ForeSight – User-Centered and Personalized Privacy and Security Approach for Smart Living

Jochen Bauer[1(✉)], Reiner Wichert[2], Christoph Konrad[1], Michael Hechtel[1], Simon Dengler[1,3], Simon Uhrmann[4], Mouzhi Ge[4], Peter Poller[5], Denise Kahl[5], Bruno Ristok[3], and Jörg Franke[1]

[1] Institute for Factory Automation and Production Systems,
Friedrich-Alexander-Universität Erlangen-Nürnberg,
Egerlandstraße 7, 91054 Erlangen, Germany
jochen.bauer@faps.fau.de

[2] SageLiving GmbH, Borngartenstraße 10, 64319 Pfungstadt, Germany

[3] C&S Computer und Software GmbH, Wolfsgäßchen 1, 86153 Augsburg, Germany

[4] Deggendorf Institute of Technology, Deggendorf, Germany

[5] German Research Center for Artificial Intelligence (DFKI),
Saarland Informatics Campus, Saarbrücken, Germany

Abstract. With the emerging Internet of Things (IoT) techniques in smart home applications, artificial intelligence (AI), and highly interoperable IoT s ystems enable the development of context-sensitive multi-domain services in smart homes [1]. However, while such systems create enormous challenges regarding security and privacy, the IoT practitioners may overlook certain security and privacy concerns such as European Union (EU) General Data Protection Regulation (GDPR). This paper describes the necessities to consider privacy- and security-related challenges for smart living platforms. Core elements of this contribution are a user survey to detect key aspects to fulfill users' expectations and an in-detail description of a Gaia-X-compatible software technology stack for the smart living domain. The concept will be applied to a smart kitchen use case.

Keywords: Active assisted living · Gaia-X · Smart home · Smart living

1 Introduction

The world is getting more and more connected and the smart home market has proven its relevance [2,3]. In Germany there is a market potential of 129 billion EUR, and the scenario is similar for other European countries. Therefore the smart home is a core element in a connected world. Among smart homes

Supported by German Federal Ministry for Economic Affairs and Climate Action (ForeSight, Team-X), European Union (Activage (IoT-01-2016 - Large Scale Pilots Programme)), Bavarian State Ministry of Health and Care (Dein Haus 4.0).

N. A. Streitz and S. Konomi (Eds.): HCII 2022, LNCS 13326, pp. 18–36, 2022.
https://doi.org/10.1007/978-3-031-05431-0_2

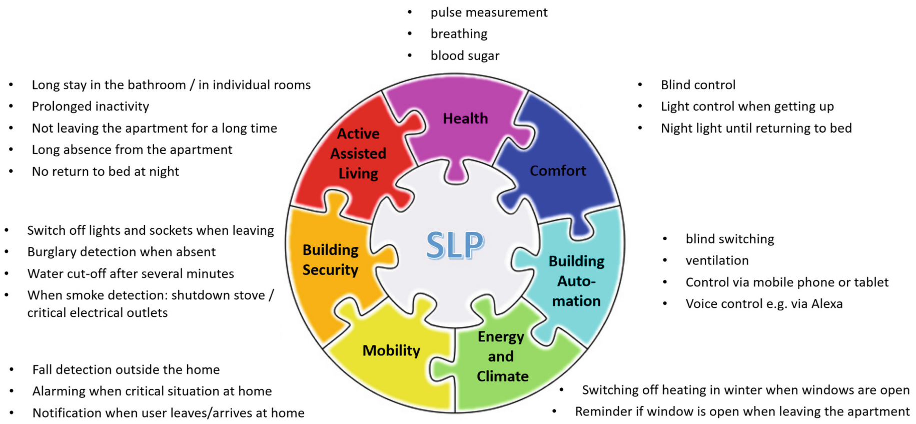
pulse measurement
breathing
blood sugar
Long stay in the bathroom / in individual rooms
Prolonged inactivity
Not leaving the apartment for a long time
Long absence from the apartment
No return to bed at night
Blind control
Light control when getting up
Night light until returning to bed
Active Assisted Living
Health
Comfort
SLP
Building Security
Building Auto-mation
Mobility
Energy and Climate
Switch off lights and sockets when leaving
Burglary detection when absent
Water cut-off after several minutes
When smoke detection: shutdown stove / critical electrical outlets
blind switching
ventilation
Control via mobile phone or tablet
Voice control e.g. via Alexa
Fall detection outside the home
Alarming when critical situation at home
Notification when user leaves/arrives at home
Switching off heating in winter when windows are open
Reminder if window is open when leaving the apartment

Fig. 1. Considered SLP use cases and relevant close-by domains that usually describe their own requirements.

and smart living several other domains are interwoven, e.g. energy management, health, and common smart home devices (see Fig. 1).

Future technological systems and their components need to be able to work together more closely to reuse solutions that have already been purchased and installed and to combine data for completely new applications. This requires open platforms that is capable of dynamically responding to changes. Once a system has been deployed, it adapts to different life situations and life phases. In order to be able to add dynamically, update or exchange offers from third-party providers, whether hardware or software, it is recommended to implement solutions on open semantic platforms. Such platforms need to consider and support privacy, security, and extendibility.

2 Challenges

According to the introduction several challenges arise in this heterogeneous field. The main challenges are related to the platform itself and the requirements regarding privacy and security.

2.1 Platform and Access-Management

Today's state-of-the-art situation is proprietary platform technologies that give one manufacturer power over all users. This lock-in effect is further coupled with opaque cloud architecture and a comprehensive consent form so that users can surrender their rights and data can be sold or used for marketing purposes accordingly. A solution for this is a user-individual and independent rights assignment system. This further enables both extensive context recognition and local execution so that the user's data is subject to a strict privacy and security code.

Due to the local nature of access management, the problem of decentralized trust also becomes omnipresent. As described by the European cloud initiative Gaia-X, this trust must be in place to allow local participants, detached from the cloud, to join a network.

