed based on the presented system.

Parts of this chapter were published in the peer-reviewed papers "The Need for Emergency-Based Access Control in AAL Systems" (Kuijs et al., 2022).

Chapter 11

Conclusion

This thesis has examined the question whether it is possible to provide an AAL platform with existing technical requirements in the cloud. It was found that the central personal information that enables the current context to be determined, which is in turn used to tailor services to a user, is a valuable asset that must be protected. As a result of the research, the following items have been of focus:

- The adaptability of services based on user context and personalization based on user preferences in a cloud-based AAL platform,
- the development of a privacy module, together with a necessary privacy policy language, and
- the extension to include context specifically, but not exclusively, designed for AAL applications

were the focus of this work.

11.1 Achievements of the Research

In this thesis, a PaaS approach for a platform for AAL was developed. The PaaS supports all common concepts of already existing platforms, is based on OSGi as universal middleware technology and was extended by the ability of scalability.

This means that individual services of an existing platform as well as the platform itself can run in a cloud infrastructure.

Even though this thesis did not finally address the possible cost savings of a cloud platform compared to a locally installed AAL system, it can be deduced from the presented cloud basics that this is already one of the biggest motivations for existing cloud solutions. Technically, however, it does offer the possibility of subsequently increasing, reducing and shifting resources, thus allowing flexible adaptation to the respective usage scenario: the platform is able to respond to the user's specific requirements.

In the second part of the thesis, special attention was paid to the adaptability of the system. It was argued that optimal support depends on the response to the user's context. By using an ontology-based database, collected data and additional contextual information can be evaluated and system responses can be precisely adapted as a result. This was also the result of the user survey taken halfway through work on the thesis. On the other hand, however, users surveyed also expressed concerns about data security in a cloud computing environment. The question was how to ensure that only authorized individuals can access personal information.

When implementing the subsequently developed privacy policy, the context, which is important for the AAL area, was also introduced as an additional element in order to define conditions for an access right. It has been shown that extension through context offers new opportunities for creating access rights.

To prove this on the one hand and to check whether the users understand the concept on the other, a final user test was carried out. An emergency scenario was used to test whether users would grant different permissions in an emergency than in normal operation of the platform. It was shown that the willingness to disclose private information increases significantly in emergency situations and that the policy itself, with context as an input variable, offers added value.

11.2 Limitations of the Research

Within the current landscape of research and development, PaaS designed for AAL has not achieved significant traction or widespread adoption. Despite the potential benefits and opportunities it could offer, the uptake and active development of such platforms within the research and development sphere remain limited or relatively subdued.

Adjacent topics that arise directly from the new possibilities presented, but unfortunately could not be conclusively clarified, revolve around the implications of the newly gained results for users: Usability and user experience are questions that still need to be clarified and also still have implications for the overall system.

Although monitoring as a central element was theoretically classified and technically solved as a basis for the PbD strategy "Inform", the accumulating information for the user in this area is simply overwhelming and very difficult to assess. Figure 11.1 shows some mock-ups that were created during the research, but they only represent initial approaches. Therefore, this thesis does not include a graphical evaluation and focuses on the creation of rules.

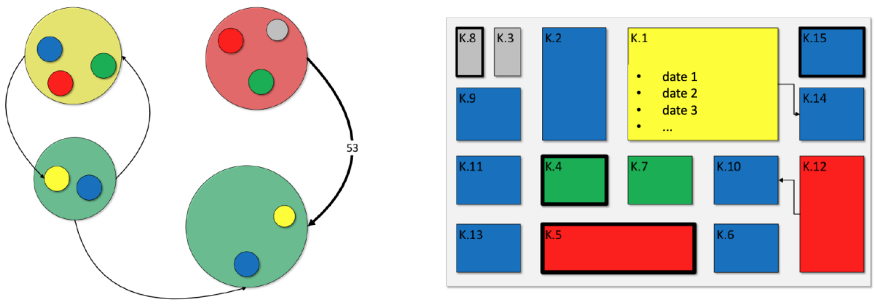

Figure 11.1: Prototypes for visualizing monitored data: Features like colour, line thickness, and item size represent data types, frequency of access or the number of data

But here, too, a self-explanatory user interface is the key to success (as discussed in chapter 9.7). In the end, the motivation of the user also determines the success of the overall system and its possibilities. Related to transparency, for example, the question arises, what could be the way in which the information is displayed

to the user and the motivation for a user to allow the transfer of data to a third party: If information is too detailed for the user (especially in the field of AAL) the user gets unsettled, confused or annoyed. Especially when a service is expected to be adapted continuously, the user is required to examine each changes or tick the infamous 'Always' box, that is also often used in personal firewall installations when a service changes its connections. The second question that comes to mind is: Why would a user do it in the first place? What is the benefit for the user of having the information shared with third parties, or for our cloud-bursting scenario, of having the service running in the Public Cloud (or by lack of concept 'somewhere else')? The considerations of the service provider (reduced costs or extending resources) can't be transferred to the user.

11.3 Future Challenges for Platforms for AAL

As shown in chapter 2 the market for systems in the field of AAL changed during the research. The market in general for smart homes has grown significantly, and AAL systems are part of the "Security" branch of that market.

UniversAAL, the biggest EU FP7 consortium of 2016, regrouped and is now focusing on the IoT (The universAAL IoT Coalition, 2022). They missed their goal of building a common ground for system vendors in the field of AAL. At the same time, smart-home ecosystems powered by big tech companies like Apple or Amazon gained tractions and are now often seen as the basis for healthcare-systems, e.g. Alarms for low glucose-readings (Dexcom Inc., 2022) or emergency calls upon fall-recognition through Apple services (Apple Inc., 2022).

On the other hand, the mainstream adoption of smart home technology is also a development that counters one of today's main problems of supporting older people through technology: The scepticism of using new systems in the home. Today, it is often only a small step from a smart speaker that plays the radio and tells the weather to much more sophisticated support for older people using additional sensors and services.

The direction of development within the AAL industry and the potential emergence of a fourth generation of smart home technologies propelled by advancements in artificial intelligence, exemplified by OpenAI, wearables, and smart home voice assistant systems like Amazon Alexa or Google Assistant, are yet to unfold and determine the future trajectory of AAL systems. A promising step in this direction is the agreement of a large consortium of platform operators, consumer goods manufacturers, and security solution providers on a unified standard: Matter 2.0 has been announced for 2022 and the first devices are available (matter-smarthome, 2022).

AAL systems can greatly benefit from AI technologies. Machine learning models can be used to analyse vast amounts of data collected from AAL environments. This enables the creation of personalized assistance for individuals based on their specific needs, routines, and preferences. AI tools can continuously monitor various parameters in AAL environments, such as movement patterns, vital signs, and activity levels. This allows for early detection of abnormalities or changes in behaviour, enabling proactive interventions or alerts to caregivers or medical professionals. As they process more data and interactions, they can improve their recommendations and responses, becoming more effective in assisting users within AAL settings.

But there are several risks and challenges associated with their integration:

- **Privacy Concerns:** A major risk involves the collection and utilization of personal data within AAL systems. Third-party Machine Learning tools might need access to sensitive information to function effectively, raising concerns about data security and the potential for misuse or unauthorized access.
- **Reliability and Accuracy:** There's a risk of errors or inaccuracies in the predictions or recommendations made by these systems, which could lead to incorrect actions being taken in AAL environments, impacting user safety.
- **Ethical Challenges:** AAL systems may make decisions affecting individuals'

lives, raising ethical questions about the criteria used in decision-making processes.

- **Dependency on Technology:** Over-reliance on AI-driven AAL systems might lead to a loss of human touch or the ability to function without technology. This dependency could have adverse effects if the systems fail or encounter technical difficulties.

- **Lack of User Understanding**: Users might not fully understand how the AI within AAL systems works, leading to distrust or misunderstanding. This could result in resistance to adopting these technologies, even if they could greatly benefit users.

To mitigate these risks, it's crucial to implement robust security measures, prioritize data privacy, ensure transparency in AI decision-making, conduct regular system checks for accuracy and reliability, and involve users in the design and testing phases to enhance understanding and trust. Additionally, continuously updating and improving AI models can help address some of these risks over time.

Regardless of the development of the platform, the need for detailed control of data access, specifically to personal data, which this work deals with, is essential and unavoidable to meet the requirements of the EU GDPR: The control of their data should always remain with the user.

References

104th Congress. Health Insurance Portability and Accountability Act of 1996 | ASPE, 1996. URL https://aspe.hhs.gov/reports/health-insurance-portability-accountability-act-1996.

a4cloud. A4Cloud - The Cloud Accountability Project, 2016. URL http://www.cloudaccountability.eu/.

AAL Association. AAL Home 2020 - AAL Programme, 2023. URL https://www.aal-europe.eu/.

E. Aarts and R. Wichert. Ambient intelligence. In H.-J. Bullinger, editor, *Technology Guide: Principles - Applications - Trends*, pages 244–249. Springer Berlin Heidelberg, Berlin, Heidelberg, 2009. ISBN 9783540885450. doi: 10.1007/978-3-540-88546-7{_}47. URL http://dx.doi.org/10.1007/978-3-540-88546-7_47.

Y. Al-Issa, M. A. Ottom, and A. Tamrawi. eHealth Cloud Security Challenges: A Survey. *Journal of Healthcare Engineering*, 2019, 2019. ISSN 20402309. doi: 10.1155/2019/7516035. URL /pmc/articles/PMC6745146//pmc/articles/PMC6745146/?report=abstracthttps://www.ncbi.nlm.nih.gov/pmc/articles/PMC6745146/.

M. R. Alam, M. B. I. Reaz, and M. A. M. Ali. A review of smart homes - Past, present, and future. *IEEE Transactions on Systems, Man and Cybernetics Part C: Applications and Reviews*, 42(6):1190–1203, 2012. ISSN 10946977. doi: 10.1109/TSMCC.2012.2189204.

M. Almalki, M. H. Alsulami, A. A. Alshdadi, S. N. Almuayqil, M. S. Alsaqer, A. S. Atkins, and M. A. Choukou. Delivering Digital Healthcare for Elderly: A Holistic Framework for the Adoption of Ambient Assisted Living. *International Journal of Environmental Research and Public Health 2022, Vol. 19, Page 16760*, 19 (24):16760, 12 2022. ISSN 1660-4601. doi: 10.3390/IJERPH192416760. URL https://www.mdpi.com/1660-4601/19/24/16760/htmhttps://www.mdpi.com/1660-4601/19/24/16760.

