Privacy concerns in Ambient Assisted Living systems for home environments

MIKAEL SÖDERQVIST
Privacy concerns in Ambient Assisted Living systems for home environments

Mikael Söderqvist
mickeso@kth.se
Supervisor: Sonja Buchegger
Examiner: Jonas Beskow
2019-05-17
Privacy concerns in Ambient Assisted Living systems for home environments
Abstract

By 2060 it is estimated that 30% of the European population will be 60 years or older. An aging society will put a heavy strain on the healthcare system. To mitigate this strain and enable elderly to live autonomously in their homes the AAL program was formed. With healthcare and health monitoring systems operating in home environments questions regarding privacy and security should be among the top priorities. The aim with this systematic literature study is to identify common privacy concerns, analyze and map them to areas within the field of computer science. 1000 studies were reviewed and passed through a three step inclusion process. Leading to 30 included studies representing different research fields and user surveys.

Included studies were categorized regarding privacy concerns and ended up as 18 vague- and 12 strong concerns and 8 solutions. Most common privacy concern among users were the unspecified privacy concern which might be a hindrance for acceptance of AAL systems in home environments. Other significant findings include the need for further research in representing data flow for users, user consent gathering and privacy vs. usability trade-offs.
Sammanfattning


Contents

1. Introduction 1
   1.1. Research question 1

2. Background 2
   2.1. Smart homes 2
   2.2. Ambient Intelligence 2
   2.3. Ambient Assisted Living 2
   2.4. Wireless Sensor Networks 3
   2.5. Context Awareness 3
   2.6. Human Activity Recognition 3
   2.7. Privacy 4
      2.7.1. Privacy-Enhancing Technologies 5
      2.7.2. Privacy by Design 5
      2.7.3. General Data Protection Regulation 5
   2.8. Related work 6
   2.9. News value 7

3. Method 9
   3.1. Search terms 9
   3.2. Databases 9
   3.3. Study selection 9
   3.4. Stopping rule 10
   3.5. Hypotheses 10
   3.6. Evaluation 10

4. Literary review 11
   4.1. The papers 11
      4.1.1. User surveys 11
      4.1.2. Literature reviews 12
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1.3. Wireless sensor networks</td>
<td>14</td>
</tr>
<tr>
<td>4.1.4. Contextual awareness</td>
<td>15</td>
</tr>
<tr>
<td>4.1.5. Privacy enhancing technologies</td>
<td>16</td>
</tr>
<tr>
<td>4.1.6. Privacy-by-design</td>
<td>16</td>
</tr>
<tr>
<td>4.1.7. Other</td>
<td>17</td>
</tr>
<tr>
<td>5. Quantitative analysis</td>
<td>18</td>
</tr>
<tr>
<td>5.1. Overview</td>
<td>18</td>
</tr>
<tr>
<td>6. Qualitative analysis</td>
<td>21</td>
</tr>
<tr>
<td>6.1. Privacy - user concerns</td>
<td>21</td>
</tr>
<tr>
<td>6.2. Context awareness</td>
<td>22</td>
</tr>
<tr>
<td>6.3. GDPR compliance</td>
<td>24</td>
</tr>
<tr>
<td>6.4. Ethics</td>
<td>25</td>
</tr>
<tr>
<td>7. Conclusions</td>
<td>26</td>
</tr>
<tr>
<td>7.1. Evaluation</td>
<td>27</td>
</tr>
<tr>
<td>7.2. Identified open problems</td>
<td>28</td>
</tr>
<tr>
<td>7.3. Future work</td>
<td>29</td>
</tr>
<tr>
<td>A. Studies included in the literature review</td>
<td>30</td>
</tr>
</tbody>
</table>
1. Introduction

Internet of Things (IoT) can be seen as a new paradigm of Internet enabled physical devices, a paradigm with an unprecedented growth of connected devices and fast paced development of enabling technologies. [1] In a forecast from IHS the IoT market will grow from 15.4 billion devices in 2015 to 30.7 billion devices in 2020 and 75.4 billion in 2025 [2]. As the IoT more and more enters our everyday lives in the form of smart devices our homes are becoming Smart Homes. One field is autonomous home systems which augments the gathered environmental data in an effort to assist in everyday life.

Ambient Assisted Living (AAL) is a multi-disciplinary field aiming to use Information and Communication technologies, such as IoT, in personal health systems. AAL systems consists of medical sensors, wearable device, wireless networks, computers, cameras and software application for health monitoring. Such systems could help mitigate the strain on traditional health care given a growing population of elderly, as well as enabling elderly autonomous lives in their homes[3]. By 2050 over 21% of the worlds population will be 60 years or more [4], which motivates the continued development for AAL systems. However, by exposing such systems on the Internet there are security and privacy concerns that needs to be addressed.

1.1. Research question

Main goals with this thesis is to answer the following research questions (RQ):

- RQ1: What are the main privacy concerns in AAL?
- RQ2: Which trade-offs are being considered (eg., privacy v. usability, privacy v. accountability, privacy v. resource constraints)?
- RQ3: How can we contribute to a solution for a concrete, small subset of the concerns identified in RQ1, from a Computer Science perspective?
Privacy concerns in Ambient Assisted Living systems for home environments

2. Background

2.1. Smart homes

The term "Smart home" (SH) is often applied to home environments attached with smart devices, such as computers, sensors and networks. Giving the inhabitants ways to either control or interact with their environment. Use cases include surveillance, entertainments systems, observation of energy consumption among others [5, 6].

2.2. Ambient Intelligence

Ambient Intelligence (AmI) as a term was originated through a EU initiative in 2001. AmI is a developing technology that aims to enable our environments to be responsive and supportive to it’s occupants needs e.g. in home health, entertainment or heating [7, 8].

2.3. Ambient Assisted Living

The Ambient Assisted Living (AAL) Joint Programme programme was an European effort between 2008-2013 to support applied research on innovative ICT-enhanced technologies and services in the area of aging well [9]. The original programme ended in Spring 2013 and after a review period a new programme Active and Assisted Living Joint Programme (AAL JP) was announced as a continuation with the aim to tackle the ageing challenge. This supportive programme is set to run through 2014-2020.