2.2 Privacy, Security and Scalability

The EU regulates GDPR to set the rules for general data processing. The idea of GDPR is therefore to protect consumers and their data, so that a promising semantic platform approach needs to consider these privacy-related requirements [1,4]. Privacy cannot be achieved with a lack of security. It is especially challenging to ensure privacy and security in a home environment, where guests are often invited to the local network and many devices from different vendors are accessing these networks. Moreover, such networks are usually managed by nonprofessionals. For this user group, best-practice information security management strategies are hard to implement. In the end, there is a need for a solid identity and access management (IAM) routine that includes the local network and the cloud. Furthermore, such an IAM strategy should be user-centered and scalable to match the requirements for personal data, smart home data, smart building data, and smart city data. All these levels need their corresponding access rules. To enable the user as the owner of this data and the person in charge, a corresponding dashboard needs to be created and offered to everyone, that a user can track the frequency and the purpose of each data access event. Gaia-X as a decentralized cloud-based and service-oriented architecture seems to offer a promising approach for these requirements.

3 Approach

After the challenges have been described, we explain our approach in more detail. In this section, the subsections privacy and security, the platform components, the scalability, and the use case description are addressed.

3.1 Privacy and Security

The EU GDPR law [5] inevitably prescribes in Art. 25 GDPR Privacy by Design (PbD) with the wording "data protection by design and by default". For this purpose, suitable technical and organisational measures (TOM) must be taken both during the design phase and during subsequent data processing, such as strict data minimisation. In addition, data storage and use are subject to a general purpose limitation according to Art. 5 GDPR. A more precise interpretation of which TOMs must be taken in order to meet the requirements of the GDPR will only become apparent from future developments. Basically, PbD means that already in the design phase measures should be taken to minimize the risk of potential data loss and data misuse over the entire data life cycle – consisting of demand-oriented collection, processing, storage and deletion.

The four fundamental elements for sustainable compliance with data protection requirements are lawfulness of processing, risk management, TOMs and privacy friendly defaults (see Fig. 2). Ensuring the lawfulness of processing is the starting point. In the case of a SLPs, both a privacy policy and a declaration of consent as well as data processing agreements for third-party service providers are required as a legal basis. Besides the informed consent, the fulfillment of legal or contractual obligations and the associated legitimate interest may also be such a legal basis. Particularly in such a case, the purpose limitation and individual data erasure periods need to be observed. Due to the partly high protection requirements for the data to be processed, the data privacy aspects must be considered more carefully in the case of data transfer to third parties. According to Art. 35 GDPR, a data protection impact assessment must also be prepared by creating a structured risk analysis of the planned data processing based on the records of processing activities and examining the necessity and proportionality of the processing. Therefore, an accompanying risk management must be established by adapting the "IT-Grundschutz-Vorgehensmodell" (information technology (IT) basic protection procedure model) of the German Federal Office for Information Security (German abbreviation 'BSI') in the form of a data protection management system (DPMS). The organizational structure should be based on that of established information security management system (ISMS) such as ISIS12 [6] and VdS 10000 [7], so that the DPMS and the ISMS complement each other. Such a system can ensure the lawfulness, necessity as well as the fulfillment of data subjects' rights and data protection principles. According Art. 30 GDPR, a record of processing activities must also be kept in text form, containing the name and contact details of the responsible entity and, if applicable, the commissioner for data protection, the purposes of the processing, a description of the categories of data subjects and affected personals, categories of recipients, erasure periods and the categories of processing activities, as well as a description of the TOMs. This record, in turn, serves as the input parameter for risk management and represents the basis for fulfilling the documentation obligation, also with regard to the data subject's rights. It will also be able to transparently present the processing purposes. In order to comply with the data protection principles, aspects of data security, responsible data collection and processing, purpose limitation and transparency must be fulfilled. After identifying and assessing the risks, the objectives from a privacy perspective can be determined in addition to the data protection objectives in accordance with the Standard Data Protection Model (German abbreviation 'SDM') [8] of the committee of Independent German Federal and State Data Protection Supervisory Authorities – in abbreviated form German Data Protection Conference (German abbreviation 'DSK') – and addressed by specific countermeasures with suitable TOMs as part of a data protection concept. In this regard, it is possible to build on research conducted in the context of the telematics infrastructure, in which the data protection model was also applied, for example [9], the selection of TOMs in implementation is made in accordance with the "state of the art", whereby TeleTrust publishes a regularly updated guideline for this purpose [10].

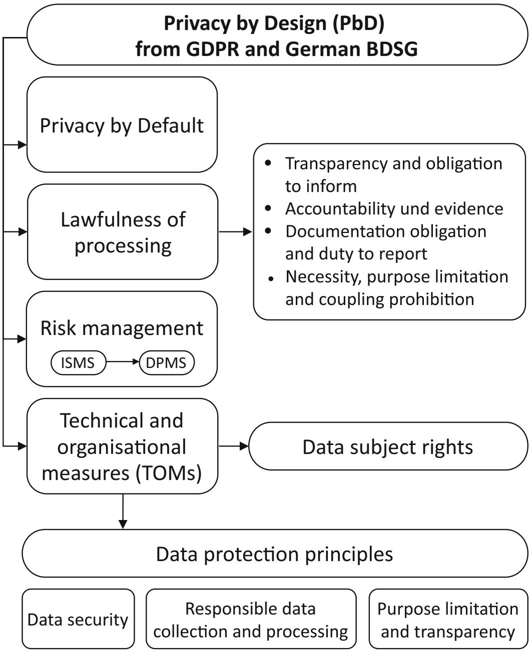
Privacy by Design (PbD) from GDPR and German BDSG
Privacy by Default
Lawfulness of processing
Risk management
ISMS
DPMS
Technical and organisational measures (TOMs)
Transparency and obligation to inform
Accountability und evidence
Documentation obligation and duty to report
Necessity, purpose limitation and coupling prohibition
Data subject rights
Data protection principles
Data security
Responsible data collection and processing
Purpose limitation and transparency

Fig. 2. Overview of the concept of PbD with the four basic elements for sustainable compliance and the data subjects' rights and data protection principles to be addressed.