Amazon Web Services. AWS Command Line Tools, 2022. URL https://aws.amazon.com/cli/.

E. A. Ambugo, S. R. De Bruin, L. Masana, J. MacInnes, N. C. Mateu, T. P. Hagen, and B. Arrue. A Cross-European Study of Informal Carers' Needs in the Context of Caring for Older People, and their Experiences with Professionals Working in Integrated Care Settings. *International Journal of Integrated Care*, 21(3):2, 7 2021. ISSN 1568-4156. doi: 10.5334/ijic.5547.

Apache Software Foundation. Apache Stratos - Open Enterprise PaaS. http://stratos.apache.org/, 2015a.

Apache Software Foundation. ZooKeeper: Because Coordinating Distributed Systems is a Zoo, 2015b. URL https://zookeeper.apache.org/doc/r3.5.1-alpha/.

Apache Software Foundation. Apache CXF – Distributed OSGi, 2015c. URL https://cxf.apache.org/distributed-osgi.html.

Apache Software Foundation. jclouds - The Java Multi-Cloud Toolkit, 2015d. URL https://jclouds.apache.org/.

Apache Software Foundation. Apache CXF - DOSGi Single Bundle Distribution, 2016a. URL https://mvnrepository.com/artifact/org.apache.cxf.dosgi/cxf-dosgi-ri-singlebundle-distribution.

Apache Software Foundation. Apache CXF - DOSGi Discovery Demo Page, 2016b. URL http://cxf.apache.org/dosgi-discovery-demo-page.html.

Apache Software Foundation. Apache Felix, 2016c. URL http://felix.apache.org/.

Apache Software Foundation. Apache JMeter, 2016d. URL http://jmeter.apache.org/.

Apple Inc. Exposure Notification Overview, 2020. URL https://developer.apple.com/exposure-notification/.

Apple Inc. Use fall detection with Apple Watch – Apple Support (UK), 2022. URL https://support.apple.com/en-gb/HT208944.

Arcserve Inc. 7 Most Infamous Cloud Security Breaches, 2022. URL https://www.arcserve.com/blog/7-most-infamous-cloud-security-breaches.

Article 29 Data Protection Working Party. Opinion 4/2007 on the concept of personal data. *Wp*, 0(Lx):136, 2007. URL http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf.

M. Assad, D. J. Carmichael, J. Kay, and B. Kummerfeld. PersonisAD: Distributed, Active, Scrutable Model Framework for Context-Aware Services. *Pervasive Computing*, 4480:55–72, 2007. ISSN 0302-9743. doi: 10.1007/978-3-540-72037-9{_}4. URL http://dx.doi.org/10.1007/978-3-540-72037-9_4https://link.springer.com/chapter/10.1007/978-3-540-72037-9_4.

D. Balfanz, M. Klein, A. Schmidt, and M. Santi. Participatory development of a middleware for AAL solutions : requirements and approach – the case of SOPRANO. *GMS Medizinische Informatik, Biometrie und Epidemiologie*, 4(3):1–11, 2008. ISSN 1860-9171.

M. Becker, A. Malkis, and L. Bussard. S4P: A generic language for specifying privacy preferences and policies. *Microsoft Research*, pages 0–35, 2010. URL https://wwwbroy.in.tum.de/~malkis/BeckerMalkisBussard-S4P-AGenericLanguageForSpecifyingPrivacyPreferencesAndPolicies.pdf.

E. Bekiaris and S. Bonfiglio. The OASIS Concept. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 5614 LNCS(PART 1):202–209, 2009. ISSN 03029743. doi: 10.1007/978-3-642-02707-9{_}22. URL https://link.springer.com/chapter/10.1007/978-3-642-02707-9_22.

M. Berger, F. Fuchs, and M. Pirker. Ambient Intelligence - From Personal Assistance to Intelligent Megacities. In J. C. Augusto and D. G. Shapiro, editors, *Advances in Ambient Intelligence*, volume 164 of *Frontiers in Artificial Intelligence and Applications*, pages 21–35. IOS Press, 2007. URL http://www.booksonline.iospress.nl/Content/View.aspx?piid=7295.

S. Blackman, C. Matlo, C. Bobrovitskiy, A. Waldoch, M. L. Fang, P. Jackson, A. Mihailidis, L. Nygård, A. Astell, and A. Sixsmith. Ambient Assisted Living Technologies for Aging Well: A Scoping Review. *Journal of Intelligent Systems*, 25(1):55–69, 1 2016. ISSN 03341860. doi: 10.1515/jisys-2014-0136. URL http://www.degruyter.com/view/j/jisys.2016.25.issue-1/jisys-2014-0136/jisys-2014-0136.xml.

J. Borking and C. Raab. Laws, PETs and Other Technologies for Privacy Protection. *Journal of Information Law & Technology*, 1(February):1–14, 2001. URL http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2001_1/borking/.

J. A. Botia, A. Villa, and J. Palma. Ambient Assisted Living system for in-home monitoring of healthy independent elders. *Expert Systems with Applications*, 39 (9):8136–8148, 2012. ISSN 09574174. doi: https://doi.org/10.1016/j.eswa.2012.01.153.

A. Braun, F. Kirchbuchner, and R. Wichert. Ambient Assisted Living. In *eHealth in Deutschland*, pages 203–222. Springer Berlin Heidelberg, Berlin, Heidelberg, 2016. doi: 10.1007/978-3-662-49504-9{_}10. URL http://link.springer.com/10.1007/978-3-662-49504-9_10.

BREATHE Project Consortium. D5.3 - White paper on aal systems and associated privacy issues. Technical Report January, BREATHE Project Consortium, 2015. URL http://www.breathe-project.eu/gallery/16/D5_3_-_Whitepaper_on_AAL_systems_and_associated_privacy_issues_v10.pdf.

G. v. d. Broek, F. Cavallo, L. Odetti, and C. Wehrmann. AALIANCE Ambient Assisted Living Roadmap. In *Ambient Intelligence and Smart Environments*, volume 6, page 110, 2010. ISBN 9781607504986.

J.-M. C. Brook, V. Chin, H. Foskett, A. Getzin, V. Hargrave, S. Levy, A. McCormick, S. Pieraldi, M. Roza, M. Ryan, A. Schindel, and S. Shamban. Top Threats to Cloud Computing - Pandemic Eleven. Technical report, Cloud Security Alliance, 2022. URL https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-pandemic-eleven/.

H. Burns. How To Protect Your Users With The Privacy By Design Framework, 2017. URL https://www.smashingmagazine.com/2017/07/privacy-by-design-framework/.

A. Cavoukian. The 7 Foundational Principles - Implementation and Mapping of Fair Information Practices, 2010. URL https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf.

E. Celeste. Digital Sovereignty in the EU: Challenges and Future Perspectives. In F. Fabbrini, E. Celeste, and J. Quinn, editors, *Data Protection beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty*. Hart, 2021. ISBN 9781509940677. doi: http://dx.doi.org/10.5040/9781509940691.ch-013. URL https://www.oxfordreference.com/view/10.1093/acref/9780199290543.001.0001/acref-9780199290543-.

Chaos Computer Club. 10 requirements for the evaluation of "Contact Tracing" apps, 2020. URL https://www.ccc.de/en/updates/2020/contact-tracing-requirements.

Cloud Foundry. BOSH, 2023. URL https://bosh.cloudfoundry.org/docs/.

L. Cranor, B. Dobbs, S. Egelman, G. Hogben, J. Humphrey, M. Langheinrich, M. Marchiori, M. Presler-Marshall, J. Reagle, M. Schunter, D. A. Stampley, and R. Wenning. The Platform for Privacy Preferences 1.1 (P3P1.1) Specification, 2006. URL https://www.w3.org/TR/P3P11/.

G. Danezis, J. Domingo-Ferrer, M. Hansen, J.-H. Hoepman, D. Le Métayer, R. Tirtea, and S. Schiffner. Privacy and Data Protection by Design - from policy to engineering. Technical report, European Union Agency for Network and Information Security (ENISA), Heraklion, Greece, 2015. URL https://www.enisa.europa.eu/media/news-items/cloud-computing-speech.

P. Dario and F. Cavallo. AALIANCE2 Project – Deliverable 2.7. Technical report, AALIANCE2, 9 2014. URL http://www.aaliance2.eu/sites/default/files/AA2_WP2_D27_RM2_rev5.0.pdf.

M. de Mooy. Rethinking Privacy Self-Management and Data Sovereignty in the Age of Big Data. Technical report, Bertelsmann Stiftung, 2017. URL https://www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/GrauePublikationen/RethinkingPrivacy_2017_final.pdf.

B. Delacretaz. OSGI stress test utility, executes framework operations semi-randomly, 11 2012. URL https://github.com/bdelacretaz/osgi-stresser.

Department Of Economic And Social Affairs. World Social Report 2023: Leaving No One Behind In An Ageing World. Technical report, United Nations, 2023.

Dexcom Inc. How do I set up Siri on the G6 app? | Dexcom, 2022. URL https://www.dexcom.com/en-GB/faqs/how-do-i-set-siri-g6-app.

A. Dey and G. Abowd. Towards a Better Understanding of Context and Context-Awareness. In *Handheld and Ubiquitous Computing*, pages 304–307, 1999. ISBN 978-3-540-66550-2. doi: 10.1007/3-540-48157-5{_}29. URL http://dx.doi.org/10.1007/3-540-48157-5_29.

Directorate-General for Communication of the European Union. Adequacy decisions, 2021. URL https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

Docker Inc. Docker: Accelerated Container Application Development, 2023. URL https://www.docker.com/.

B. Ehringer. Kontextsensitive Systeme – Stand der Technik, 2009. URL https://docplayer.org/2916283-Kontextsensitive-systeme-stand-der-technik.html.

E. Ekonomou, L. Fan, W. Buchanan, and C. Thüemmler. An integrated cloud-based healthcare infrastructure. *Proceedings - 2011 3rd IEEE International Conference on Cloud Computing Technology and Science, CloudCom 2011*, pages 532–536, 2011. doi: 10.1109/CloudCom.2011.80.