Making use of technologies from IoT, AmI and SH, AAL systems aim to assist and enable the subjects with their daily lives through monitoring and guidance. One of the use cases is to enable elderly an independent life in their homes with the goal of a maintained quality of life. [9]

---

[1] the AmI challenge
2.4. **Wireless Sensor Networks**

Wireless sensor networks (WSN) are groups of autonomous actuators and sensors connected through a wireless infrastructure intended to gather and control a physical environment. A WSN co-operatively collects environmental information and passes it through the network to a main location for processing and/or sends a control command to an actuator. Devices in a WSN is often of low power and resource constrained, making use of communication protocols such as 6LowPAN, ZigBee, IEEE 802.15.4 [10].

Wireless Body Sensor Networks (WBSN) is when a sensor network is applied on a person, to monitor vital signs such as movement, heart-rate, blood sugar for example. These networks can be autonomous and with the use of actuators trigger an action given the data collected. WBSNs can also be connected to a third party e.g. a Medical Center who monitors the data and takes actions if needed [11].

2.5. **Context Awareness**

Context aware-systems takes environmental information as input, determines the context and performs an action according the context. If there is a change in context the performed action might differ. Contextual information is all measurable parameters such as location, time, heat, heart-rate and thereof derived information [12].

In AAL systems context awareness often means user-context; what context is the user in and what action is required?

2.6. **Human Activity Recognition**

A key component in AAL systems is Human Activity Recognition (HAR) responsible to recognize various activities of the subjects. Activities are induced from low-level sensor data or from aggregated data from multiple sensors
Privacy concerns in Ambient Assisted Living systems for home environments

[13]. By gathering activity data profiling is possible and can be used to detect pattern anomalies which could suggest sickness. Activity recognition can also be a tool to suggest activities to help keeping the subject staying active.

2.7. Privacy

Privacy is about being able to chose when information about oneself is shared with any given entity, whether it’s with corporates, nations or other persons. Privacy can be broken down into two categories; physical privacy (which concerns one’s physical space and solitude and informational privacy (concerns about identifiable informations about oneself) [14]. Informational privacy has considerable overlaps with computer security and is strongly connected to integrity [15]. Informational privacy can further be broken down into four categories [16].

- Anonymity: "ensures that a user may use a resource or service without disclosing the user’s identity."
- Pseudonymity: "ensures that a user may use a resource or service without disclosing its user identity, but can still be accountable for that use."
- Unlinkability: "ensures that a user may make multiple uses of resources or services without others being able to link these uses together."
- Unobservability: "ensures that a user may use a resource or service without others, especially third parties, being able to observe that the resource or service is being used."

As we connect ourselves more and more, we enable the collection, monitoring and storing of personal data. Which can lead to breaches in our right to privacy. In some cases a trade-off between privacy and utility might be needed for certain systems to be able to perform its tasks, e.g. using different
degrees of privacy filters in video recognition systems [17]. Trade-off between privacy and utility\(^2\) can be hard to measure and the question of when privacy can be reduced in favor of utility is hard to answer in a general way. In privacy preserving video systems image obfuscation techniques are used to protect a persons identity but the obfuscation is such that a persons activity and actions can still be identified [17].

2.7.1. Privacy-Enhancing Technologies

Privacy-Enhancing Technologies (PETs) are technologies aimed towards protecting the privacy of users, without losing functionality of the systems [18]. PETs include such technologies as encryption (e.g VPN, TLS) and identity hiding (e.g onion routing, automatic anonymization).

2.7.2. Privacy by Design

Privacy by Design can be seen as a development paradigm where privacy is a core element and not a feature or an add-on; taking privacy into account throughout the whole development processes [19].

2.7.3. General Data Protection Regulation

General Data Protection Regulation (GDPR) is an EU regulation intended to strengthen data- and privacy protection for the EU population. Key changes to be noted from the previous directive include [20]

- GDPR will now be applied to all businesses working within EU, not only those based within the EU.
- GDPR offers strengthen conditions for consent and terms of consent must be provided in an intelligible and easily accessible form. Consent must also be easily revocable.

\(^2\)allowing a system the information it needs to be useful
• Data minimization, during data processing only the data necessary to successfully achieve a given task is allowed to be used.

• Data collected for one purpose is not allowed to be repurposed without further consent.

• In accordance to GDPR data breaches at companies must now be communicated to affected customers within 72 hours from knowledge of the breach.

• GDPR gives data subjects (users) the right to know what data is being collected, for what purpose and gives the data subjects the right to obtain a digital copy of all collected personal data.

• For companies in breach of GDPR there will now be rather heavy fines (up to 4% of annual global turnover or €20 Million, whichever is greater).

GDPR defines terms such as Data concerning health, Genetic data and Biometric data and these types of data will be subject to a higher standard of protection than general personal data [21]. For processing on a large scale of the three mentioned data types GDPR will require "data protection impact assessments" (DPIAs) which is a risk assessment of the data processing [21]. GDPR will be activated and enforced from 25 May 2018 [20].