For platform operators, there are some economical advantages: there is the reduction of risks in the area of IT security and the reduction of the effects of cyber attacks through distributed data storage and processing. In addition, data minimization would reduce compliance risks or at least make them calculable by reducing the complexity of data flows and strictly observing earmarking. This also applies to the overhead of complying with the prescribed documentation and evidence obligation. In addition to the preceding indirect advantages, a strict pursuit of PbD principles results in direct advantages for value creation and in competition with other platforms [11]. On the one hand, an adaptation of the architecture in responses to increasingly stringent legal requirements, if it is necessary to involve less effort and costs. An additional data abstraction, besides the desired semantic interoperability level, will also serve this goal. On the other hand, a feeling of insecurity has developed in a large portion of the population due to a loss of control and thus a more aware handling of personal data. By creating transparency in a central data protection control center and visualizing the generated data, both added value for the end user and trust in the provider can be strengthened and customer loyalty can be established [12,13], as is now also common with smartphone operating systems, for example. The current change in awareness could also lead to an increase in the willingness to pay, which in turn opens up new opportunities for monetization [12].

3.2 Platform Architecture

The ForeSight project follows the approach of a semantic platform that integrates solutions based on AI, interoperability, context-awareness, and smart home and smart building technologies into a flexible smart living platform [1,14]. ForeSight offers a flexible mechanism to handle requests, i.e. the requests are handled in the local network or, if necessary, will be offloaded to cloud services to increase performance. The core of ForeSight's architecture approach is the so-called thinking object (TO) – a device or group of devices that offers a specific service to the user or other TOs. There are three main modules, which are interacting to fulfill the system needs, here a service engineering module for service providers, e.g. a company of the housing industry, and an AI module to handle requests for computationally intensive operations, e.g. visually-based object identification, and an IoT module to connect to different smart home middleware systems, e.g. openHAB [15], which will connect to many different vendor-specific systems. In this work, ForeSight is connecting to openHAB to ensure interoperability on a syntactic level [14,20]. Besides, ForeSight will enable the usage of different smart home middleware systems like universAAL. To enrich this data with semantic information the Web of Things (WoT) approach is a key element.

IoT-Middleware. The openHAB is a smart home middleware, and it is possible to control different systems in one single graphical user interface (GUI) or app. The software uses specific components to offer an abstraction layer for all of its subsystems [14,16]. To connect to a third-party system like Homematic, it is necessary to create a binding. The binding coordinates the openHAB elements, here channels, items, and sitemaps to configure systems behavior. For automating event-driven tasks, there is the concept of rules, a script-like openHAB feature. There are several other smart living middleware systems or promising approaches apart from openHAB such as universAAL [17], HomeKit [18] and Matter [19].

Backend. In general, ForeSight tries to follow Gaia-X-compability (see Fig. 3) and explores several ways to achieve that, e.g. Sovereign Cloud Stack (SCS), Open Shift and Apache Kafka. Therefore we strive to identify challenges to gain Gaia-X-compatibility from a streaming platform to a common platform-as-a-service-provider.

Gaia-X offers users and providers of cloud services or cloud backends for on-premises applications the ability to negotiate securely and oligopolistically and to draft a user agreement without undesirable clauses. This offers the user the option to guarantee high scalability of the service without lock-in effects that would harm the end-users self-sovereign data usage (see Fig. 4).

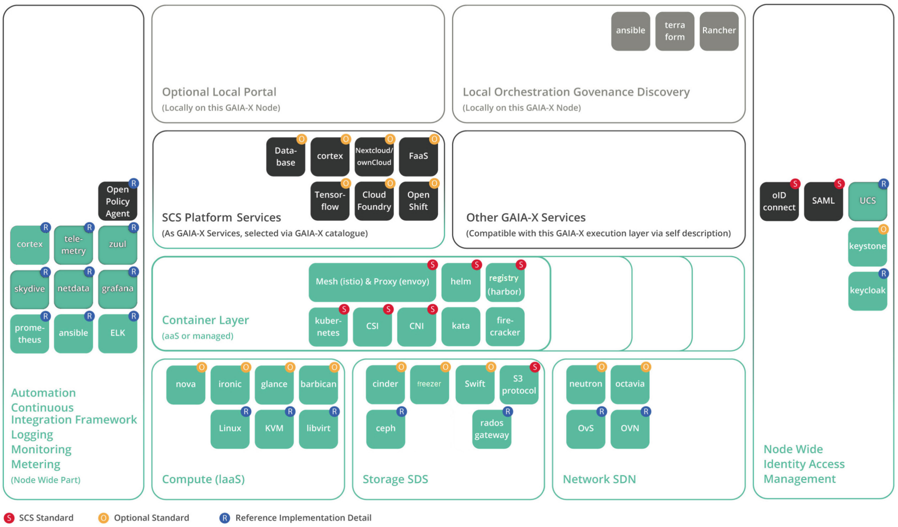

Fig. 3. Architectural overview of the SCS as used by Gaia-X with exemplary components [21]

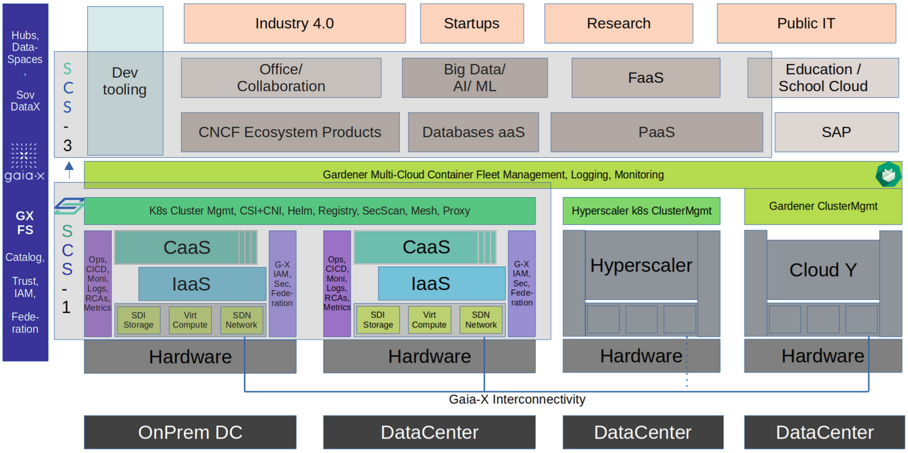

Fig. 4. Exemplary ecosystem overview of the SCS [21]

At the center of Gaia-X's decentralized trust model (see Fig. 5) is the user with his or her Self-Sovereign Identity (SSI). This identity is stored in a repository on a medium, such as a smartphone or an access card with built-in near-field communication (NFC). The user's SSI in turn consists of verifiable credentials issued by certified providers. This can be a citizens' office that verifies personal data from the identifier (ID) card. With the necessary credentials, users can then go to service providers and confirm their use with their SSI without having to disclose any specific data. The service provider thus trusts the verification by the provider of the verifiable credentials. However, it is important that there is a trust anchor that the service provider regards as trustworthy. This can be either the reputation of a company or a cryptographic check such as the eIDAS specifications.