A. El Murabet, A. Anouar, A. Touhafi, and A. Tahiri. Towards an SOA Architectural Model for AAL-Paas Design and Implimentation Challenges. *International Journal of Advanced Computer Science and Applications*, 8(7), 2017. ISSN 2158107X. doi: 10.14569/ijacsa.2017.080708.

A. El Murabet, A. Abtoy, A. Touhafi, and A. Tahiri. Ambient Assisted living system's models and architectures: A survey of the state of the art. *Journal of King Saud University - Computer and Information Sciences*, 32(1):1–10, 1 2020. ISSN 13191578. doi: 10.1016/j.jksuci.2018.04.009.

European Parliament. EU coordinated action to combat the COVID-19 pandemic and its consequences, 2020. URL https://www.europarl.europa.eu/doceo/document/TA-9-2020-0054_EN.pdf.

European Union. MEMO/07/159 - Privacy Enhancing Technologies (PETs), 2007. URL http://europa.eu/rapid/press-release_MEMO-07-159_en.htm?locale=en.

EuroPriSe GmbH. Euro PriSe - European Privacy Seal, 2017. URL https://www.european-privacy-seal.eu/EPS-en/Home.

eurostat - European Union. Population structure and ageing - Statistics Explained, 2 2023. ISSN 2443-8219. URL https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Population_structure_and_ageing.

L. Fan, W. Buchanan, C. Thüemmler, O. Lo, A. Khedim, O. Uthmani, A. Lawson, and D. Bell. DACAR platform for eHealth services cloud. In *Proceedings - 2011 IEEE 4th International Conference on Cloud Computing, CLOUD 2011*, pages 219–226, 2011. ISBN 9780769544601. doi: 10.1109/CLOUD.2011.31.

Federal Trade Commision (FTC). Protecting Consumer in an Era of Rapid Change: Recommendations for Businesses and Policymakers. Technical Report March, Federal Trade Comission, 2012. URL https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers.

M. Férnandez, A. Gómez-Pérez, and N. Juristo. METHONTOLOGY: From Ontological Art Towards Ontological Engineering. Technical report, AAAI, 1997. URL https://www.researchgate.net/publication/50236211_METHONTOLOGY_from_ontological_art_towards_ontological_engineering.

E. Ferro, M. Girolami, D. Salvi, C. Mayer, J. Gorman, A. Grguric, R. Ram, R. Sadat, K. M. Giannoutakis, and C. Stocklöw. The UniversAAL Platform for AAL (Ambient Assisted Living). *Journal of Intelligent Systems*, 24(3):301–319, 8 2015. ISSN 03341860. doi: 10.1515/JISYS-2014-0127.

S. Fischer-Hübner, J. Angulo, and T. Pulls. How can Cloud Users be Supported in Deciding on Tracking and Controlling How their Data are Used ? In M. Hansen, J. Hoepman, R. Leenes, and D. Whitehouse, editors, *IFIP Advances in Information and Communication Technology (IFIPAICT)*, volume 1983, pages 77–92. Springer, Berlin, Heidelberg, 2014. ISBN 9783642551369.

A. Forkan, I. Khalil, and Z. Tari. CoCaMAAL: A cloud-oriented context-aware middleware in ambient assisted living. *Future Generation Computer Systems*, 35: 114–127, 2014. ISSN 0167739X. doi: 10.1016/j.future.2013.07.009.

Fraunhofer AAL. PERSONA - PERceptive Spaces prOmoting iNdependent Aging within dynamic ad-hoc Device Ensembles, 2008. URL `http://www.aal.fraunhofer.de/projects/persona.html`.

C. Fredrich, H. Kuijs, and C. Reich. An Ontology for User Profile Modelling in the Field of Ambient Assisted Living. In A. Koschel and A. Zimmermann, editors, *Service Computation 2014*, volume 5, pages 24–31. IARIA, 2014. ISBN 9781612083377. URL `http://www.thinkmind.org/index.php?view=article&articleid=service_computation_2014_1_40_10014`.

W. Fumy, M. D. Soete, E. J. Humphreys, T. Chikazawa, J. Amsenga, and K. Rannenberg. ISO/IEC 27018:2014 - Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors. Technical Report attachment 1, ISO, 2014. URL `https://www.iso.org/standard/61498.htmlhttp://www.iso.org/iso/catalogue_detail?csnumber=61498`.

O. Gadyatskaya, F. Massacci, and A. Philippov. Security-by-Contract for the OSGi Platform. In *SEC 2012: Information Security and Privacy Research*, pages 364–375. Springer, Berlin, Heidelberg, 2012. doi: 10.1007/978-3-642-30436-1{_}30. URL `http://link.springer.com/10.1007/978-3-642-30436-1_30`.

H. Gassmann. OECD guidelines governing the protection of privacy and transborder flows of personal data, 1981. ISSN 03765075.

N. Geoffray, G. Thomas, G. Muller, P. Parrend, S. Frénot, and B. Folliot. I-JVM: A Java virtual machine for component isolation in OSGi. In *Proceedings of the International Conference on Dependable Systems and Networks*, pages 544–553. IEEE, 6 2009. ISBN 9781424444212. doi: 10.1109/DSN.2009.5270296. URL `http://ieeexplore.ieee.org/document/5270296/`.

P. Georgieff. Ambient Assisted Living: Marktpotenziale IT-unterstützter Pflege für ein selbstbestimmtes Altern. *Informations- und Medientechnologie in Baden-Würtemberg*, Marktanaly:1829–1841, 2008. ISSN 1861-5066. URL `http://en.scientificcommons.org/41985737`.

Glen McCluskey. Using Java Reflection. Technical report, Oracle, 1998. URL `https://www.oracle.com/technetwork/articles/java/javareflection-1536171.html`.

Google. Change app permissions on your Android phone, 2022. URL https://support.google.com/googleplay/answer/6270602?hl=en.

Google. Privacy and Security - Permissions and APIs that Access Sensitive Information, 2023. URL https://support.google.com/googleplay/android-developer/answer/9888170?hl=en&ref_topic=9877467&sjid=17921467802154490878-EU.

J. Graham-Cumming. Inside the Log4j2 vulnerability (CVE-2021-44228), 12 2021. URL https://blog.cloudflare.com/inside-the-log4j2-vulnerability-cve-2021-44228/.

A. Grguric, D. Huljenic, and M. Mosmondor. AAL ontology: From design to validation. *2015 IEEE International Conference on Communication Workshop, ICCW 2015*, pages 234–239, 9 2015. doi: 10.1109/ICCW.2015.7247184.

B. M. V. Guerra, E. Torti, E. Marenzi, M. Schmid, S. Ramat, F. Leporati, and G. Danese. Ambient assisted living for frail people through human activity recognition: state-of-the-art, challenges and future directions. *Frontiers in Neuroscience*, 17, 2023. ISSN 1662453X. doi: 10.3389/FNINS.2023.1256682. URL /pmc/articles/PMC10577184//pmc/articles/PMC10577184/?report=abstracthttps://www.ncbi.nlm.nih.gov/pmc/articles/PMC10577184/.

S. Guilloteau and V. Mauree. Privacy in Cloud Computing. Technical Report March, ITU-T Technology Watch, 2012. URL http://www.itu.int/ITU-T/techwatchhttp://www.itu.int/en/ITU-T/techwatch/Pages/cloud-computing-privacy.aspx.

K. Z. Haigh and H. Yanco. Automation as Caregiver: A Survey of Issues and Technologies. In *Proceedings of the AAAI-02 Workshop "Automation as Caregiver"*, pages 39–53, 2002.

S. Helal, W. Mann, H. El-Zabadani, J. King, Y. Kaddoura, and E. Jansen. The Gator Tech Smart House. *Computer*, 38(3):50–60, 2005.

H. Hietala, V. Ikonen, I. Korhonen, J. Lähteenmäki, A. Maksimainen, V. Pakarinen, J. Pärkkä, and N. Saranummi. Feelgood-Ecosystem of PHR based products and services. Technical report, VTT Technical Research Centre of Finland, 2009.

J.-H. Hoepman. Privacy Design Strategies (extended abstract). In N. Cuppens-Boulahia, F. Cuppens, S. Jajodia, A. Abou El Kalam, and T. Sans, editors, *SEC 2014: ICT System Security and Privacy Protection*, volume 428, pages 446–459. Springer, Berlin, Heidelberg, 2014.

C.-C. Huang, P.-C. Wang, and T.-W. Hou. Advanced OSGi Security Layer. In *21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07)*, pages 518–523. IEEE, 2007. ISBN 0-7695-2847-3. doi: 10.1109/AINAW.2007.70. URL http://ieeexplore.ieee.org/document/4224156/.

M. Huch. Identification and characterization of the main stakeholder groups for "ICT for Ageing" solutions. Technical report, BRAID Project, 2010.

ISO/IEC 27001. Information technology — Security techniques — Information security management systems — Requirements. *Iso/Iec*, pages 1–24, 2013. ISSN 0317-0861. doi: 10.1109/IEEESTD.2005.339589.

M. D. Janse. Amigo Final Report. Technical report, Amigo project consortium, 2004.

M. D. Janse. AMIGO - Ambient Intelligence for the Networked Home Environment. Technical report, Amigo project consortium, 2008. URL http://www.hitech-projects.com/euprojects/amigo/amigo.htm.

P. Jaszczyk and D. Król. Updatable multi-agent OSGi architecture for smart home system. Technical report, UN: Department of Economics and Social Affairs - Population Division, Berlin Heidelberg, 2010. URL http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6258524.

Jondos GmbH. JonDonym - the anonymisation service, 2011. URL https://anonymous-proxy-servers.net/index.html.

D. Kafura. OASIS eXtensible Access Control Markup Language (XACML) TC, 2004. URL http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml.

E. Kedrosky. Worst AWS Data Breaches of 2021, 12 2021. URL https://sonraisecurity.com/blog/worst-aws-data-breaches-of-2021/.

J. E. Kim, G. Boulos, J. Yackovich, T. Barth, C. Beckel, and D. Mosse. Seamless integration of heterogeneous devices and access control in smart homes. *Proceedings - 8th International Conference on Intelligent Environments, IE 2012*, pages 206–213, 2012. doi: 10.1109/IE.2012.57. URL http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6258524.