2.8. Related work

In the field of AAL concerns regarding privacy is reoccurring in some form in most AAL research. Handling and possibly transmitting sensitive data is a big part of any AAL system, without the data the system has no utility and can not make informed decisions. In many cases there is a need for trade-off between privacy and utility (i.e. the systems can not make an informed decision because of a lack in information) [22]. In some cases the offered service could be deemed so valuable that privacy considerations are less of an
issue (e.g. in emergency, life-or-death situations) and in other cases the value of the service is not worth losing privacy for. Safekeeping this information can be done through quite a few different approaches; in the design phase making decisions about how to keep data safe and not store more information than what is needed [19], using authentication, encryption and authorization that enables granting access to chosen users [23] this is often combined with privacy policies [24] and lastly by using contextual information and to make the system adapt the privacy settings and needs depending on situational-, environmental- and system-contexts [25, 12, 26]. It is however suggested that context aware systems can be lead to compromised privacy [27] e.g. by setting up context based access constraints one could possibly determine locations or other sensitive information based on given access. As electronic health services (e-health) gains more traction in efforts to decrease healthcare costs and providing faster processing to meet an aging population concerns and research regarding privacy and security in e-health becomes more important. Research surveys in areas related to AAL and privacy have been performed e.g. in IoT [28, 1, 29], traditional health care systems [30, 31], AmI [32, 33] and even in the field of AAL [3, 34]. In these surveys privacy and privacy concerns are often stated as barriers to reach user acceptance for healthcare systems in home environments. These surveys do however not combine both user and technical aspects to determine which privacy concerns are most common among users and map those to possible solutions. By doing a broad literature study in the field of AAL and privacy and by including user surveys regarding privacy in healthcare systems we mean to lessen this research gap.

2.9. News value

Initial research shows that in the multidisciplinary field of AAL concerns about privacy is often brought up, but without making claims of finding or suggesting solutions - merely voicing the concerns. By pinpointing a recurring
Privacy concerns in Ambient Assisted Living systems for home environments

privacy concern(s) and mapping it to solutions from the field of computer science/computer security we would add to the knowledge base of the field.
3. Method

Methodology used in this thesis was a systematic literary review with the purpose of identifying research regarding privacy concerns in AAL systems. By reviewing research we aimed to pinpoint common privacy concerns in AAL and map these towards solutions within the field of Computer Science. As straightforward mappings \textit{problem} $\leftrightarrow$ \textit{solution} were not identified the results were analyzed and discussed to give insights to what pieces are missing and where future research could be directed at.

3.1. Search terms

Literary review used a constrained, combined set of keywords gathered through a pre-study - Ambient Assisted Living and privacy.

3.2. Databases

The literary review was focused on material published from the last decade; 2007 up to 2017. Research resources was gathered through searches in the Google scholar digital database (\url{https://scholar.google.com/}).

3.3. Study selection

Inclusion process for studies consisted of (1) selection based on title; (2) selection based on abstract; and (3) selection based on paper content. Papers were also categories in respect to RQ1 in section 1.2 and the following three categories was used (1) vague privacy concern; (2) strong privacy concern; (3) prosed solution to concern. This three step process along with the categorization narrowed down the amount papers considered for inclusion to the thesis research base. The selection process was used in conjunction with optionally including papers brought up in cited-by functions at the used databases and related works sections from papers chosen in the initial three-step process.
3.4. Stopping rule

Before the review process a stopping rule were set in place; "if a clear pattern of precise privacy concerns is found, that would act as a stopping rule for the review and the continuation of this thesis project would then be concentrated towards finding possible solutions for that precise problem". The criteria for the stopping rule was not met during the review and the review continued until 1000 papers were researched.

3.5. Hypotheses

Hypotheses for this thesis project was the following:

1. There exists common privacy concerns within the field of AAL.

2. There exists straightforward mappings for these privacy concerns within the research field of computer science, that can be applied within the context of AAL.

3. There does not yet exist straightforward mappings to the concerns.

3.6. Evaluation

When the research found during the literary review has been gathered and analyzed, privacy concerns identified, proposed solutions discussed and future research suggestions based on this research is given we analyzed to which degree our research questions were answered.
4. Literary review

During the literature search 1000 papers were identified and reviewed in accordance to the inclusion criteria described in section 3.3. From the initial 1000 papers 144 were selected in the first selection round. Of those 144 studies 79 were selected in the second selection round and in the final selection round 29 papers of interest were identified and one paper was additionally added. The 30 selected studies all focused on AAL, privacy or both. During round two and three consideration were given to exclude studies that greatly overlapped, were older or were less referenced by others. Due to the subjectivity involved in privacy, user surveys on privacy in AAL-like systems were included to determine the level of user concerns in regard to privacy.

The stopping rule described in section 3.4 was not enforced as a pattern of specific privacy concerns was not found during the literature review.

4.1. The papers

This section presents the review papers categorized in field of main contribution.

4.1.1. User surveys

K. Spitalewsky et al. shows through their survey that one of the top research concerns are “definition of an acceptable level of data protection and data security” and that privacy challenges is well known in the medical informatics community and states that experience from that area could be applicable in an ICT and AAL context [35]. [36] finds that healthy persons in general (and women in particular) found data protection and privacy more relevant in an AAL system whereas ailing elderly had less privacy concerns. [37] finds that data protection and data misuse is less of a concern than having system components visible in their home environment. The survey notes
that security features such as emergency and burglary detection was valued higher than e.g. disease detection and living comfort features. Surveyed users have overall highest concerns towards combined behavior collection and emergency detection systems [37]. Sack et al. finds in their user survey that the participants had the highest concerns about privacy and pointed out the importance of feedback; which data is collected, stored and forwarded. Main take-away is that the users clearly wants to be in control of their data. The study also shows that the degree of technology knowledge is linked to the degree of concerns regarding privacy, participants with lower knowledge were more concerned about their privacy which could be explained by lack of control [38]. In [39] elderly were surveyed on a primarily non-health monitoring AAL system, but a system meant to aid the elderly in maintaining an active life through activity suggestions, match-making with other elderly with similar interests e.g. Among the main findings are prevalent privacy concerns and concerns about intrusiveness of the system.

4.1.2. Literature reviews

Carie et al. suggests that there is no single definition of privacy and privacy is sometimes seen as a human right whereas in some cases privacy is a commodity, exchanged for e.g. higher quality service. The authors further discuss the quantification of privacy, putting an estimated monetary value on privacy and trade-offs between utility and privacy [40].