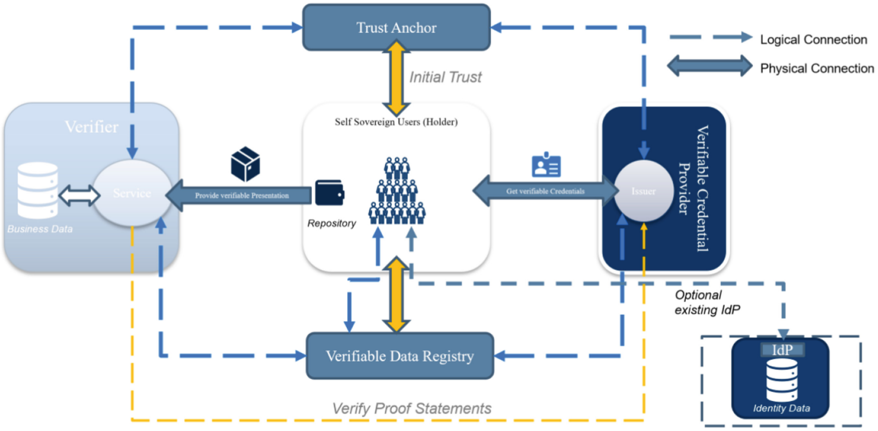

Fig. 5. Gaia-X-based concept of establishing trust in decentralized systems [22].

The Gaia-X Data Exchange Logging Service (see Fig. 6) allows traceability of transactions in the Gaia-X ecosystem without violating privacy and security requirements. The logging service is a stateless microservice that depend on other federation services, as it is directly coupled to a service [23]. The logging service is accessed by both providers and consumers to report changes to contracts. A token is used to validate if the contract exists and if the executing action is allowed. Likewise, it is possible for provider and consumer to talk to each other to retrieve accessible events. It is also foreseen that third-party providers are allowed to retrieve log messages. However, this must be approved by the service provider and provider/consumer. According to the specification, the stored log messages need to follow the W3C Linked Data Notification Protocol, which enables a very high level of interoperability, reusability, and decentralization of the notifications.

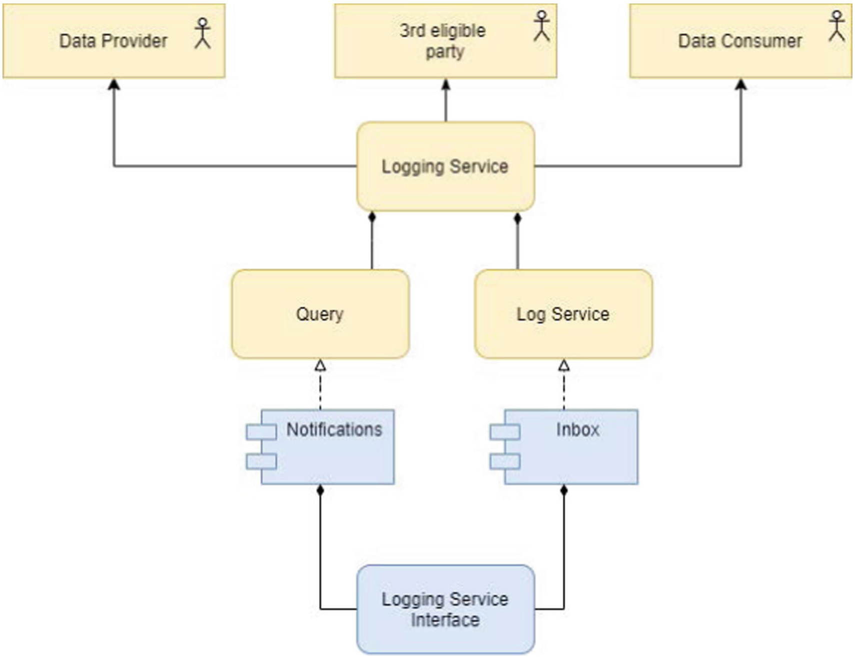

Fig. 6. Gaia-X logging mechanism to enable monitoring of service to service calls by granted users [24].

3.3 Scalability

To this end, architectures should be implemented either without cloud services, combined, or purely on the cloud side. According to this, Smart Living/Ambient Assisted Living (AAL) systems need to be structured so that they are able to combine and evaluate data both exclusively in the households and purely on the cloud side on a server. In addition, the merging and analysis of data should be distributed on both sides at the edge [25]. With this approach, users can decide where their data is collected and analyzed, giving a more secure feeling of data sovereignty. In solutions that are implemented together on client and server sides, the data is mirrored via a server-side gateway (digital twin), and thus services can be implemented on both sides. It should be possible to connect several platforms to implement cross-domain solutions. Since the user quickly loses control over who has access to the data with domain-overlapping applications and the merging of data, this leads to very high requirements for the protection of privacy and more complex requirements due to a large number of vulnerable accounts of IT security at each domain boundary. At the same time, systems are given the necessary flexibility for users to enable new business models for companies. For semantic platforms, there are completely new possibilities for recognizing specific situations and providing assistance in a variety of precisely tailored domains. Therefore, the installed sensors and actuators can be reused for other purposes and thus lead to cost savings [26] (see Fig. 1).

The merging of data across spatial boundaries can also generate additional added value such as building, facility, or quarter management, or enable optimized urban water and energy management and municipal traffic planning. Thus, the future platform systems should also enable scaling from the Smart Home, the building, the neighborhood (quarter), and finally to Smart City approaches [4]. Among the boundaries of these different spatial habitats and at all cloud connections, high-security requirements for data protection and IT security must be implemented so that the users would agree to the merging and extensive use of the data across living spaces. Different security levels have to be implemented at each of these borders, and the closer we get from the city to the apartment and the body space, the more stringent restrictions on privacy have to be implemented [26] (see Fig. 7).