M. Klein, A. Schmidt, and R. Lauer. Ontology-Centred Design of an Ambient Middleware for Assisted Living: The Case of SOPRANO. In *Context*, volume 10, page 2007, 2007. URL http://publications.andreas.schmidt.name/klein_schmidt_lauer_AIM-CU_KI07.pdf.

S. Korff. PETs in Your Home - How Smart is That? *Symposium on Usable Privacy and Security*, 2013.

H. Kuijs and C. Reich. An Ambient Assisted Living Platform as a Service Architecture for Context Aware Applications and Services. *Proceeding - 1. Baden-Württemberg Center of Applied Research Symposium on Information and Communication Systems*, 1:70–74, 2014.

H. Kuijs and C. Reich. Towards Privacy for Ambient Assisted Living in a Hybrid Cloud Environment. *Proceedings - 2nd Baden-Württemberg Center of Applied Research Symposium on Information and Communication Systems*, 2:41–45, 2015.

H. Kuijs, C. Rosencrantz, and C. Reich. A Context-aware, Intelligent and Flexible Ambient Assisted Living Platform Architecture. *CLOUD COMPUTING 2015 : The Sixth International Conference on Cloud Computing, GRIDs, and Virtualization*, pages 70–76, 2015. ISSN 2308-4294.

H. Kuijs, C. Reich, M. Knahl, and N. Clarke. A Scalable Architecture for Distributed OSGi in the Cloud. In *Proceedings of the 6th International Conference on Cloud Computing and Services Science*, pages 109–117. SCITEPRESS - Science and and Technology Publications, 2016. ISBN 978-989-758-182-3. doi: 10.5220/0005810301090117.

H. Kuijs, T. Bayer, C. Reich, M. Knahl, and N. Clarke. Privacy enhancing data access control for ambient assisted living. In *CLOSER 2019 - Proceedings of the 9th International Conference on Cloud Computing and Services Science*, 2019. ISBN 9789897583650. doi: 10.5220/0007735804480455.

H. Kuijs, C. Reich, M. Knahl, N. Clarke, and I. Ognjanovic. The Need for Emergency-Based Access Control in AAL Systems. *2022 11th Mediterranean Conference on Embedded Computing (MECO)*, pages 1–6, 6 2022. doi: 10.1109/MECO55406.2022.9797201. URL https://ieeexplore.ieee.org/document/9797201/.

C. Kunze and M. Renyi. ZAFH-AAL - Zentrum für angewandte Forschung an Hochschulen für Ambient Assisted Living, 2015. URL https://imtt.hs-furtwangen.de/imtt/portfolio/zafh-aal/.

S. Lauriks, A. Reinersmann, H. G. Van der Roest, F. J. Meiland, R. J. Davies, F. Moelaert, M. D. Mulvenna, C. D. Nugent, and R. M. Dröes. Review of ICT-based services for identified unmet needs in people with dementia. *Ageing Research Reviews*, 6(3):223–246, 2007. ISSN 15681637. doi: 10.1016/J.ARR.2007.07.002.

D. le Métayer. A Formal Privacy Management Framework. *Formal Aspects in Security and Trust*, 5491:162–176, 2009. ISSN 03029743. doi: 10.1007/978-3-642-01465-9{_}11. URL http://www.springerlink.com/index/q7505648948p9710.pdf.

C. Lewis and T. Buffel. Aging in place and the places of aging: A longitudinal study. *Journal of Aging Studies*, 2020. doi: 10.1016/j.jaging.2020.100870. URL https://doi.org/10.1016/j.jaging.2020.100870.

Linux Foundation Collaborative Projects. Cloud Foundry | The Industry Standard For Cloud Applications, 2015. URL https://www.cloudfoundry.org/.

L. Litz and M. Gross. Covering assisted living key areas based on home automation sensors. In *2007 IEEE International Conference on Networking, Sensing and Control, ICNSC'07*, pages 639–643. IEEE, 2007. ISBN 1424410762. doi: 10.1109/ICNSC.2007.372854. URL http://ieeexplore.ieee.org/document/4239067/.

F. Liu, J. Tong, J. Mao, R. Bohn, J. Messina, L. Badger, and D. Leaf. NIST Special Publication 500-292: Cloud Computing Reference Architecture. Technical report, National Institute of Standards and Technology, Gaithersburg, 2011. URL http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=909505.

D. Liveri, A. Drougkas, and A. Zisi. Cloud Security for Healthcare Services. Technical report, European Network and Information Security Agency (ENISA), 1 2021. URL https://www.enisa.europa.eu/publications/cloud-security-for-healthcare-services.

F. Lupescu. Foreword. In G. van den Broek, F. Cavallo, L. Odetti, and C. Wehrmann, editors, *Ambient Assisted Living Roadmap*, chapter Foreword, pages VII–X. VDI/VDE-IT, 2009. URL https://www.digitalhealthnews.eu/images/stories/aaliance-roadmap-document-august-2009.pdf.

matter-smarthome. FAQ – frequently asked questions about Matter • matter-smarthome, 2022. URL https://matter-smarthome.de/en/matter-faq-en/.

Q. McNemar. Note on the sampling error of the difference between correlated proportions or percentages. *Psychometrika*, 12(2):153–157, 6 1947. ISSN 0033-3123. doi: 10.1007/BF02295996.

K. Meier, F. Kemmer, C. Reich, V.-S. Buck, and M. Duffner. RZV StudiCloud – Kooperative Dienste des Regionalen Zentrums Virtualisierung. *Kooperation von Rechenzentren*, pages 255–268, 10 2016. doi: 10.1515/9783110459753-021/PDF.

P. Mell and T. Grance. NIST Special Publication 800-145: The NIST Definition of Cloud Computing. Technical report, NIST, 2011. URL https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf.

M. Memon, S. R. Wagner, C. F. Pedersen, F. H. Aysha Beevi, and F. O. Hansen. Ambient Assisted Living Healthcare Frameworks, Platforms, Standards, and Quality Attributes. *Sensors 2014, Vol. 14, Pages 4312-4341*, 14(3):4312–4341, 3 2014. ISSN 1424-8220. doi: 10.3390/S140304312. URL https://www.mdpi.com/1424-8220/14/3/4312/htmhttps://www.mdpi.com/1424-8220/14/3/4312.

Microsoft. Microsoft HealthVault, 2016. URL https://www.healthvault.com.

Miele & Cie. KG. Miele@home - Intelligente Vernetzung für Zuhause, 2022. URL https://www.miele.de/haushalt/mieleathome-11825.htm.

M. Mikalsen. MPOWER. http://www.sintef.no/Projectweb/MPOWER/, 9 2009.

A. u. T. B.-W. Ministerium für Wirtschaft. Digitale Souveränität / Wirtschaft Digital BW, 2022. URL https://www.wirtschaft-digital-bw.de/aktuelles/thema-des-monats/digitale-souveraenitaet.

J. B. Mocholí, P. Sala, C. Fernández-Llatas, and J. C. Naranjo. Ontology for modeling interaction in ambient assisted living environments. *IFMBE Proceedings*, 29: 655–658, 2010. ISSN 16800737. doi: 10.1007/978-3-642-13039-7{_}165/COVER. URL https://link.springer.com/chapter/10.1007/978-3-642-13039-7_165.

J. Moore. Which sectors are most vulnerable to cyber attacks?, 1 2020. URL https://www.ifsecglobal.com/cyber-security/which-sectors-are-most-vulnerable-to-cyber-attacks/.

J. C. Naranjo, C. Fernandez, P. Sala, M. Hellenschmidt, and F. Mercalli. A modelling framework for ambient assisted living validation. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 5615 LNCS(PART 2):228–237, 2009. ISSN 03029743. doi: 10.1007/978-3-642-02710-9{_}26/COVER. URL https://link.springer.com/chapter/10.1007/978-3-642-02710-9_26.

National Academies of Sciences / Engineering / Medicine. Social Isolation and Loneliness in Older Adults: Opportunities for the Health Care System. *Social Isolation and Loneliness in Older Adults*, 2 2020. doi: 10.17226/25663.

I. Niles and A. Pease. Towards a standard upper ontology. *Formal Ontology in Information Systems: Collected Papers from the Second International Conference*, pages 2–9, 2001. doi: 10.1145/505168.505170.

N. F. Noy and D. L. McGuinness. Ontology Development 101: A Guide to Creating Your First Ontology. *Stanford Knowledge Systems Laboratory*, page 25, 2001. ISSN 09333657. doi: 10.1016/j.artmed.2004.01.014. URL http://www.ksl.stanford.edu/people/dlm/papers/ontology101/ontology101-noy-mcguinness.html.

OneCommons. Open Cloud Services, 2022. URL http://www.onecommons.org/open-cloud-service-definition.

OpenESB. Manage your services in a smart way, 2023. URL https://www.open-esb.net/.

Oracle Corporation. OpenJDK, 2016. URL http://openjdk.java.net/.

OSGI Alliance. OSGi Service Platform Core Specification. Technical Report Release 4, Version 4.3, The OSGi Alliance, 4 2011.

OSGi Alliance. OSGi Service Platform Service Compendium. Technical Report Release 4, Version 4.3, The OSGi Alliance, 2012.

OSGi Alliance. Smart Home Market, 2016. URL http://www.osgi.org/Markets/SmartHome.

P. Parrend, S. Frenot, and S. Hohn. Privacy-Aware Service Integration. In *IEEE International Conference on Pervasive Services*, pages 397–402. IEEE, 7 2007. ISBN 1-4244-1326-5. doi: 10.1109/PERSER.2007.4283946. URL http://ieeexplore.ieee.org/document/4283946/.

S. Pearson and M. Casassa-Mont. Sticky Policies: An approach for managing privacy across multiple parties. *Computer*, 44(9):60–68, 9 2011. ISSN 00189162. doi: 10.1109/MC.2011.225. URL http://ieeexplore.ieee.org/document/5959137/.

Peerbits. Explore the Pros and Cons of Cloud Computing in Healthcare, 2023. URL https://www.peerbits.com/blog/pros-and-cons-of-cloud-computing-in-healthcare.html.