Costa et al. investigates the legal aspects of AAL and privacy and states that for health systems there has to be a trade-off between the legal rights to privacy and the right to health care. A health care system will not be able to function without access to the appropriate user data. The authors draws a parallel to conventional health care where sensitive, personal information is shared with caregivers and where caregivers are subject to secrecy and respect for privacy [41]. Another interesting finding is that the desire to live
Privacy concerns in Ambient Assisted Living systems for home environments

independently in some cases was so strong that it superseded intrusiveness and privacy concerns [42]. In agreement with the mentioned studies M. Lopez et al. draws the conclusion that among the use cases of ambient systems health care is the field of application that has to have the highest level of data protection, because of the sensitive nature of information. M. Lopez et al. further states that health care systems must be able to identify the user and that transmissions must comply with confidentiality, integrity, availability of personal data [32, 33]. In [33] the authors also adds the concepts of six different privacy systems ranging from privacy oblivious systems (POS) to privacy shielding systems (PSS), where POS systems does not include any privacy considerations and PSS is a system able to prevent any privacy violations.

In the review by Joseph Bugeja et al. [43] privacy and security aspects in smart homes is investigated and four major fields of continued research is identified; (1) Identity management, (2) risk assessment, (3) information flow control and (4) security management. With devices and systems connected to the Internet the need of strong authentication and authorization of both users and third-parties is encouraged in 1, 2 and 3 is meant to empower users in making decisions about their privacy. In 4 it is noted that there is a shortage of privacy-by-design measures in development of smart home systems. A 2013 review on AAL draws similar conclusions; during the design of the system care should be given to privacy concerns (privacy-by-design) but also that the system should not rely on user’s effort, due to their cognitive, perceptual, or physical limitations. Furthermore it is noted the need for further research in privacy preserving technologies e.g. noninvasive user authentication methods [44].

In a IoT survey by Pawar and Ghumbre different IoT based healthcare services are reviewed and investigated in terms of security and privacy. Findings include recommendations about anonymization of data that is to be stored in the cloud and to use available PET [28]. In the literature review [34] it is found that privacy concerns along with usability and perceived usefulness is
major barriers for adoption of AAL technology.

Machine learning techniques is an integral part of AAL systems which enables the system to learn and adapt to different contexts. In [45] it is shown that machine learning research in AAL is mainly focused on a conceptual level and the authors requests more data-driven research in the field, using larger datasets or even continuous data streams from AAL systems.

### 4.1.3. Wireless sensor networks

Zubiete ED et al. describes WSNs to be an important part of AAL systems, enabling wireless sensors to capture vital information about a user and its ambient environment. In their review, including 126 papers on WSN they identify several challenges including a low rate of privacy- and security considerations in the review papers and that although the WSNs are carrying sensitive medical information. Furthermore they discuss that standard interfaces in WSNs would ease the use and development of such systems [46].

In [47] WBSN or Wireless Body area networks (WBANs) and their technology and fields of application are reviewed. Information gathered in such systems are very sensitive both security and privacy are important issues. Authors suggests the IEEE 802.15.6 standard to achieve efficient and secure communication [47].

Kamrul Islam et al. researched security and privacy aspects of WSNs and presents two major privacy categories “data-oriented” and “context-oriented”. In the former the focus is on the data gathered by the systems different sensors and the aim is to keep it safe from adversaries, usually through the means of encryption and authentication. In context-oriented privacy the sensitive information includes location, timings and communication patterns. Solutions include hiding data, sending fake traffic. Through their study they identify different attack vectors and common solutions, but leaves the general security in WSNs open to further research; much to the resources constrained nature
of WSN devices [48].

### 4.1.4. Contextual awareness

Forkan et al. [49] proposes an cloud-based context-aware middleware for AAL systems; a middleware that given input of environmental data, sensor data and medical history determines context and which action is most suitable given that context. The aim of their proposed system is that it should be general and with a large enough model space to be able to accommodate a wide range of different AAL systems and with the ability to determine a wide range of different contexts. Privacy and security aspects is however ignored and is left opened. Schaub et al. describes the difficulties in user control of privacy settings in ubiquitous computing and proposes an extension to contextual AAL systems with a privacy decision engine (PDE). In the dataflow the PDE is placed after the context decision module and determines a privacy policy to the given context, e.g. non-emergency situation in bathroom yields a state of higher privacy were shared sensor data is limited [50]. According to Padilla-Lopez et al. [51] the context must provide enough information in order to adapt privacy policies to the users preferences. They therefor suggests that the context should not only include user specific details but also information about the observer of the information, e.g. a relative could be given limited whereas a medical caregiver gets unrestricted access to the information given the context. Privacy vs. utility is also discussed and the importance of trade-off between the two, high privacy might lead to low or no utility rendering the system unable to perform its intended purpose. Finding the trade-off balance between privacy and utility is left as an open problem that’s according to the authors is not solved in state-of-the-art research. Md Sakib Nizam Khan suggests a privacy enhancement schema by using contextual changes to identify changes in device ownership [52].
4.1.5. Privacy enhancing technologies

He et al. [53] proposes an authentication protocol for AAL WBAN systems, using elliptic curve cryptography to lessen the strain on the resource constrained devices in the WBAN. The proposed systems consists of an AAL server, a WBAN controller and the user. They further show that the proposed protocol is attack resistant and efficient enough for constrained devices.

Massacci and Nguyen propose a role and purpose based access control systems for AAL. Access is based on roles and purposes, e.g. a role could be nurse but without a purpose access to sensitive data will be denied. If the role has an active purpose e.g. in an emergency access will be granted. By limiting authorization to be event driven (emergency, scheduled visit etc.) the authors aim to only have granted access to when they are needed and states "no purpose, no data" [54].

In [29] the authors investigate different security and privacy issues and solution in healthcare systems built upon IoT technologies, such as AAL. Among the findings in the field of privacy it is noted that users should have the right to know who owns their data, location privacy (keep location private), maximize data locality (keep data local) and privacy-by-design should be used during and before development.