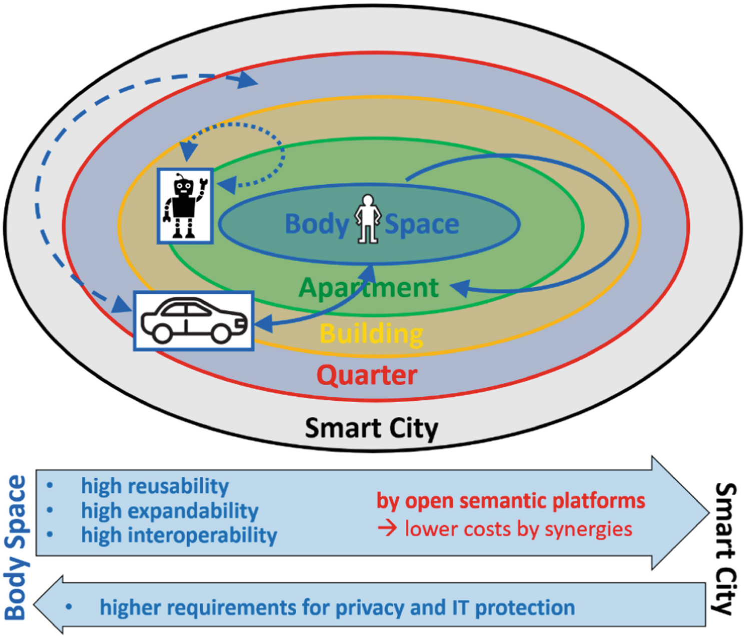

Fig. 7. High requirements for data protection and IT security between living spaces.

In order to meet this hurdle, software architectures need to build in such a way that they allow data to be merged across system boundaries to enable societal changes, the spread of diseases, and also linkage with other domains such as transport, energy, and water supply. This is to ensure optimal reusability, extensibility, and interoperability. The body space is to be understood as a mobile space that can move within the apartment. However, a user can also leave the apartment with his body space (close-to-the-body sensors and devices, e.g., blood glucose sensor for diabetes or his mobile phone) and enter other spaces, for example, other buildings, or be out in the city. He can also go to another mobile space like his car or public transport and move to other spaces. In this sense, a robot is also a mobile space that communicates with sensors and actuators in other spatial areas and with different users. There is also a sharp demarcation between the spatial areas from the point of view of privacy and IT protection. Otherwise, data across domain boundaries could not be appropriately delimited securely [25].

In the ForeSight project [27], these findings lead to the fact that a cross-domain use of data in the cloud must be subject to special attention both at the hierarchical levels in a spatial view and the merging and use of common data from different domains for aggregation. In many cases, it is no longer sufficient to consider the earmarked use required by the GDPR, because users can very rarely imagine what can be read from merged data. Suppose permission is given to use individual separated data, such as a motion detector to create movement profiles to switch on lights, for example, an electronic house access system to get easy access by mobile phone and a bed occupancy sensor to create a nice wake-up scenario with music and blinds. In that case, it could result in an analysis of who is currently in the apartment and what is happening in the bedroom, even the user has accepted only to use the data from the motion detector, access system, and bed sensor. Thus, any new application based on merged data need to allow the user to reconsider his consent.

Therefore, our approach is to make a direct request to the user, who can decide whether he wants to consent to this new purpose. However, since this information come from different domains and can also be used across spatial boundaries, the authorization for each spatial area and each domain must be set and stored separately in each piece of information in order to be able to define a control option for the use of information at the domain borders or a spatial area. For example, similar to rights management for apps on the mobile phone, which must be set explicitly, this can be implemented similarly for software services within the information. The rights management within the information determines the purpose for which it may be used. For example, movement data from the motion detector can be used for private services within the dwelling but not for the administration of the building, while ventilation data within the same dwelling would only be allowed for energy billing with the user's consent on a wider spatial scale. In return for consent to data use, a user could then be persuaded to agree to cheaper apartment rent. However, the decision-making authority must align with the user so that he can decide whether the information provided is of equal value, which conflicts with the most commonly used metaphor, "data is the new oil which possession can lead to great wealth. The profits generated from data resources belong to those who process the data, not those who originated it." [28] In contrast, with our approach, the decision-making authority should be returned to the user, where we believe that it will lead to a greater acceptance of the users.

3.4 Smart Kitchen Use Case

The Smart Kitchen use case contains a comprehensive assistance system in the area of nutrition, and includes a multitude of interconnected individual components, which continuously support the user over the course of a day. The ForeSight platform serves as a central data provision and exchange instrument based on semantically enriched information that can be accessed from anywhere. ForeSight-specific AI-driven services enable individually tailored assistance providing nutrition recommendations, nutrition preparation, household management, shopping support, and sporting activity recommendations, independent of the location and the devices used. Access to the individual services is based on authentication and the services themselves can be configured individually. This also means that the amount of personal data provided is entirely in line with the report-based privacy and security approaches presented. The more data a person provides about him or herself, the more efficient the individual services can be in providing support.

The core elements of the smart kitchen use case are the identification of food products based on image data, the digitization of purchasing data, intelligent household inventory management as well as two recommender systems, one for food selection and one for useful sports or recreation activities. The two systems intend to improve the client's health. In addition, the smart home system contains the integration of smart devices, e.g., a food processor, fridge, and pantry. The smart home also provides a small amount of context recognition, such as information about which person is in which room at runtime. Other necessary information comes from remote sources such as web services.

The household inventory management system combines food product identification and receipt digitization. After a purchase, the products are stored in the refrigerator or the pantry and automatically recorded by the camera. The shopping receipt is also photographed in a corresponding app and automatically digitized to a product list. The system then determines the new household inventory based on the last household inventory, the detected objects in the fridge and pantry, and the digitized receipt elements.

The food recommendation system provides the user with the ten most appropriate meals by taking into account the user's preferences. When proposing recipes, the availability of the ingredients and specific important details, such as weather conditions or the current side effects of team sport events, like the location or the organizing group, are taken into account. In addition to that, the system tries to reduce the overall waste by presenting a warning if a best consumption date is getting closer or indirectly by preferring recipes containing perishable products close to a best before date.