M. Petzold, K. Kersten, and V. Arnaudov. OSGi-based E-Health / Assisted Living. Technical report, ProSyst, 9 2013. URL http://www.prosyst.com/fileadmin/ProSyst_Uploads/pdf_dateien/ProSyst_M2M_Healthcare_Whitepaper.pdf.

A. Pfitzmann and M. Hansen. A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management. *Technical University Dresden*, pages 1–98, 2010. ISSN 00031224. doi: 10.1.1.154.635. URL http://dud.inf.tu-dresden.de/Anon_Terminology.shtml.

P. Pritzker and P. D. Gallagher. NIST Special Publication 500-291 Cloud Computing Standards Roadmap. Technical report, NIST, 2013. URL https://www.nist.gov/system/files/documents/itl/cloud/NIST_SP-500-291_Version-2_2013_June18_FINAL.pdf.

Publications Office of the European Union. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995. URL https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995L0046.

Publications Office of the European Union. Regulation (EU) 2016/679 Of The European Parliament And Of The Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016. URL https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679.

Publications Office of the European Union. Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, 2018. URL https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32018R1725.

Publications Office of the European Union. European Parliament resolution of 20 May 2021 on the ruling of the CJEU of 16 July 2020 — Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems ('Schrems II'), Case C-311/18 (2020/2789(RSP)), 2021. URL https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021IP0256.

Publications Office of the European Union. Search - CORDIS - European Commission, 2023. URL https://cordis.europa.eu/search?q='aal'AND'platform'&p=1&num=10&srt=Relevance:decreasing.

C. Reich, H. Kuijs, K. Wallis, and T. Bayer. Architektur zum Schutz der Privatsphäre in AAL-Systemen. In C. Kunze and C. Kricheldorff, editors, *Assistive Systeme und Technologien zur Förderung der Teilhabe für Menschen mit Hilfebedarf – Ergebnisse aus dem Projektverbund ZAFH-AAL*, chapter 2, page 156. Pabst, Freiburg, 2017. ISBN 978-3-95853-362-2.

Robert-Koch-Institut. Open-Source Project Corona-Warn-App, 2020. URL https://www.coronawarn.app/en/.

C. Rosencrantz, H. Kuijs, C. Reich, B. Weber-Fiori, and M. H.-J. Winter. Entwicklung einer Informations- und Kommunikationsplattform für ältere Menschen. *ENI 2015, IT im Gesundheits-, Pflege- und Sozialbereich: Qualität und Effizienz durch IT*, 2015.

M. Rost. Datenschutz bei Ambient Assist Living (AAL) durch Anwendung der Neuen Schutzziele. Technical report, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, 2011. URL www.maroki.de/pub/privacy/DS_in_AALSystemen.pdf.

M. Rost and K. Bock. Privacy by Design und die Neuen Schutzziele: Grundsätze, Ziele und Anforderungen. *DuD - Datenschutz und Datensicherheit*, 35(1):30–35, 2011. ISSN 1614-0702. doi: 10.1007/s11623-011-0009-y.

P. Rothenpieler, C. Becker, and S. Fischer. Privacy concerns in a remote monitoring and social networking platform for assisted living. In *IFIP Advances in Information and Communication Technology*, volume 352 AICT, pages 219–230, 2011. ISBN 9783642207686. doi: 10.1007/978-3-642-20769-3{_}18. URL http://www.itm.uni-luebeck.de/.

C. Rottondi, G. Verticale, and A. Capone. Privacy-preserving smart metering with multiple data Consumers. *Computer Networks*, 57:1699–1713, 2013. doi: 10.1016/j.comnet.2013.02.018.

R. Sadat, P. Koster, M. Mosmondor, D. Salvi, M. Girolami, V. Arnaudov, and P. Sala. Part III: The universAAL Reference Architecture for AAL. In R. Sadat, editor, *Universal Open Architecture and Platform for Ambient Assisted Living*. SINTEF, 11 2013.

B. Schilit, N. Adams, and R. Want. Context-aware computing applications. In *Workshop on Mobile Computing Systems and Applications*, pages 85–90, 1994. ISBN 0-8186-6345-6. doi: 10.1109/MCSA.1994.512740. URL http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=512740.

A. Schmidt, A. Schmidt, P. Wolf, P. Wolf, M. Klein, M. Klein, D. Balfanz, and D. Balfanz. SOPRANO Ambient Middleware: Eine offene, flexible und marktorientierte semantische Diensteplattform für Ambient Assisted Living. *2. Deutscher Kongress Ambient Assisted Living, Berlin, Januar 2009*, 2009. URL http://publications.andreas.schmidt.name/Schmidt_Wolf_Balfanz_Klein_SOPRANO_AAL09.pdf.

T. G. Silva and F. Alencar. An Ontology as Support for Specification of Non-functional Requirements of AAL Systems Considering Compliance Aspects. *The Computer Journal*, 5 2023. ISSN 0010-4620. doi: 10.1093/COMJNL/BXAD053. URL https://dx.doi.org/10.1093/comjnl/bxad053.

K. L. Skillen, L. Chen, C. D. Nugent, M. P. Donnelly, W. Burns, and I. Solheim. Ontological user profile modeling for context-aware application personalization. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, volume 7656 LNCS, pages 261–268. Springer Berlin Heidelberg, 2012a. ISBN 9783642353765. doi: 10.1007/978-3-642-35377-2{_}36. URL http://link.springer.com/10.1007/978-3-642-35377-2_36.

K. L. Skillen, L. Chen, C. D. Nugent, M. P. Donnelly, and I. Solheim. A user profile ontology based approach for assisting people with dementia in mobile environments. *Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, 34:6390–6393, 8 2012b. ISSN 1557-170X. doi: 10.1109/EMBC.2012.6347456. URL http://www.ncbi.nlm.nih.gov/pubmed/23367391http://ieeexplore.ieee.org/document/6347456/.

SoSci Survey GmbH. SoSci Survey - the Professional Solution for Your Online Survey, 2022. URL https://www.soscisurvey.de/en/index.

A. Sowa-Kofta, I. Marcinkowska, A. Ruzik-Sierdzińska, and R. Mackevičiūtė. Ageing policies - access to services in different Member States, 10 2021. URL https://www.europarl.europa.eu/RegData/etudes/STUD/2021/662940/IPOL_STU(2021)662940_EN.pdf.

State of Lower Saxony. Zweites Buch: Digitalisierung von Wirtschaft und Gesellschaft, 2020. URL https://www.niedersachsen.de/startseite/themen/digitales_niedersachsen/masterplan_digitalisierung/zweites_buch_digitalisierung_von_wirtschaft_und_gesellschaft/zweites-buch-digitalisierung-von-wirtschaft-und-gesellschaft-167943.html.

Statista. Smart Home - worldwide | Statista Market Forecast, 2016. URL https://www.statista.com/outlook/279/100/smart-home/worldwide.

Statista. Cloud Computing Dossier. Technical report, Statista, 2022a. URL https://de.statista.com/statistik/studie/id/22297/dokument/cloud-computing-statista-dossier/?locale=en.

Statista. Public Cloud - Market data analysis & forecasts. Technical report, Statista, 9 2022b. URL https://www.statista.com/study/85676/public-cloud-report/?locale=en.

Statista. Statista Digital Market Outlook / Product and Methodology. Technical report, Statista, 2022c. URL https://cdn.statcdn.com/static/img/emarkets/dmo-methodology-en.pdf.

T. Strang and C. Linnhoff-Popien. A Context Modeling Survey. *Workshop on Advanced Context Modelling, Reasoning and Management, UbiComp 2004 - The Sixth International Conference on Ubiquitous Computing*, Workshop o(4):1–8, 2004. doi: 10.1.1.2.2060. URL http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.2.2060&rep=rep1&type=pdf.

O. Stutz, S. Todt, S. Venzke-Caprarese, S. Boll, W. Heuten, and T. Wallbaum. Implementing Data Protection and Information Security in AAL. In *Ambient Assisted Living*, pages 59–68. Springer, Cham, 2016. doi: 10.1007/978-3-319-26345-8{_}6. URL http://link.springer.com/10.1007/978-3-319-26345-8_6.

L. Sweeney. k-ANONYMITY: A MODEL FOR PROTECTING PRIVACY. *International Journal on Uncertainty*, 10(5):557–570, 2002. ISSN 0218-4885. doi: 10.1142/S0218488502001648.

The Eclipse Foundation. What Is OSGi?, 2015. URL https://www.osgi.org/resources/what-is-osgi/.

The Eclipse Foundation. Eclipse desktop & web IDEs, 2022. URL https://www.eclipse.org/ide/.

The Kubernetes Authors. Kubernetes, 2023. URL https://kubernetes.io/.

The Linux Information Project. Vendor lock-in definition, 4 2006. URL http://www.linfo.org/vendor_lockin.html.

The OpenStack project. Application Programming Interfaces, 2015. URL http://developer.openstack.org/.

The OSGi Alliance. The OSGi Alliance OSGi Core. *OSGi Secification*, 6, 2014.

The universAAL IoT Coalition. universAAL IOT - a Technical Overview. Technical report, universAAL, 2022. URL https://github.com/universAAL/.

C. Thomborson. A Framework for System Security. In P. Stavroulakis and M. Stamp, editors, *Handbook of Information and Communication Security*, chapter 1, pages 3–19. Springer Berlin Heidelberg, 1 edition, 2010. ISBN 978-3-642-04116-7. doi: 10.1007/978-3-642-04117-4.

Tor Project. Tor Project: Anonymity Online, 2016. URL https://www.torproject.org/.

U.S. Department of Commerce. Safe Harbor Privacy Principles, 2000. URL https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/laws-regulation/data-protection-privacy/safe-harbor-privacy-principles.

U.S. Department of Commerce. Privacy Shield, 2016. URL https://www.privacyshield.gov/Program-Overview.

U.S. Department of Justice. Clarifying Lawful Overseas Use of Data Act - CLOUD ACT, 3 2018. URL https://www.justice.gov/criminal-oia/page/file/1152896/download.

User Interface Design GmbH. AttrakDiff, 2008. URL http://attrakdiff.de/index-en.html.

J. van Heek, S. Himmel, and M. Ziefle. Privacy, data security, and the acceptance of AAL-systems – A user-specific perspective. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, volume 10297 LNCS, pages 38–56. Springer, Cham, 2017. ISBN 9783319585291. doi: 10.1007/978-3-319-58530-7{_}4. URL http://link.springer.com/10.1007/978-3-319-58530-7_4.