4.1.6. Privacy-by-design

Henze et al. addresses privacy aspects regarding outsourcing of sensitive information to cloud services e.g. a backend server in an AAL system. As cloud services are typically not developed for one specific user the authors claims that it is infeasible to decide on all privacy aspects during development of the service as privacy-by-design suggests. They suggest that privacy choices should be left to the users, which can be achieved through privacy policy models to which the authors suggest Privacy Development Language (PDL). A model written in PDL enables a developer to greatly detail privacy configurations available
Privacy concerns in Ambient Assisted Living systems for home environments

to the user [55]. Another approach to privacy policies is found in [24] where the authors use the W3C standard P3P[^1] to express privacy configurations and is used as constraints while querying data. According to the authors this would offer a more fine-grained access control than typical access control lists (ACLs).

4.1.7. Other

In [56] the use of audio based channels of information is examined and with the use of machine learning techniques the authors show a small system able to recognize phrases and common activities. In the study it is suggested that only certain pre-determined phrases would lead to a response by the systems and this to protect the privacy of the user.

Rothenpieler et al. proposes an AAL system that incorporates a social network-like component, both so that caregivers can get to know the user and to enable user to user interaction. Giving the caregivers insight in the users daily life and background is meant to decrease depersonalization which is stated to be a strong concern regarding how caregivers deal with a users privacy [57].

In [58] an offline solution for temporary care data storage is proposed, using RFID tags as small writable databases. In the paper it is noted that a commonly available RFID tag can hold up to 83 logged care events with each event being up to 32 bytes.

Privacy preservation in behavior analyzing system is shown in [59] were infrared ceiling sensors are able to detect activities such as walking, reading, falling etc. from low level binary information. By using a mesh of binary sensors which in singular can not identify a subject but together is able to classify a range of normal activities the authors claim to have proposed a activity detecting system that at sensor level is privacy-preserving.

[^1]: [https://www.w3.org/P3P/](https://www.w3.org/P3P/)
Privacy concerns in Ambient Assisted Living systems for home environments

5. Quantitative analysis

The aim of this section is to quantify relevant information from the literary review and analyze if trends can be seen in the AAL and privacy research.

5.1. Overview

Studies excluded in the selection process met one of the following criteria

- Not about AAL nor privacy
- Low relevance to the research questions
- Study that greatly overlapped other already included study
- Less referenced by others
- Older study (search results were restricted to 2007 and onward)

In step 1 and 2 of the inclusion process there were tendencies of erring to inclusion rather then to discard and in step 3 a more restrictive stance to inclusion was used. In table 1 each step of the inclusion process is shown, how many included papers up to each round and if extra papers were added (through references e.g.). In round 3 four papers were added from references in included studies and in the final step one additional study was added and the total number of included studies ended at 30.

Table 1: Number of studies evaluated at each stage of selection process.

<table>
<thead>
<tr>
<th>Round</th>
<th>Papers</th>
<th>Added papers</th>
</tr>
</thead>
<tbody>
<tr>
<td>1: By title</td>
<td>1000</td>
<td>0</td>
</tr>
<tr>
<td>2: By abstract</td>
<td>144</td>
<td>0</td>
</tr>
<tr>
<td>3: By paper</td>
<td>79</td>
<td>4</td>
</tr>
<tr>
<td>Final: Selected papers</td>
<td>30</td>
<td>1</td>
</tr>
</tbody>
</table>
Privacy concerns in Ambient Assisted Living systems for home environments

Each of the included studies were categorized in accordance to section 3.3 and is shown in table 2. Notable is that all studies categorized as solution were also categorized as a strong concern. Among the papers categorized as vague a majority briefly mentions that privacy and security are top concerns in the field of AAL, but without going into more detail.

Table 2: Number of studies in each category

<table>
<thead>
<tr>
<th>Class</th>
<th>#</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vague</td>
<td>18</td>
<td>47</td>
</tr>
<tr>
<td>Strong</td>
<td>12</td>
<td>32</td>
</tr>
<tr>
<td>Solution</td>
<td>8</td>
<td>21</td>
</tr>
</tbody>
</table>

In table 3 the most reoccurring areas of privacy concerns are shown. As the reoccurring concerns were mostly found in the user surveys they are to be viewed as user concerns. Users want to be in control of their environment and be able to know who has access to the information gathered by the system and when. Unobtrusiveness of devices is another common concern as it might be perceived as shameful or stigmatized to have fully visible health monitoring devices in the home. Another claim is that using AAL systems can lead to depersonalization of the caretakers and that the depersonalization can lead to decreasing regard for privacy and even further that caregivers see privacy as a hindrance to get their job done [35].

Table 3: Reoccurring concerns found in studies categorized as vague

<table>
<thead>
<tr>
<th>Concern</th>
<th>#</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feedback on who receives information</td>
<td>4</td>
</tr>
<tr>
<td>User control of system</td>
<td>5</td>
</tr>
<tr>
<td>Unobtrusive devices</td>
<td>3</td>
</tr>
<tr>
<td>Depersonalization</td>
<td>2</td>
</tr>
</tbody>
</table>
Among the studies categorized as Strong concerns the area of privacy concern and area of solution is shown in table 4. Most commonly discussed area is Context awareness/context detection and this as a area of solution to privacy concerns.

Table 4: Distribution of concerns / solution areas found in studies categorized as strong

<table>
<thead>
<tr>
<th>Concern</th>
<th>#</th>
</tr>
</thead>
<tbody>
<tr>
<td>Context awareness</td>
<td>4</td>
</tr>
<tr>
<td>Privacy policies</td>
<td>2</td>
</tr>
<tr>
<td>Privacy in WSNs</td>
<td>1</td>
</tr>
<tr>
<td>Access control</td>
<td>2</td>
</tr>
<tr>
<td>Authentication</td>
<td>2</td>
</tr>
<tr>
<td>Hardware / low level sensors</td>
<td>1</td>
</tr>
</tbody>
</table>

In table 5 the distribution of origin (based on continent) of the included studies is shown. Europe is the most common contributing continent to the field of AAL. As AAL is an European effort to stimulate research and development it is likely the reason that the majority of both the included and discarded studies are from countries within the European Union. If search terms other than AAL or Ambient Assisted Living were used the distribution would likely be different.