The following user story will describe one specific daily routine to increase the understanding of the smart kitchen use case. In the morning, the system detects that someone has entered the kitchen and determines who it is. Afterwards, a menu tailored to this person's preferences is recommended by the system based on his or her health related data, taste profile, food availability and established health goals. When preparing the meal, the person receives assistance from a smart kitchen such as the Cookit food processor. After having breakfast, the meal is evaluated by the scale of 5 stars. Additionally, the person can ask for a recipe recommendation for lunch. Out of the proposed recipes one is selected. A comparison of the ingredients of this recipe with the household inventory is performed and not available products are automatically added to the shopping list. When shopping, augmented reality (AR)-supported assistance in locating the products via a corresponding app is provided. Once at home, the household inventory is supplemented with the purchased products. After the products have been sorted, a comparison is made between the contents of the fridge, the contents of the pantry and the purchase receipt. After work, the person receives a recommendation for a sporting activity based on his preferences. When the activity is finished, the person evaluates it in the same way as he or she did before with the meal. The system can optimize the person's individual recommendations. In his or her absence, there is a maintenance message in the fridge and a corresponding dialog-supported data release for the installer or fridge owner. In the evening, the person displays the privacy report regarding the data generated by him and what services used what kind of data and how often they accessed this information. The interaction with the system takes place individually on the preferred channel, such as voice, mobile device or the computer. In addition to that, user's health related data are considered to improve recommendations or track the overall success of the health improvement process. Integrations of promising third-party approaches like the Gaia-X health projects [29], e.g. TEAM-X or HEALTH-X are currently considered to enable and improve health data management.

3.5 Implementation

In an intelligent kitchen environment, we demonstrate our current approach at the end of 2022. Due to the dynamic Gaia-X project progress and the decision that our efforts will be compatible with the Gaia-X ecosystem, we adapt to the current recommended technologies and semantically enriched information. To improve our development cycles dynamically, we are integrating users, external experts and experiences from other research projects continuously to carry out surveys and usability tests.

4 Methods

During the ForeSight project, usability tests, user surveys and expert interviews are happening. Out of a technical perspective, we are tracking Gaia-X-based recommendations and requirements. We strive to implement different technology approaches like Apache Kafka, OpenShift or SCS for the Backend and openHAB or universAAL as an IoT-module. After the implementation further tests regarding the technological robustness will be carried out.

To improve user-centered design and development, we carried out a survey to users of the universAAL system. Therefore the participants were used to smart home systems and everybody (n = 261) have been asked to rate the grade of importance (0 to 10 (highest importance)) and make an assumption how successfully this attribute is already implemented in the universAAL platform, so far (0 to 10 (very sophisticated)).

5 Results

Despite the complexity resulting from such vast integration of different domains, privacy protection is one of the most important aspects for humans and is extensively protected as a private retreat by Art. 13 GG of the German Constitutional Law. This has also been recognized by the Federal Ministry of Education and Research and demanded in the framework program "digital, safe, sovereign" through the focus on privacy, data protection, and self-determination of information. In order to find out the importance of privacy protection, the German deployment of the ACTIVAGE project [30] has been evaluated with 261 users, where the system evaluation is according to the importance of the system properties for the users, such as (1) privacy, (2) IT protection, (3) inconspicuousness, (4) maintainability, (5) costs, (6) interoperability, (7) reusability, (8) expandability and (9) accuracy [31]. It intended to find the importance of different quality characteristics the system has on the one side (in blue) and how the system has solved these characteristics (in orange) (see Fig. 8).

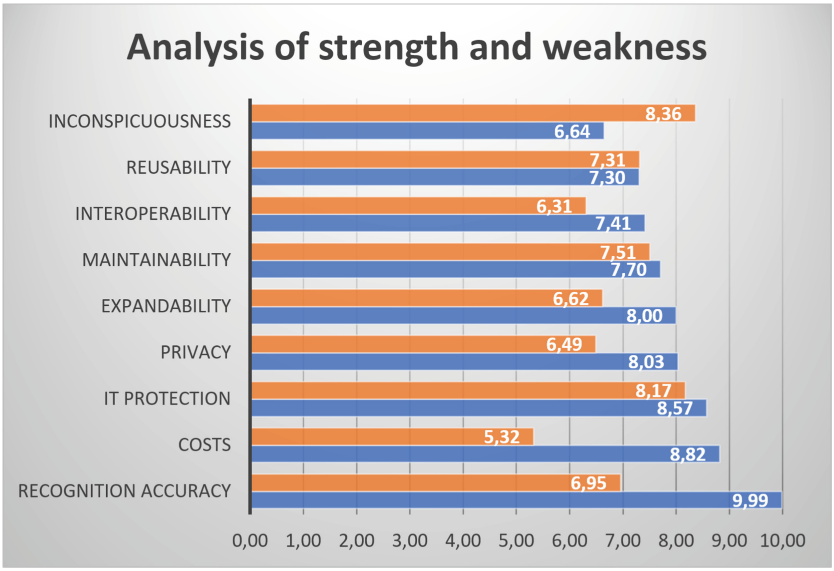

Fig. 8. Analysis of strengths and weaknesses of the ACTIVAGE project. (Color figure online)

This evaluation results showed that users consider a specific situation as the most important quality (9.99 out of 10). However, data protection and IT security (8.53/8.03) were observed as almost synonymous with the costs of the system (8.82). Therefore, these properties must be given special focus when implementing the system. This evaluation also showed that special priorities for further development had to be centered on privacy, security, costs, and accuracy. A reimplementation of the system by taking these four points into account had very positive effects for the acceptance due to the strict compliance with privacy by exclusively analysing data on the local controller, so that by the end of the project, the rejection rate of users in the apartments had been decreased from 11,7% to 5.3% [32]. Especially the younger residents with a higher technical understanding have very positive attitude towards such systems (0% rejection rate at the age of younger than 70).

The current technology stack and concept is evaluated based on reported requirements (see Table 1) of this paper.

Table 1. Fulfilled requirements regarding the here described technology stack.

