Journal of Smart Cities and Society 2 (2023) 99–121
DOI 10.3233/SCS-230015
IOS Press

Security and privacy concerns in assisted living environments

Paulo A. Condado [a,*] and Fernando G. Lobo [b]

[a] *CENSE – Center for Environmental and Sustainability Research & CHANGE – Global Change and Sustainability Institute, NOVA School of Science and Technology, NOVA University Lisbon, Campus de Caparica, 2829-516 Caparica, Portugal*
E-mail: pcondado@gmail.com

[b] *CENSE – Center for Environmental and Sustainability Research & CHANGE – Global Change and Sustainability Institute, Departamento de Engenharia Electrónica e Informática, Faculdade de Ciências e Tecnologia, Universidade do Algarve, Campus de Gambelas, 8005-139 Faro, Portugal*
E-mail: fernando.lobo@gmail.com

Received 29 June 2023
Accepted 4 August 2023

Abstract. Assisted living environments use interconnected devices to assist people with limitations in performing daily activities. In these environments, human activity recognition is critical for detecting abnormal situations, such as falls or health problems, and providing appropriate assistance to inhabitants. Despite their advantages, assisted living environments raise security and privacy concerns due to the collection and storage of sensitive data about their inhabitants.

This paper addresses security and privacy concerns related to intelligent environments designed to assist individuals with limitations. It discusses the weaknesses of IoT devices and domotic technologies and presents research conducted by authors to mitigate these issues. This study shows that, despite hardware constraints, it is possible to design a relatively secure assisted living environment that prevents hacker attacks and data leaks. Additionally, it is essential to comprehend which information should be shared with external entities, such as health care services, and when to share it to ensure the inhabitants' well-being.

Our main goal has been to gather knowledge to improve the privacy and data protection of technology-rich assisted living environments implemented to assist people with limitations and their family members in performing their daily tasks.

Keywords: Assisted living environments, security, privacy, data protection, assistive technologies, low cost solutions, intelligent environments, cerebral palsy, older adults

1. Introdution

People with physical, mental, or sensory limitations are often unable to perform their daily tasks. Fortunately, there are several assistive technologies that allow them to have a more independent life [1,4,17,18,26,29–31,33,59,61,65]. Some of these technologies have been used to enable people with limitations[1] to use intelligent envi-

*Corresponding author. E-mail: pcondado@gmail.com.

[1]The term *people with limitations* is used throughout this paper as an inclusive term that refers to individuals with disabilities, older adults, and those who are injured and unable to perform common tasks.

ronments, namely easy-to-use interaction methods [7,18,25,52], assistive robotic solutions [19,20], fall detection systems [23,32,50,51] and monitoring systems [6,12,35,48,58].

An intelligent environment refers to a home or workplace equipped with interconnected devices such as sensors, actuators, appliances, and other internet of things (IoT) devices, which users can access and control to perform daily activities. Systems for monitoring human activities are also used in assisted living environments [12,35] to detect abnormal situations, such as falls or health problems, and alert relatives or health care services [19]. Although assisted living environments can increase the quality of life for people with limitations, there are security and privacy concerns that should be taken into consideration.

Data security and data privacy are two different but related concepts that are often confused. Data security refers a set of measures to ensure the confidentiality, integrity and availability of data [11]. It is essential to prevent unauthorized access and data loss. Thus, only an authorized user should be able to access and control his/her assisted living environment. On the other hand, data privacy refers to the right of a person to protect his/her personal information. As referred by [14], it is not possible to guarantee data privacy without data security.

In assisted living environments, a huge quantity of sensitive information is collected by a large number of interconnected and heterogeneous devices. However, standard security solutions cannot be implemented in most of these devices due to their limited processing power and memory. As referred by [18] and [15], there are many communication protocols that have been used in assisted living environments, such as ZigBee, Z-Wave, Insteon, LoRa, KNX, among others. Due to non-standardization of communication protocols, it becomes a challenge to ensure a high level of security in technology-rich assisted living environments. Moreover, it is important to stress that each one of these devices collects data that, when taken individually, may not be considered personal data. However, when the data generated by different IoT devices is combined, it can create detailed profiles of inhabitants, leading to a severe invasion of privacy. For instance, the simple fact that a person's smartwatch tracks his/her daily exercise routine, including for example a one-hour walk on the public park every morning, may not be considered personal data. Nevertheless, if the smartwatch is connected to his/her intelligent environment and a breach on the security system reveals that his/her house is empty during the same one-hour period, it becomes a serious invasion of privacy and a potential security risk.

Several research studies have been conducted to improve the security of intelligent environments [13,27,36,37,56], such as smart homes or assisted living environments. [13] presented an interesting and extensive overview about the current solutions to ensure the security of heterogeneous smart environments and concluded that the intelligent environments have several vulnerabilities. They mention that it is important to have external entities, such as the network operators, to manage security in intelligent environments. Despite there being various mechanisms to guarantee the security and privacy of data stored on cloud providers [49,55], we argue that these services are untrusted.