S. Walderhaug, E. Stav, and M. Mikalsen. The MPOWER Tool Chain - Enabling Rapid Development of Standards-based and Interoperable Homecare Applications. *Norsk Informatikk Konferanse*, pages 103–107, 2007. URL https://www.researchgate.net/publication/230724821_The_MPOWER_Tool_Chain_-_Enabling_Rapid_Development_of_Standards-based_and_Interoperable_HomeCare_Applications.

T. Wang, J. Wei, W. Zhang, and H. Zhong. A framework for detecting anomalous services in OSGi-based applications. In *Proceedings - 2012 IEEE 9th International Conference on Services Computing, SCC 2012*, pages 250–257. IEEE, 6 2012. ISBN 9780769547534. doi: 10.1109/SCC.2012.59. URL http://ieeexplore.ieee.org/document/6274151/.

F. Wartena, J. Muskens, L. Schmitt, and M. Petković. Continua: The reference architecture of a personal telehealth ecosystem. In *The 12th IEEE International Conference on e-Health Networking, Applications and Services*, pages 1–6, 2010. doi: 10.1109/HEALTH.2010.5556588.

WeDo partnership. European quality framework for long-term care services : Principles and guidelines for the wellbeing and dignity of older people in need of care and assistance. Technical report, European Commission, 2012.

W. Wilkowska, J. Offermann, S. Spinsante, A. Poli, and M. Ziefle. Analyzing technology acceptance and perception of privacy in ambient assisted living for using sensor-based technologies. *PLoS ONE*, 17(7), 7 2022. ISSN 19326203. doi: 10.1371/JOURNAL.PONE.0269642. URL /pmc/articles/PMC9255774//pmc/articles/PMC9255774/?report=abstracthttps://www.ncbi.nlm.nih.gov/pmc/articles/PMC9255774/.

P. Wolf, A. Schmidt, J. P. Otte, M. Klein, S. Rollwage, B. König-Ries, T. Dettborn, and A. Gabdulkhakova. openAAL - The Open Source Middleware for Ambient Assisted Living (AAL). *AALIANCE conference*, pages 1–5, 2010. ISSN 00948276. doi: 10.1029/2006GL026143. URL http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.231.9106&rep=rep1&type=pdf.

B. Zander-Jentsch, F. Wagner, N. Rzayeva, and R. Busse. Germany, 2019.

S. Zavialova. Smart Home – Market Data & Forecast 2022 | Statista. Technical report, Statista, 12 2022. URL https://www.statista.com/study/42112/smart-home-report/?locale=en.

Acronyms

a4cloud Accountability for the Cloud. 51

AAL Ambient Assisted Living. 1–7, 9–14, 16–18, 20–23, 32, 33, 48, 52–54, 56–59, 61–67, 69–72, 74, 79, 103, 110, 117, 125, 126, 135, 157–159

AALIANCE European Ambient Assisted Living Innovation Alliance. 12, 15, 16, 59, 70

AI Artificial Intelligence. 11, 30, 159

AmI Ambient Intelligence. 9, 10

AMIGO Ambient Intelligence for the networked home environment. 59

API Application Programming Interface. 30, 43, 84

BDSG Bundesdatenschutzgesetz. 38

BRAID Bridging Research in Ageing and ICT Development. 17

CDT Center for Democracy and Technology. 48

CIO chief information officer. 50

CLI command-line interface. 85

CoCaMAAL Cloud-oriented Context-aware Middleware for Ambient Assisted Living. 67, 69

COTS commercial-of-the-shelf. 62, 101

CSA Cloud Security Alliance. 35

dOSGi Distributed OSGi. xi, 82, 83, 85–91, 95, 100

EC European Commission. 38, 39

ENISA European Network and Information Security Agency. 45, 119

EU European Union. 39, 50

EU GDPR General Data Protection Regulation of the European Union. 2, 34, 39, 40, 42, 49, 55, 74, 152, 160

FTC Federal Trade Comission. 48, 49

HRW Hochschule Ravensburg Weingarten. 108, 112

IaaS Infrastructure as a Service. 26–30, 80, 81, 84, 85, 89, 100

ICT Information and Communication Technology. 10, 11, 17, 44, 116

IoT Internet of Things. 30, 158

ISD informational self-determination. 48

JVM Java Virtual Machine. 70

MPOWER Middleware platform for eMPOWERing cognitive disabled and elderly. 60

NIST National Institute for Standards and Technology. 25, 27, 35

OASIS Open architecture for Accessible Services Integration and Standardization. 63, 64

OECD Organisation for Economic Co-operation and Development. 39

OSGi Open Service Gateway initiative. 7, 59, 63, 72, 80, 82, 83, 101

P3P Platform for Privacy Preferences. 46, 126

PaaS Platform as a Service. 2–7, 23, 26, 28, 30, 79, 81, 84–86, 89, 96, 100, 101, 155, 157

PbD Privacy by Design. 34, 36, 42, 45, 55, 56, 138, 143, 152, 157

PET Privacy Enhancing Technology. 44, 45, 55

PHP PHP: Hypertext Preprocessor. 142

PII Personal Identifiable Information. 3, 5, 37, 41, 45, 51, 117, 135

S4P SecPAL for Privacy. 47, 126

SaaS Software as a Service. 26–29, 50, 80, 81, 87, 89, 108

SIMPL SIMple Privacy Language. 47, 126

SLA Service Level Agreement. 28

SOPRANO Service Oriented PRogrammable smArt enviroNments for Older Europeans. 21, 61, 62, 64

SpeciAAL Security and Privacy Enhanced Cloud Infrastructure for Ambient Assisted Living. xi, xii, 6, 7, 69, 74–77, 80, 83, 84, 87–90, 96, 100, 103–106, 108, 116, 117, 120–123, 131–133, 139

TET Transparency Enhancing Tool. 51, 53

UI user interface. 85, 152

UniversAAL Universal Platform for Ambient Assisted Living. 53, 64–66, 69, 70, 158

VM Virtual Machine. 80, 82

XACML eXtensible Access Control Markup Language. 127, 129

Appendices

Appendix A

Posters for the Field Test

In order to clarify the individual scenarios in our field test (cf. chapter 8.4) to the test persons, posters with the individual tasks were printed and shown to them one after the other. The description of the individual tasks for the test persons was given orally. The test persons were able to reproduce the tasks directly on the prototype.

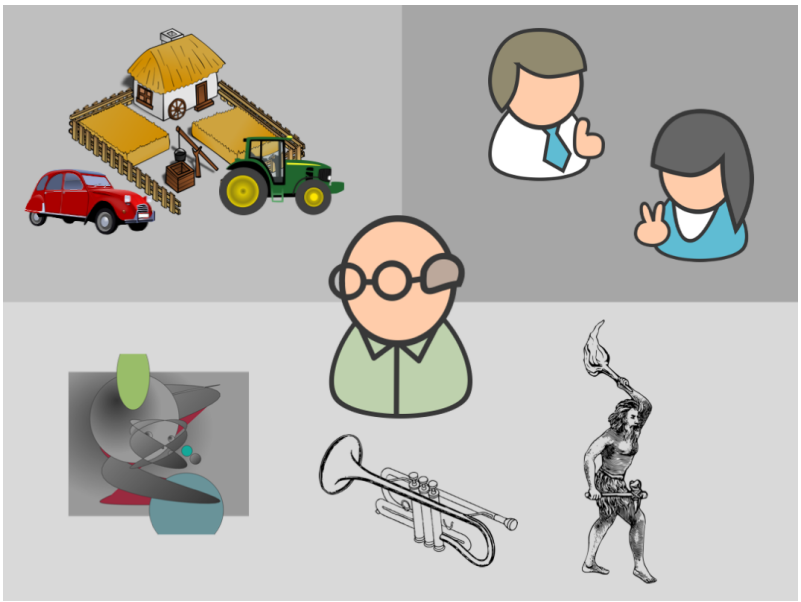

Figure A.1: Mr. F lives in a rural region and has two children living far away. He is interested in the arts, music and local history.

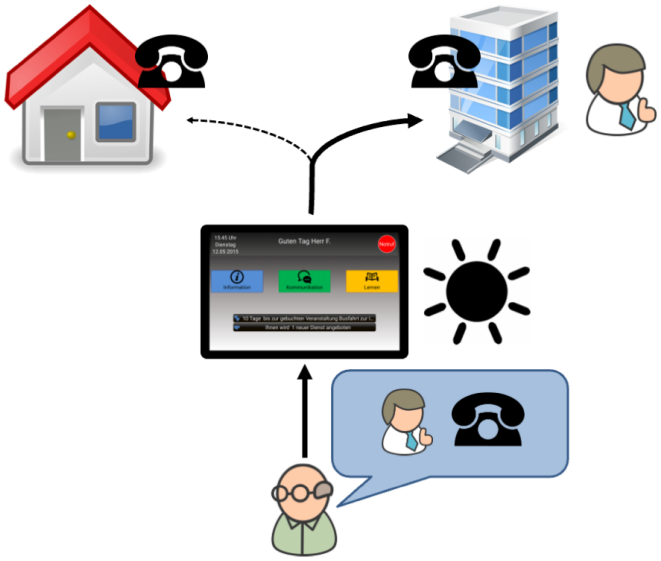

Figure A.2: Use Case A: Communication. During the day, the system automatically dials his son's office number.

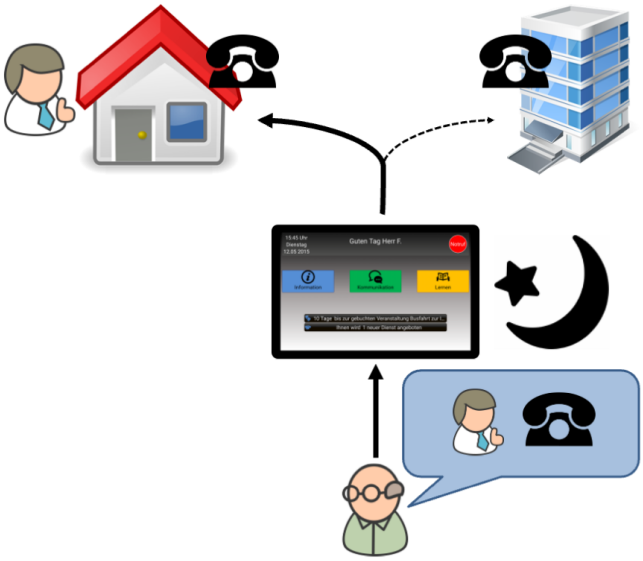

Figure A.3: Use Case A: Communication. During the night, the system automatically dials his son's private number.