Requirement	Fulfilled	Comment
GDPR-ready	Yes	Possible due to context-sensitivity (user-room-mapping at runtime)
Extendable	Yes	Service-based architecture offered by Gaia-X
Semantic layer	Yes	WoT-based approach to add semantic information
Transparency	Yes	Service-to-service logging mechanism in combination with user dashboard
Runtime checks and permissions	Yes	Users can grant access to services at runtime
AI-service sharing	Yes	Sharing of common AI-driven services like object identification are possible
User-specific privacy	Yes	IoT-module with cloud-mirrored IAM strategies
Information security system	Yes	Adapted ISMS best practices from ISIS12 for non professional management by tenants
Data space connecting capabilities	Yes	Eclipse Dataspace Connector is used
Distance-related privacy	No	Concept of body space, house space, building space is still work in progress
Integrations of other domains	No	Mobility, energy, health connectors are in still under development

After the user survey and the technical analysis we further investigate if an already running data acquisition project can benefit from this approach. The project DeinHaus 4.0 [33] focuses on equipping 100 households with smart home sensors and medical devices to enable elderly people to live as long as possible in their own house or apartment. In general the data has two origins: First the smart home sensors that are connected via Z-Wave and transmit the data via MQTT from the home to a database for later analysis; second are medical devices that transmit the data to the Withings cloud application from where it is mirrored to our data storage.

Privacy and security considerations are very important, because DeinHaus 4.0 handles highly sensitive medical data. Thus, the ethics proposal of the project required a data protection impact assessment of multiple data sources. And again, the well established and easily adaptable architecture and designs like Gaia-X could make this less time-consuming. The approach in DeinHaus 4.0 was to pseudo-anonymized all data leaving the household [34].

Further, the processes of PbD of Gaia-X will reduce the error-prone organizational data protection first with a well-structured process and second with technical implementations like the logging mechanism. The standardized and decentralized backend architecture of Gaia-X will reduce the complexity to combine several data sources in a custom DeinHaus 4.0 app. The app has the goal of facilitating health competence by visualizing the gathered data and explaining the data in the corresponding videos. The explanation of the data might be included in openHAB. Summing up, several ideas of this approach can enrich the current DeinHaus 4.0 data handling procedures and add more flexibility and transparency.

6 Discussion

The analysis of the DeinHaus 4.0 project has shown that our approach is capable of creating beneficial effects for ongoing projects, because usually third-party clients can connect to Gaia-X-compatible data spaces and get in touch with people who explicitly want to share their data. Furthermore, it is possible to integrate specific parts of our approach for existing projects, for example, access existing AI-services or ask for interoperability and context-sensitivity to enrich a third party application.

The smart kitchen use case is suitable to demonstrate the successful implementation of the reported requirements, e.g. context sensitivity, Gaia-X-compatibility, and the user-centered development approach. It is an appropriate scenario to show specific properties of an advanced privacy and security system for the smart living domain.

The results of the survey show that privacy, security, and recognition accuracy are highly appreciated by the tenants. Therefore, context sensitivity and improved robustness will optimize recognition accuracy. Furthermore, our implementation efforts are focusing on the most important features due to the users' survey that will have positive effects on later system's acceptance. The latest interviews show that transparency regarding service-to-service communication is important for users and service developers and so the necessity for a transparency dashboard has been confirmed. The technological backbone needs to ensure that these service-to-service interactions are logged reliably.

Gaia-X compatible architectures are capable of meeting privacy and security-related requirements. Currently, the federated services are developed by the Gaia-X community. The quality and scope of these modules will determine the possibilities to use and extend these software components and therefore, there will be an impact regarding our necessary efforts to fulfill the mentioned requirements regarding the cloud backend, e.g., implementing our approach on a sovereign cloud stack. This approach creates a user-centric data ecosystem in which users have maximum control over how their data is used. Furthermore, Gaia-X is responsible for certifying suitable service providers and has very precise requirements for the infrastructure and software modules used, so that interoperability is largely guaranteed when changing providers.

7 Conclusion

In the context of the presented project, the approach for the presented cloud concept of Gaia-X and the model for privacy by design were exemplarily implemented. As shown, this demonstrator was evaluated by means of corresponding surveys and analyses, so that a derivation can be made for the following further developments and adaptations. The current approach will be further implemented and improved during the ForeSight, Team-X and other related projects. Simultaneously the possibility to adapt its strengths to other researching projects will be evaluated. Moreover we will analyse if and how our ideas can enrich live systems of the health, care and energy domain.

References

1. Bauer, J., et al.: ForeSight - platform approach for enabling AI-based services for smart living. In: Pagán, J., Mokhtari, M., Aloulou, H., Abdulrazak, B., Cabrera, M.F. (eds.) ICOST 2019. LNCS, vol. 11862, pp. 204–211. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-32785-9_19
2. IDC Worldwide: Quarterly Smart Home Device Tracker (2019). https://www.idc.com/getdoc.jsp?containerId=prUS44971219. Accessed 18 Feb 2020
3. MarketsandMarkets: Smart Home Market by Product (Lighting Control, Security & Access Control, HVAC, Entertainment, Smart Speaker, Home Healthcare, Smart Kitchen, Home Appliances, and Smart Furniture), Software & Services, and Region - Global Forecast to 2024 (2019). https://www.marketsandmarkets.com/Market-Reports/smart-homes-and-assisted-living-advanced-technologie-and-global-market-121.html. Accessed 18 Feb 2020
4. Bauer, J., et al.: ForeSight approach to improve privacy and security in the smart living domain. Curr. Dir. Biomed. Eng. **7**(2), 903–906 (2021). https://doi.org/10.1515/cdbme-2021-2230
5. European Parliament and Council: General Data Protection Regulation (GDPR). In: Schulz, M., Hennis-Plasschaert, J.A. (eds.) Official Journal European Union (OJ), L 119, pp. 1–88, Brussels (2016)
6. Moses, F., Kampmann, M., Struve, F., Wiesbeck, S.: Handbuch zur effizienten Gestaltung von Informationssicherheit für Kleine und Mittlere Organisationen (KMO). ISIS12. IT-Sicherheitscluster e.V., Regensburg (2020)