It is a fact that big companies employ the most advanced techniques to ensure data protection and privacy. However, a pertinent question arises: Can these companies decrypt users' data? Basically, as described by [55], private data can be snooped on by a curious administrator. In other words, a secure system cannot ensure users' privacy.

As described in Section 2, the process of designing and implementing an intelligent environment should take into account mechanisms to guarantee the privacy and data protection of the inhabitants. However, in some cases, due to the limitations of certain inhabitants, it may be necessary to develop an environment that is able to determine which personal information should be shared with external entities and when it should be shared. It is a challenging task to implement a system that not only respects the privacy requirements of each inhabitant but also identifies situations where sharing data with external entities is necessary for the well-being of the inhabitants. Another challenge is to develop an assisted living environment that uses low-cost technologies widely available on the market, while ensuring that devices do not share data with their manufacturers. Once again, we argue that manufacturers are untrusted entities and should not receive any information regarding inhabitants' activities.

The remainder of this paper is organized as follows. In the next section, we provide a literature review of the different approaches proposed to ensure data security and privacy in smart environments. Section 3 presents our main insights regarding inhabitants' privacy and data protection in assisted living environments, based on various informal interviews, an online survey, and an analysis of the network traffic generated by low-cost IoT solutions. Finally, Section 4 concludes this paper by presenting a discussion of the technologies currently used to protect

inhabitants' privacy and raising questions that require further research to make assisted living environments more secure and affordable.

2. Previous work

Home automation systems, assistive robotic solutions and other advanced technologies have been used to implement technology-rich assisted living environments [18,20,31,32,52] enabling people with limitations to perform their daily activities. These environments allow inhabitants with limitations to control the physical world using appropriate user interfaces [7,18,25,59]. For instance, a person with cerebral palsy can use a mobile application or a brain-computer interface system to turn on/off lights, adjust air conditioner temperature, open/close doors, control media centers and other home appliances. Monitoring systems [12,35] are used to ensure the well-being of inhabitants, detecting falls [23,32,51] and health problems and alerting health care services.

Fall detection systems and monitoring systems are fundamental in technology-rich assisted living environments, but, as argued by [19], these technologies should respect the right of inhabitants preserve their privacy. For example, an assisted living environment should only alert health care service under special conditions in order to preserve inhabitants' privacy.

Since 1950, the European Council has created legislation to protect the rights to privacy and personal data. Article 8 of the European Convention on Human Rights, which took effect in 1953, ensures "*the right to respect for private and family life, home and correspondence*" [62]. In 1981, as also described by [62] and [22], the European Council adopted the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, known as Convention 108, that was the initial "*legally binding international instrument*" in data protection. Convention 108 has been modernized to deal with the new challenges arising from technological developments. Article 6 of Convention 108[2] establishes that health data falls into special categories of data. Thus, "*the processing of health data shall only be allowed where appropriate safeguards are enshrined by law, complementing those of*" Convention 108 and "*such safeguards shall guard against the risks that the processing of sensitive data may present for the interests, rights and fundamental freedoms of the data subject, notably a risk of discrimination*".

To increase the data protection and privacy, standardizing the legislation across all EU member states, the European Commission promulgated the Data Protection Directive 95/46/EC, which was subsequently replaced by the General Data Protection Regulation (GDPR)[3] [54]. It is important to stress that, as defined in the Article 3 of the GDPR, this regulation applies to any organization that collects and/or processes personal data from European citizens, regardless of whether the organization is located in the European Union (EU) or not [67]. Article 9 of the GDPR also establishes that health data falls into special categories of data, defining situations in which the processing of these categories shall be prohibited or not. As addressed in Section 3.2, the GDPR also has very strict regulations regarding to transfers of personal data to third countries or international organizations [41,44].

As described by [10], preserving the privacy of users is one of the nine key principles that an intelligent environment should aspire to have in order to empower people. The other eight principles are:

- "*to be intelligent to recognize a situation where it can help*"-
- "*to be sensible to recognize when it is allowed to offer help*".
- "*to deliver help according to the needs and preferences of those which is helping*".
- "*to achieve its goals without demanding from the user/s technical knowledge to benefit from its help*"-
- "*to prioritize safety of the user/s at all times*".
- "*to have autonomous behaviour*".
- "*to be able to operate without forcing changes on the look and feel of the environment or on the normal routines of the environment inhabitants*".
- "*to adhere to the principle that the user is in command and the computer obeys, and not viceversa*".

[2]The document is available at https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf (accessed on July 28, 2023).

[3]The General Data Protection Regulation is available at https://gdpr-info.eu/.

These principles are essential to design technology-rich assisted living environments, as they are used to create systems that empower both people with limitations and their family members to accomplish their daily activities. Using similar principles, [19] have developed intelligent environments and assistive robotic solutions to empower individuals with limitations in performing their daily tasks. They advocate that data collected with respect users' daily activities within their living environment should be stored on local servers to protect their privacy.