Table 5: Number of studies from continent

<table>
<thead>
<tr>
<th>Continent</th>
<th>#</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Europe</td>
<td>25</td>
<td>83</td>
</tr>
<tr>
<td>Asia</td>
<td>2</td>
<td>7</td>
</tr>
<tr>
<td>Americas</td>
<td>3</td>
<td>10</td>
</tr>
</tbody>
</table>
6. Qualitative analysis

Identifying common privacy concerns in AAL systems through a literary review was one of the main goals with this thesis project. Another main goal was to address this found common concern either through a prototype implementation or through a literature based discussion. In this section a brief description of the common concerns will be given.

6.1. Privacy - user concerns

Number one concern found during the review was vague privacy concerns [35, 36, 37, 43, …]. Not specifying closer what the concern consists of makes it difficult to approach. From a user perspective it is often a case of not having any (or enough) knowledge about the technologies used in system and therefore not being in control. Enabling user to be in control of their privacy and their data is a recurring topic [43, 38, …] and is therefore suggested as a topic for future research. This is also in line with the legislations of GDPR, enabling user to make decisions about the usage of their identifiable data and give them the option to "opt-out". As GDPR will be activated and enforced in May 2018 it will effect how AAL systems can be developed and deployed. Much of the concerns found in the reviewed user surveys will be addressed with GDPR. There are however studies that claim that all form of user input or user interaction should be kept to a minimum or should not be an option at all in AAL systems, with the reasoning that the users might be suffering from diseases that warrants constant monitoring (eg. in the case of users with dementia [44]). When enabling users to make active decisions about privacy settings in AAL systems it is of importance to ensure that the users understand what they sign up on [57]. Configuring fine grained privacy policies [24] is therefore not a task for cognitively impaired users and the interface to make these configurations needs to be easy-to-use [39]. In table 3 in section 5 it can be seen that users ask for feedback on who receives information gathered by
the system. Visualization of information flow is therefore another suggested topic for future research. Furthermore it can be noted in table 3 that sensors and devices placed in homes should be unobtrusive and preferable not be seen this is also in-line with findings in [34].

By further researching the suggested topics the most common user concerns found in this work could be solved. This could in turn lead to a lesser amount of user hesitation and increased adaptation rate for AAL technology in home environments.

6.2. Context awareness

Most common topic among the studies categorized as strong was Context awareness (see table 4). The concerns that context aware systems tries to answer is that of privacy vs. utility, to keep privacy as high as possible given the current context. If the system finds that a certain context requires more detailed information to ensure utility, privacy related information could temporarily be accessible for data processing or transmitted to a healthcare center. Context aware devices and systems are common in AAL and the constant flow of data can be a privacy concern [27], it could even be used as a privacy preserving function [33]. Making use of contextual information and utilize the information in context aware systems to help preserve privacy is an interesting field with great overlap of AmI, AAL, machine learning and AI [50, 55, 51, 52].

By using contextual information privacy settings can be adjusted to what the current context dictates, e.g. in emergency situations privacy settings might be lessened as identification is necessary. Enabling the system to configure privacy settings regarding to context (and pre-determined policies) is one solution to privacy vs. utility problem, as the system can adhere to high privacy preserving when needed to and be intelligible when needed to. The reviewed studies does however draw conceptual prototypes and/or use rather small datasets when testing the system. Future research recommendation are there-
Privacy concerns in Ambient Assisted Living systems for home environments

for more realistic, fuller datasets, implemented prototypes able to showcase the technology in real-life situations preferable in home environments with multiple inhabitants.

In [52] a rather basic system context parameter is used to determine ownership change. Parameter used is the name of the network to which the device was connected (SSID) and up on detected change in SSID the system is set to interpret this as an ownership change and therefore keep the previous owners information safe or safely remove it from the device.

In the future work section of [52] authentication is one of the main suggestions that is needed to improve the work. In the prototype implementation user profiles are protected by plain passwords and encryption keys are derived from the password. This opens up for brute-force attacks. By implementing the proposed AAL authentication protocol given in [53] the work in [52] would be improved. The suggested authentication protocol is benchmarked to be able to run in resource constrained devices and fitting for an AAL system.

Closer to the main work of that paper is how to improve the context change detection, in the future work section it is suggested to involve all available sensor modalities to determine and detect contextual changes. Furthermore it is noted that for devices using other means of communication than Wi-Fi the proposed solution does not work. One thing that makes [52] stand out is that the leveraged context is device or system centric whereas in [50, 55, 51] it is user-centric. By incorporating the proposed ideas from the user-centric context studies into [52] the work could be improved. In the case of mobile devices territorial privacy mechanisms [50] might be incorporated to set up privacy boundaries which would outline the systems physical range of operation and beyond that a contextual change could be triggered.
6.3. GDPR compliance

By comparing the major privacy concerns found in this thesis with the regulations found in GDPR we aim to showcase the overlap and which concerns GDPR does not answer. It is however worth pointing out that GDPR does not offer any solutions, but requirements that software dealing with personal data needs adhere to. Technical solutions and implementations to achieve system compliance to GDPR are still open problems.

GDPR will be enforced from spring 2018 and the gathering, processing and storing of personal information in general and health-care data in particular will need to be in compliance to GDPR [20]. It is somewhat troublesome that the studies in this literature review did not take GDPR into account more as it will effect AAL-like systems greatly.

<table>
<thead>
<tr>
<th>Concern</th>
<th>GDPR counterpart</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data flow</td>
<td>GDPR empowers users with the right of knowing how their data is being used and forms of intelligible, easily understandable consent is mandatory.</td>
</tr>
<tr>
<td>Privacy vs utility</td>
<td>As GDPR draws up the field of were software needs to be in terms of privacy GDPR will outline how this can be done. But e.g. with the use of dynamic privacy settings and privacy policies it can be argued that they might not be easily understandable to give consent to.</td>
</tr>
<tr>
<td>General privacy concern</td>
<td>As GDPR is meant to empower user with the knowledge of when and how their data is being used and also give users the option to anytime revoke their consent. GDPR might help to with the acceptance of healthcare systems in home environments.</td>
</tr>
</tbody>
</table>
In section 7.2 more realistic and comprehensive datasets are suggested to be used in future research. As GDPR does not allow data to be repurposed and/or processed in other ways than what the users have consented to the use of real-life, realistic data in research can be affected. As GDPR is not yet active and no precedent is set in regard to GDPR it is yet not establish at to what extent datasets for research will be affected.