7. VdS Schadensverhütung GmbH: Informationssicherheitsmanagementsystem für kleine und mittlere Unternehmen (KMU). VdS 10000. Köln (2018)
8. UAG 'Standard-Datenschutzmodell' des AK Technik der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder: Das Standard-Datenschutzmodell, Version 2.0. In: Rost, M., Weichelt, R. (eds.) 98. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder. AK Technik der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder, Trier (2019)
9. Koch, M., Pawils, A., Weide, E.: Das Standard-Datenschutzmodell in der Telematikinfrastruktur. Datenschutz und Datensicherheit (DuD) **44**(2), 104–110 (2020). https://doi.org/10.1007/s11623-020-1232-1. ISSN 1614-0702
10. Bartels, K.U., Lawicki, T.: Guideline, State of the Art. IT Security Association Germany (TeleTrusT), Berlin (2021)
11. Kelber, U.: Datenschutz ist kein Hemmschuh für Innovationen. Gastbeitrag. In: Wettbewerb - Der Treiber für die Gigabit-Gesellschaft, VATM-Jahrbuch 2019, p. 76. Verband der Anbieter von Telekommunikations- und Mehrwertdiensten e.V. (VATM), Berlin (2019)
12. Thiel, C., Golle, D., Broy, M.: Privacy by Design als Win-win-Strategie für Wirtschaft und Verbraucher*innen. In: Höhne, N, Zimmer, K.B. (eds.) Digital Dialogue, Positionspapier. Zentrum Digitalisierung. Bayern, Garching (2019)
13. Pötzsch, S.: Privacy awareness: a means to solve the privacy paradox? In: Matyáš, V., Fischer-Hübner, S., Cvrček, D., Švenda, P. (eds.) Privacy and Identity 2008. IAICT, vol. 298, pp. 226–236. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-03315-5_17. ISBN 978-3-642-03314-8
14. Bauer, J., Hechtel, M., Konrad, C., et al.: ForeSight - AI-based smart living platform approach. Curr. Dir. Biomed. Eng. **6**(3), 384–387 (2020). https://doi.org/10.1515/cdbme-2020-3099
15. openHAB Homepage. openHAB Foundation e.V. https://www.openhab.org. Accessed 18 Feb 2022
16. openHAB: Concepts. openHAB Foundation e.V. https://www.openhab.org/docs/concepts/. Accessed 18 Feb 2022
17. universAAL IoT Homepage. Fraunhofer-Institut für Graphische Datenverarbeitung (IGD). https://www.universaal.info. Accessed 18 Feb 2022
18. Apple HomeKit Homepage. Apple Inc. https://developer.apple.com/homekit/. Accessed 18 Feb 2022
19. CSA Matter Homepage: The Foundation for Connected Things. Connectivity Standards Alliance. https://csa-iot.org/all-solutions/matter/. Accessed 18 Feb 2022
20. Bauer, J., et al.: ForeSight - an AI-driven smart living platform, approach to add access control to openHAB. In: Jmaiel, M., Mokhtari, M., Abdulrazak, B., Aloulou, H., Kallel, S. (eds.) ICOST 2020. LNCS, vol. 12157, pp. 432–440. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-51517-1_40
21. Open Source Business Alliance e.V.: About, Technological Vision. https://scs.community/about/. Accessed 18 Feb 2022
22. GXFS.eu.: Gaia-X Federation Services for Identity & Trust, Architecture Overview (GXFS IDM.AO). eco - Association of the Internet Industry (eco - Verband der Internetwirtschaft e.V.), p. 24. https://www.gxfs.eu/specifications/. Accessed 18 Feb 2022
23. GXFS.eu.: Gaia-X Federation Services (GXFS) Toolbox. eco - Association of the Internet Industry (eco - Verband der Internetwirtschaft e.V.). https://www.gxfs.eu/set-of-services/. Accessed 21 Feb 2022

24. GXFS.eu.: Gaia-X Federation Service for Sovereign Data Exchange, Data Exchange Logging Service, Software Requirements Specification (GXFS SDE.DELS SRS). eco - Association of the Internet Industry (eco - Verband der Internetwirtschaft e.V.), p. 7. https://www.gxfs.eu/specifications/. Accessed 18 Feb 2022
25. International Electrotechnical Commission (IEC). Active assisted living (AAL) reference architecture and architecture model - Part 1: Reference architecture. IEC 63240-1 (2020)
26. Assisted Home Solutions GmbH (AHS) Homepage. https://assistedhome.de. Accessed 18 Feb 2022
27. Forschungsvereinigung Elektrotechnik beim ZVEI e.V.: ForeSight - Plattform für kontextsensitive, intelligente und vorausschauende Smart Living Services. https://foresight-plattform.de. Accessed 18 Feb 2022
28. Nolin, J.M.: Data as oil, infrastructure or asset? Three metaphors of data as economic value. J. Inf. Commun. Ethics Soc. **18**(1), 28–43 (2020). https://doi.org/10.1108/JICES-04-2019-0044
29. Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen: Gewinnerskizzen des Gaia-X Förderwettbewerbs. https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Digitales/GAIAX/Gewinnerskizzen.pdf?-blob=publicationFile&v=6. Accessed 18 Feb 2022
30. European Commission, Horizont 2020: ACTivating InnoVative IoT smart living environments for AGEing well (ACTIVAGE). Community Research and Development Information Service (CORDIS). https://cordis.europa.eu/project/id/732679/de. Accessed 11 Feb 2022
31. Wichert, R., Tazari, S., Albrecht, A., Wichert, M.: The value of the user evaluation process in the European IoT large-scale pilot for smart living. In: Distributed, Ambient and Pervasive Interactions, 9th International Conference (DAPI), 23rd HCI International Conference (2021)
32. Wichert R., Albrecht A., Tazari S.: D9.6 DS7 WOQ final report. In: Work Package 9, LSP Deployment Sites Definition, Execution and Evaluation. Deliverable No. D9.6. ACTivating InnoVative IoT Smart Living Environments for AGEing Well (ACTIVAGE) (2020)
33. DeinHaus 4.0 - Länger Leben Zuhause Homepage. THD - Technische Hochschule Deggendorf. https://deinhaus4-0.de. Accessed 21 Feb 2022
34. Schiller, L., Wuehr, M., Poeschl, R., Dorner, W.: Concept for the large scale deployment of ambient assisted living systems. In: 2020 10th International Conference on Advanced Computer Information Technologies (ACIT), pp. 288–292 (2020). https://doi.org/10.1109/ACIT49673.2020.9208911