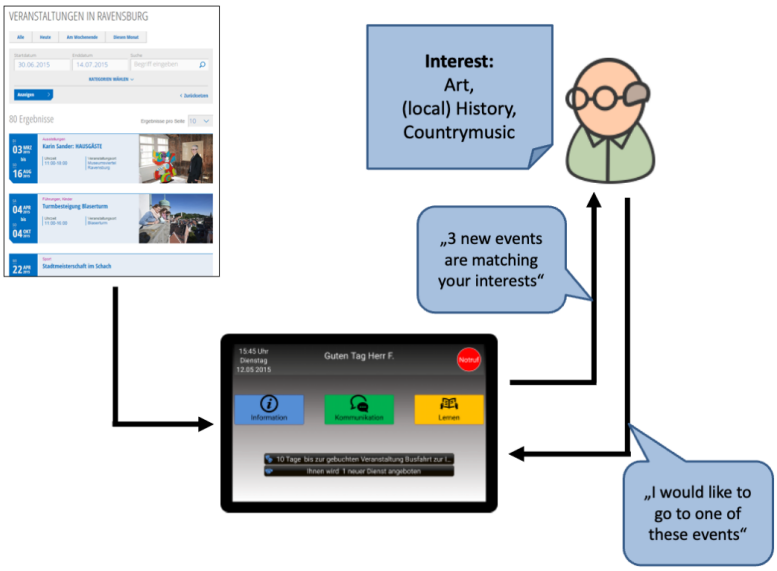

Figure A.4: Use Case B: Information. The system recommends events based on the interests of Mr. F.

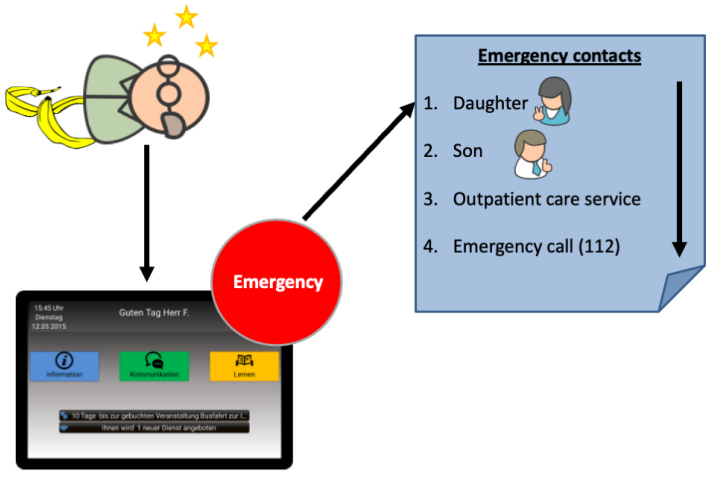

Figure A.5: Use Case C: Communication/Emergency. During an emergency, the system automatically dials a predefined set of emergency numbers to call for help.

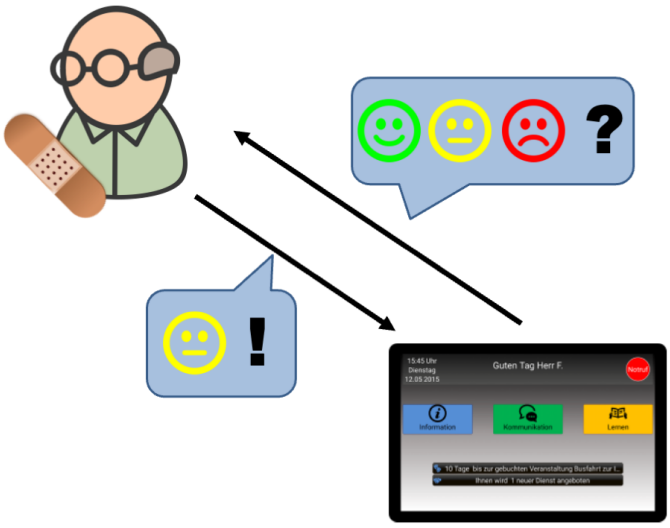

Figure A.6: Use Case D: Adaptation of Services. Everyday Mr. F. is asked how he feels.

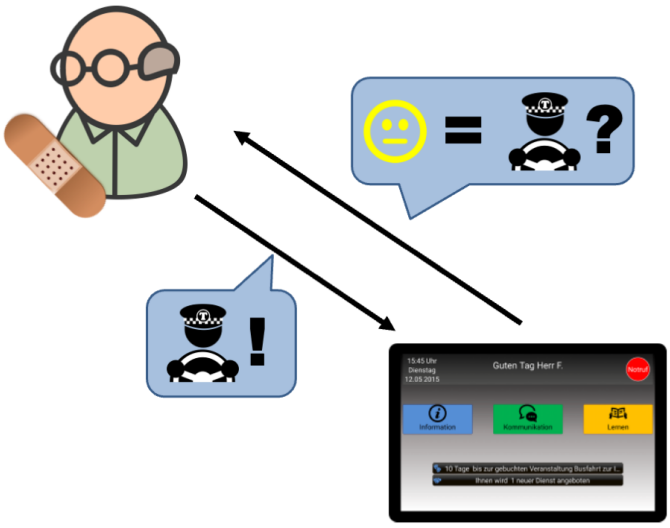

Figure A.7: Use Case D: Adaptation of Services. The system reacts to this new information by asking if he would like a lift to the event.

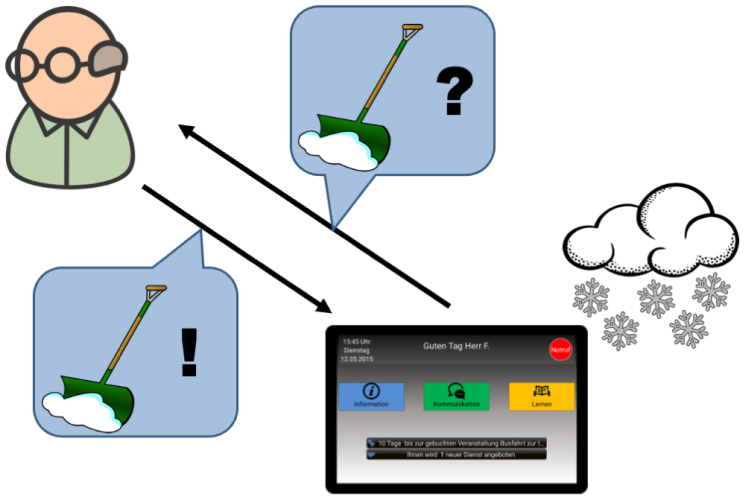

Figure A.8: Use Case E: Environment Awareness. The system receives the information that it has snowed during the night. It asks Mr F. if he would like a snow removal service.

Appendix B

Questionnaire: User Experience

This questionnaire was used to benchmark the user experience during the field test with our prototype. It is a simplified paper version of AttrakDiff (User Interface Design GmbH, 2008). Figure B.1 shows a graphical median of the results.

The study was conducted in Germany and in German. This questionnaire is a translation.

Evaluation of the SpeciAAL user interface

Please give your impression of the SpeciAAL user interface using the following word pairs.

Please tick one position in each line spontaneously - there is no right or wrong!

human								technical
isolating								connective
pleasant								unpleasant
inventive								conventional
simple								complicated
professional								unprofessional
ugly								attractive
practical								impractical
likeable								disagreeable
cumbersome								straightforward

stylish								tacky
predictable								unpredictable
cheap								premium
alienating								integrating
brings me closer to people								separates me from people
unpresentable								presentable
rejecting								inviting
unimaginative								creative
good								bad

confusing								clearly structured
repelling								appealing
bold								cautious
innovative								conservative
dull								captivating
undemanding								challenging
motivating								discouraging
novel								ordinary
unruly								manageable

Your answers will be evaluated anonymously. Background information on this questionnaire is available at https://www.attrakdiff.de/.