6.4. Ethics

In the surveyed literature there are rather few ethical analyses and discussions. As AAL systems can have the power to impact both a persons health and privacy ethical considerations should be an integral part of the research. Discussions about what the impact would be if there is breaches in these kinds of systems should be more frequent as the information managed could be very privacy compromising.

Mentionings of ethical aspects found in this thesis is limited but it is mentioned that AAL should not replace human contact. Even though AAL systems are meant to enable elderly and disabled to autonomously live in their homes longer, it might be preferable to not only rely on the AAL system but to incorporate it with more traditional home visits from caregivers. Loneliness amongst elderly is briefly mentioned and a social network aspect incorporated in the AAL system is proposed [57]. This is however mainly directed towards a caregiving center and not towards elderly living independently in their own homes. Alongside the value in offering services that enables autonomous living the users still need human contact and perhaps AAL systems could be a social tool as well?

Even if it is mentioned in the literature that AAL systems should not replace human contact they possibly could in the future. This could lead to a decline in employment rate in the fields of home nursing and caregiving, rendering people unemployed.
7. Conclusions

AAL is a broad multidisciplinary research field which can benefit from multiple computer science disciplines such as privacy, security, machine learning / AI and networking. This study has shown that even though the research in AAL is plentiful much of it is conceptual work rather than data driven and experimental, and the ones using datasets often use small, single case datasets which do not portrait real life scenarios. Among the main findings of this study is the need to find rigid solutions to ensure privacy in AAL systems, as privacy concerns is one of the reoccurring user concerns which might hinder the acceptance of AAL systems in home environments. Because of an aging population with an outlook of over 21% of the worlds population being 60 years of older by 2050 the acceptance and development of autonomous healthcare systems in home environments is needed to help mitigate the increased strain this will have on the traditional healthcare system. For contextual aware AAL systems in the context of activity- and behavior recognition there are promising solutions which tries to approach the privacy vs. utility trade-off. By allowing the system to reconfigure privacy settings dependent on current contextual situation the system and care-givers can at times of need be given full access in favor of utility and in other cases privacy is is kept to a maximum. Incorporation privacy policies and allowing the system to autonomously switch between seems from this research like a promising paradigm for AAL-like systems. GDPR will empower users and at least partly answer some of the identified concerns (see section 6.3) e.g. user consent in an understandable way, consent revocation, data minimization and disallowing data repurposing. It is clear that GDPR will have a user privacy enhancing effect but to what extent is still not totally known until precededential rulings have fallen.
7.1. Evaluation

In this thesis the aim was to approach the research questions in section 1.1. In table 7 an evaluation to if the research questions were answered can be seen and in table 8 the general mapping from concern to research field can be seen. As a whole the general goals of this thesis work have been reached.

Table 7: Evaluation of how the research questions were answered in relation to hypotheses.

<table>
<thead>
<tr>
<th>Achieved</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>RQ1 X</td>
<td>Through a broad literature study privacy concerns in AAL was identified. Main findings is that users are in general concerned about their privacy and contextual systems that can reconfigure the trade-off between privacy and utility are most common.</td>
</tr>
<tr>
<td>RQ2 -</td>
<td>The literature study did not answer this question in a satisfactory way as the topic was not covered in the literature. Privacy vs. utility trade-off is common in image/video and audio based systems.</td>
</tr>
<tr>
<td>RQ3 X</td>
<td>Contribution offered is mainly in the form of conclusions drawn and mappings between privacy concerns and fields in computer science.</td>
</tr>
</tbody>
</table>

Identifying common privacy concerns was one of the aims with this thesis. Another part was to identify mappings to the research fields of computer science. In table 8 privacy concerns and respective research field mappings are shown, in these fields solutions might be present or is subject to future research and development. In section 7.2 areas of suggested future work are presented.
Table 8: Privacy concerns and their mappings in CS

<table>
<thead>
<tr>
<th>Concern</th>
<th>Research field</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data flow, what happens to ones data</td>
<td>Transparency enhancing tools (TET)</td>
</tr>
<tr>
<td>Privacy vs utility (context)</td>
<td>Machine Learning, AI</td>
</tr>
<tr>
<td>Configuration, consent, given cognitive</td>
<td>HCI</td>
</tr>
<tr>
<td>challenges</td>
<td></td>
</tr>
<tr>
<td>Unobtrusive sensors</td>
<td>HCI/design</td>
</tr>
<tr>
<td>Research on user control, liability,</td>
<td>Multidisciplinary (HCI, medical, legal)</td>
</tr>
<tr>
<td>emergencies</td>
<td></td>
</tr>
<tr>
<td>Depersonalization</td>
<td>Multidisciplinary (HCI, psychology and social science)</td>
</tr>
</tbody>
</table>

7.2. Identified open problems

- Data flow feedback for users
  - Users want to be able to see who has access to their data and system. Research in the field of HCI regarding how to present this information in an useful way is needed, especially considering AAL systems often are headless.

- User control of privacy settings
  - Users are concerned about their privacy in AAL systems and want to be able to control privacy settings in the system. How this should be done effectively in a system directed towards elderly, disabled and/or cognitively impaired needs more research. As AAL systems are often headless in nature this needs to be incorporated in future works.

- Privacy trade-offs
  - As the literature in this study did not cover when and if privacy
Privacy concerns in Ambient Assisted Living systems for home environments

trade-offs should be considered it is suggested as an open problem and also as a future work to direct further literature study towards. Should privacy in an AAL system be lowered in the case of an emergency e.g?

- Categorize, concretise and define privacy trade-offs

• Context awareness
  - Implemented context aware systems deployed/researched in real-life home environments.
  - Larger realistic data-sets, preferable with multiple users.

7.3. Future work

During this work a few suggestions for improvement for future research have been identified.

• Establish clear grading criteria of relevance and usefulness of studies. E.g. a grade from 1-5.

• Second opinion on grading of included studies to reduce subjectivity in the inclusion process.

• Adding more keywords in the literature search, as AAL is an European effort most of the studies found were from the EU. Adding terms such as “Smart homes”, “Telecare” and similar should extend to research outside of the EU.

• Further research privacy vs. utility and privacy vs. information. Which trade offs can and should be done and when?
### A. Studies included in the literature review

<table>
<thead>
<tr>
<th>Title</th>
<th>Paper</th>
<th>Classification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A survey on ambient-assisted living tools for older adults</td>
<td>[44]</td>
<td>Weak</td>
</tr>
<tr>
<td>Authentication protocol for an ambient assisted living system</td>
<td>[53]</td>
<td>Strong, Solution</td>
</tr>
<tr>
<td>CoCaMAAL: A cloud-oriented context-aware middleware in ambient assisted living</td>
<td>[49]</td>
<td>Weak</td>
</tr>
<tr>
<td>Security and Privacy Considerations for Wireless Sensor Networks in Smart Home Environments</td>
<td>[60]</td>
<td>Strong</td>
</tr>
<tr>
<td>On Privacy and Security Challenges in Smart Connected Homes</td>
<td>[43]</td>
<td>Strong</td>
</tr>
<tr>
<td>A survey on IoT applications, security challenges and counter measures</td>
<td>[28]</td>
<td>Weak</td>
</tr>
<tr>
<td>Generating privacy constraints for assistive environments</td>
<td>[24]</td>
<td>Strong, (semi) Solution</td>
</tr>
<tr>
<td>Understanding the User’s Acceptance of a Sensor-Based Ambient Assisted Living Application</td>
<td>[39]</td>
<td>Weak</td>
</tr>
<tr>
<td>A survey of Ambient Assisted Living systems: challenges and opportunities</td>
<td>[45]</td>
<td>Weak</td>
</tr>
<tr>
<td>Privacy Challenges in Ambient Intelligence Systems</td>
<td>[40]</td>
<td>Strong</td>
</tr>
</tbody>
</table>

Continued on next page
<table>
<thead>
<tr>
<th>Title</th>
<th>Paper</th>
<th>Classification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Goal-Oriented Access Control Model for Ambient Assisted Living</td>
<td>[54]</td>
<td>Strong, Solution</td>
</tr>
<tr>
<td>Privacy Classification for Ambient Intelligence [33]</td>
<td></td>
<td>Weak</td>
</tr>
<tr>
<td>Wireless Body Area Networks: Applications and Technologies</td>
<td>[47]</td>
<td>Weak</td>
</tr>
<tr>
<td>Ambient Intelligence: Applications and Privacy [32]</td>
<td></td>
<td>Weak</td>
</tr>
<tr>
<td>Ambient Intelligence from Senior Citizens’ Perspectives: Understanding Privacy Concerns, Technology...</td>
<td>[37]</td>
<td>Weak</td>
</tr>
<tr>
<td>Visual Privacy by Context: A Level-Based Visualisation Scheme</td>
<td>[51]</td>
<td>Strong, (semi) Solution</td>
</tr>
<tr>
<td>Privacy-Preserved Behavior Analysis and Fall Detection by an Infrared Ceiling Sensor Network</td>
<td>[59]</td>
<td>Strong, Solution</td>
</tr>
<tr>
<td>A comprehensive approach to privacy in the cloud-based Internet of Things</td>
<td>[55]</td>
<td>Strong, Solution</td>
</tr>
<tr>
<td>An Extended View on Benefits and Barriers of Ambient Assisted Living Solutions</td>
<td>[34]</td>
<td>Weak</td>
</tr>
<tr>
<td>Privacy and data security in E-health: Requirements from the user’s perspective</td>
<td>[36]</td>
<td>Weak</td>
</tr>
</tbody>
</table>

Continued on next page
Privacy concerns in Ambient Assisted Living systems for home environments

<table>
<thead>
<tr>
<th>Title</th>
<th>Paper</th>
<th>Classification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy Concerns in a Remote Monitoring and Social Networking Platform for Assisted Living</td>
<td>[57]</td>
<td>Weak</td>
</tr>
<tr>
<td>Potential and requirements of IT for ambient assisted living technologies</td>
<td>[35]</td>
<td>Weak</td>
</tr>
<tr>
<td>Review of wireless sensors networks in health applications</td>
<td>[46]</td>
<td>Weak</td>
</tr>
<tr>
<td>Challenges in the processing of audio channels for Ambient Assisted Living</td>
<td>[56]</td>
<td>Weak</td>
</tr>
<tr>
<td>An Ambient Assisted Living Platform Integrating RFID Data-on-Tag Care Annotations and Twitter</td>
<td>[58]</td>
<td>Weak</td>
</tr>
</tbody>
</table>
Privacy concerns in Ambient Assisted Living systems for home environments

References


Privacy concerns in Ambient Assisted Living systems for home environments


34
Privacy concerns in Ambient Assisted Living systems for home environments


Privacy concerns in Ambient Assisted Living systems for home environments


Privacy concerns in Ambient Assisted Living systems for home environments


Privacy concerns in Ambient Assisted Living systems for home environments

DOI: 10.1007/978-3.


Privacy concerns in Ambient Assisted Living systems for home environments


[40] Patrice Caire, Assaad Moawad, Vasilis Efthymiou, Antonis Bikakis, and Yves Le Traon. “Privacy challenges in Ambient Intelligence systems”. In: Journal of Ambient Intelligence and Smart Environments 8.6 (2016), pp. 619–644.


Privacy concerns in Ambient Assisted Living systems for home environments


Privacy concerns in Ambient Assisted Living systems for home environments