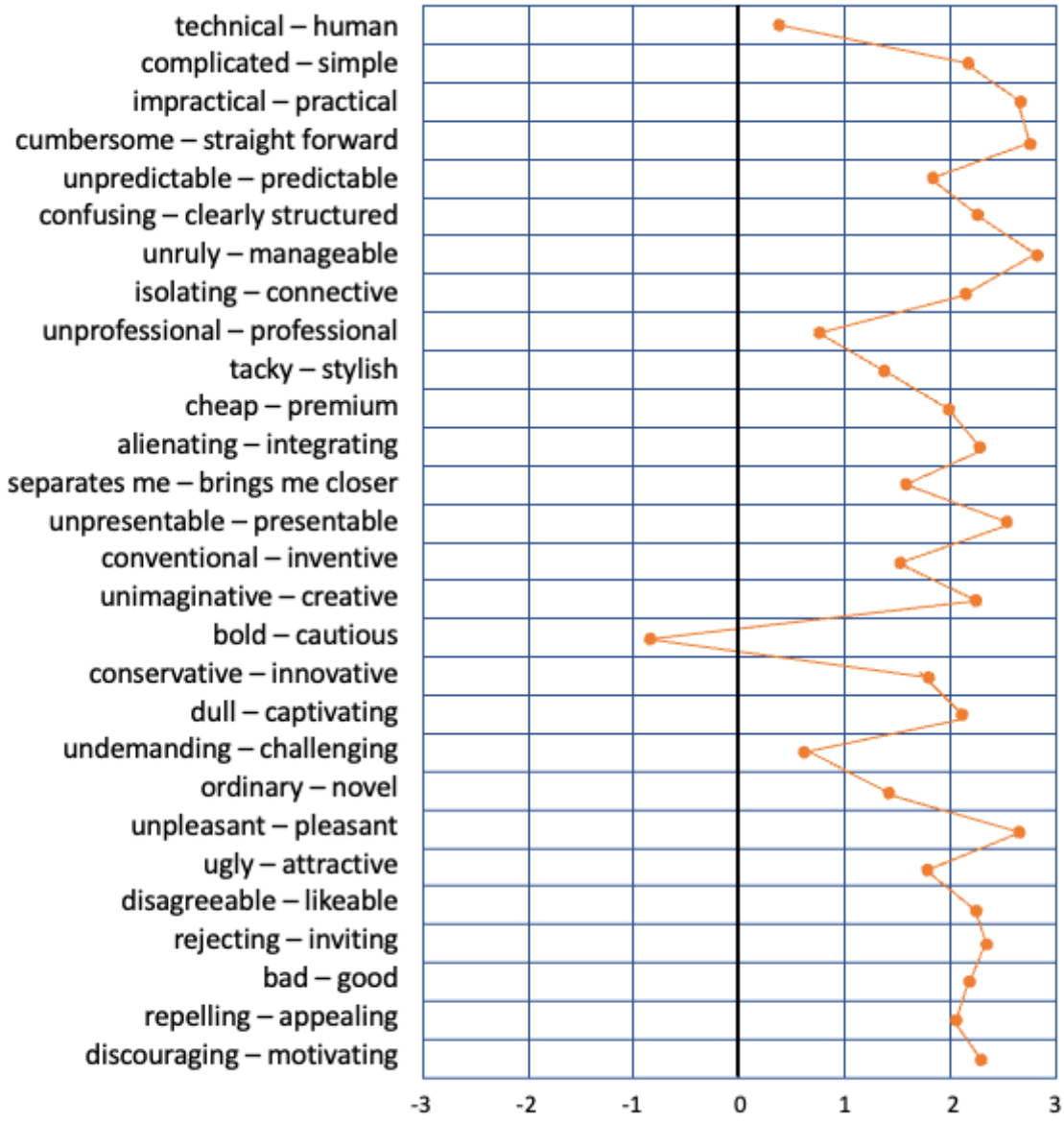

Figure B.1: Results: Median of the answers between the two word pairs

Appendix C

Questionnaire: Access Control

This questionnaire was used in the final survey in chapter 10. The dynamic function of converting the answers into natural language sentences on page 5 cannot be shown here. I therefore omitted and marked the missing elements accordingly.

The subjects could move forward and backward in the questionnaire, and of course, they were allowed to stop the interview at any time.

The study was conducted in Germany and in German. This questionnaire is a translation.

Thank you for taking the time to participate in this survey.

You are invited to take part in this research as an interviewee. Before we go any further, please read this information sheet carefully and understand what you might expect to do and what it will involve. You may discuss with others if you wish. Feel free to ask us if you need more information. Please consider if you want to take part or not in this research study.

Ambient Assisted Living (AAL) applications are designed for elderly people and collect personally identifiable information (PII), e.g., health data. During normal operations, this data should be kept private. But during emergency situations, the information is critical for carers/helpers to access. In our research, we are developing a data access control mechanism that enables users to define what data can be accessed by what other user or service. These rules can be defined during installation and changed to the user's liking during runtime. Special about this access control mechanism is the fact, that it can be adapted to the actual context (time, place, situation) of the user. In this survey, we want to find out, if special access-rules for emergency situations represent an added value to our AAL system.

Participant information Sheet (PDF)

If you have any questions, do not understand something or there is a technical problem, please feel free to contact me.
Yours sincerely
Hendrik Kuijs

Hendrik Kuijs, M. Sc.
Furtwangen University | Furtwangen University
Robert-Gerwig-Platz 1
78120 Furtwangen
Phone +49 7723 920 2370
E-mail: kui@hs-furtwangen.de

I have read the Participant Consent Form (PDF) and agree to participate in the research by starting the survey.

Please put yourself in the following situation:
You are using the system, that is able to support you in your daily tasks. It was recommended to you by your health insurance company and prepared for operation at your home by a health care provider. You yourself decide which functions and devices you want to use in your system.

You can set the system according to your wishes when installing new devices and functions.

You can determine whether only you or others can access the collected data.

- In the event that you **do not make any settings**, **only you** have access to the data.
- If you allow access to an additional person, this person is entitled to view the data via the system **at any time**.

In our examples, we use the following persons for whom you decide in the further course of this survey whether they should have access to your stored data:

- Your **relative** (partner, siblings, children, grandchildren),
- A friendly **neighbour**,
- your **doctor** or your **physician**,
- and the **device provider** of the device used to assist with questions and monitor proper operation.

You have decided to use new devices and now have the option of configuring the additional access rights.

Please put yourself in the following situation:
You have chosen a heart rate monitor and an electronic medication dispenser and are now configuring them according to your wishes.

(Please assign access rights by ticking. Multiple selection is possible.)

Heart rate monitor

A heart rate monitor automatically measures your pulse at regular intervals. The pulse data is stored in the system along with the time of measurement. If your pulse increases or decreases sharply, the system can inform you and third parties or make the log of past measurements accessible.

Who do you allow to view this data?

- ☐ Relative
- ☐ Neighbour
- ☐ Doctor
- ☐ Device provider

Medicine dispenser

An electronic medication dispenser automatically informs you whenever you need to take medication but have not yet done so. The time when the medication is taken is thereby electronically logged along with the type and quantity of the medication.

Who do you allow to see this data?

- ☐ Relative
- ☐ Neighbour
- ☐ Doctor
- ☐ Device provider

The system has been updated: You can now share not only the entire device, but different **data** of the devices with other people.

Please put yourself in the following situation:
It sometimes happens that you forget to take your tablets. For some time now, you have been suffering from sudden heart rhythm disturbances, which you have managed to control to some extent with your medication.

Heart rate monitor

In addition to the current pulse, the device also stores the occurrence of alarms, due to too high or too low a pulse, as well as an overview of all events and the complete pulse history.

Who do you allow to view the following data?

	Relative	Neighbour	Doctor	Device provider
Current pulse	☐	☐	☐	☐
Last alarm (pulse too high/ pulse too low)	☐	☐	☐	☐
Total recorded pulse waveform	☐	☐	☐	☐

Medicine dispenser

The electronic medication dispenser stores the name of the medication to be taken, the exact time and medication of the last intake and the history of all intakes in the past.

Who do you allow to view the following data?

	Relative	Neighbour	Doctor	Device provider
Name of the medicine	☐	☐	☐	☐
Last intake	☐	☐	☐	☐
All intakes	☐	☐	☐	☐

In addition to the simple yes/no rules, the system also has **situation-based access permissions**. For example, the **occurrence of an emergency situation** can grant additional access that would otherwise be prevented by the system.

Please put yourself in the following situation:
The heart rate monitor on your watch triggers an alarm in the system because your heart rate is exceptionally low. You feel as if you are about to lose consciousness.

Heart rate monitor

Who do you allow in an emergency to view the following data?

	Relative	Neighbour	Doctor	Device provider
Current pulse	☐	☐	☐	☐
Last alarm (too high/too low)	☐	☐	☐	☐
Pulse in the course	☐	☐	☐	☐

Medication dispenser

Who do you allow in case of emergency to see the following data?

	Relative	Neighbour	Doctor	Device provider
Name of the medicine	☐	☐	☐	☐
Last intake	☐	☐	☐	☐
All intakes	☐	☐	☐	☐

Page 05

[Summary of previously selected access permissions for the heart rate monitor].

Does this configuration meet your expectations?

- ○ Yes
- ○ No

[Summary of previously selected access permissions for the medication dispenser].

Does this configuration meet your expectations?

- ○ Yes
- ○ No

Page 06

[Summary of previously selected access permissions for the heart rate monitor].

You have indicated that the access rules for the heart rate monitor data do not match your expectations.

Please explain why?

[Summary of previously selected access permissions for the medication dispenser].

You have indicated that the access rules for the heart rate monitor data do not match your expectations.

Please explain why?

Which statement applies to your data in the cases described?

	I fully agree				I disagree
I can control the protection of my data with my decisions.	○	○	○	○	○
I have to make these decisions because otherwise I don't know what happens to my data.	○	○	○	○	○
I now know who can see my data in everyday life and in emergencies.	○	○	○	○	○
If I don't make a decision, other people can see my data.	○	○	○	○	○
I am aware that the system is also usable for me without these decisions.	○	○	○	○	○
My data is protected in the system against unwanted access.	○	○	○	○	○

How do you rate the presented setting of access rights?

	I fully agree				I disagree
The possibility to share only certain data of a device with others is helpful.	○	○	○	○	○
The distinction between everyday life and emergency is an added value.	○	○	○	○	○
Setting access rights is complicated.	○	○	○	○	○
I would have someone help me with the configuration.	○	○	○	○	○
I would use the system myself.	○	○	○	○	○
I would recommend the system to others around me.	○	○	○	○	○

Questions about yourself

Finally, a few questions about yourself.

1. Gender:

- ○ female
- ○ male
- ○ other, that is:

2. Which age group do you belong to?

- ○ younger than 20
- ○ 20 – 39
- ○ 40 – 59
- ○ 60 – 79
- ○ 80 and older

3. Which devices do you own yourself?

(Multiple answers possible)

- ☐ TV set
- ☐ Smartphone
- ☐ Telephone / mobile phone without internet
- ☐ Radio
- ☐ Laptop/PC
- ☐ DVD, Blu-ray-Player
- ☐ Tablet
- ☐ Game console
- ☐ E-Book-Reader
- ☐ Streaming stick or box (possibly also apps on the TV)
- ☐ Wearable (smartwatch, wristband, smart glasses, etc.)
- ☐ Smart speaker
- ☐ VR goggles
- ☐ Other:

4. How many people live in your household?

[Please select]

5. Do you regularly support others in setting up and operating technical equipment?

	I fully agree				I disagree
I help others to set up technical equipment.	○	○	○	○	○
I help others to use technical equipment.	○	○	○	○	○
I often explain technical devices to others.	○	○	○	○	○

6. Do you let others help you set up and use technical equipment?

	I fully agree				I disagree
I get help with setting up technical equipment.	○	○	○	○	○
I ask for help in using and operating technical equipment.	○	○	○	○	○
I let others explain technical devices to me.	○	○	○	○	○

Thank you for your participation!

We would like to thank you very much for your help.

Your answers have been saved, you can now close the browser window.

Hendrik Kuijs, Hochschule Furtwangen – 2022