[42] proposed an interesting ethical framework, which extended many elements of previous approaches into the engineering process, in order to address ethical issues. It was based on a manisfesto, entitled "*Intelligent Environments: a manifesto*", proposed by [10], with a special emphasis on the principles that systems must be designed to provide help according to the needs and preferences of the users, safeguard the users' privacy, ensure that the safety of the users is prioritized at all times, and, last but not least, guarantee that "*the user is in control and the computer obeys, not vice versa*". We agree with these authors that an intelligent environment, particularly an assisted living environment, should be developed to allow each user to adapt and use it according to his/her own needs, wishes and ambitions [18,19]. People with limitations have the desire to overcome or attenuate their limitations while preserving their dignity, autonomy, and independence.

As discussed in Section 4, the basic ethical principles presented by [42] should be taken into consideration during the development process of assisted living environments, as well as assistive robotic solutions and monitoring systems, to ensure that they are designed using a user-centered approach and are suitable for their inhabitants, providing privacy, data protection, security, autonomy, and transparency. These kind of systems should also be designed to prevent harm to the users and seek for opportunities to provide the appropriate assistance to users (Principles of Non-Maleficence and Beneficence). Intelligent environments should be aware of the needs, preferences and aspirations of all inhabitants in a multi-user environment. Another key ethical principle that should be taken into consideration is that a system should be accessible to all.

Privacy and data protection are especially important in the context of smart homes. After all, an intelligent environment collects a large amount of personal information and nobody wants to share their daily activities. As also refered by [19], there are many domotic technologies that rely on cloud computing [24,32,45,47]. However, despite being relatively inexpensive and user-friendly, as mentioned earlier, cloud-based services can be considered untrustworthy.

Many factors need to be addressed to guarantee the privacy of the inhabitants. Knowing that there is no privacy without data security, it is essential to ensure that assisted living environments satisfy the main security requirements, namely confidentiality, integrity, availability, authenticity, authorization and non-repudiation. Although most IoT devices have limited processing power and memory to use standard security solutions (e.g. smart bulbs, smart sockets, smart cameras, thermostats and a variety of sensors and actuators), some researchers have been working to increase the security of intelligent environments [13,37,56].

[13] stated that the heterogeneity of devices from different manufacturers, as well as protocols, contributes to an increase in security issues in intelligent environments. It is difficult to achieve a secure interconnection of devices provided by different manufacturers. We agree with these authors that nowadays data privacy is a very important topic in intelligent environments [13].

2.1. Data security in intelligent environments

Some authors proposed solutions to improve the security of smart homes [28,37,56]. [37] used reinforcement learning to develop an open-source smart home intrusion detection system (IDS), so-called MAGPIE – monitoring against cyberphysical threats, that "*is able to autonomously adjust the decision function of its underlying anomaly classification models to a smart home's changing conditions*".

Assuming that network operators should be responsible for managing security in intelligent environments [13], [28] proposed a distributed system that combines the home gateway IDS and the network operator's IDS to detect attacks against the intelligent environment. This approach attempts to solve one of the main issues with using IDS on most smart devices, which is their limited resources that make it difficult to detect new threats without a distributed architecture.

[57] used a Raspberry Pi to create a "*smart home gateway with secure applications and an energy-efficient encryption algorithm*", called Rasefiberry. It uses Snort as IDS, openHAB (open Home Automation Bus) as gateway

and some encryption algorithms for file encryption. However, this system does not provide Intrusion Protection System (IPS) to prevent denial-of-service (DoS) attacks.

Another IDS, so-called SENTINEL, was proposed by [21] and uses kernel-level system information of each IoT device connected to a network to detect attacks. This systems used various machine learning algorithms to "*distinguish benign and malicious device behavior*" and was shown to be a good solution for real-life IoT devices.

To address the dynamic behavior changes of attacks, [38] proposed using transfer learning to update deep learning-based IDS. This involves retraining pre-trained models on small datasets with new attack behaviors, which can then be leveraged to discover new types of attacks in IoT networks. [53] also proposed a similar framework for detecting both known and zero-day attacks.

IDS is one of the essential components to reach a secure assisted living environment. These systems add one more layers of protection by detecting different types of attacks in the network. After all, if an attacker gains access to a smart device, such as a surveillance camera or a thermostat, and retrieves sensitive data (e.g. usernames and passwords), she/he is able to gain access to other resources [28]. As described by [2], the insecurity of IoT devices poses a potential threat to the entire Internet. For example, there is a malware called Mirai that can infect IoT devices and turn them into a botnet. In October 2016, this botnet performed a massive distributed denial-of-service (DDoS) attack, which resulted in a widespread disruption of internet services.

[2] proposed a framework, called IoT-Sphere, that aims to improve the security of IoT devices with two layers of protection. The system defines a *sphere* of trusted addresses, allowing them to establish communication with a specific device. This first layer of security blocks all communications outside of the *sphere* of trusted addresses at the gateway level. However, as referred by authors [2], malicious communication may occur between a device and authorized addresses, which is why monitoring these communications is another layer of security to detect potential attacks or anomalies. Unlike other network security methods, such as IDS, [56] proposed an approach that uses specific permissions to block unauthorized network traffic rather than relying on a permissive approach and attempting to detect anomalous behavior. In other words, the goal is to enhance security in intelligent environments by limiting the communication capabilities of domotic devices without compromising their functionality.

[56] used a router/firewall as the main network component to improve the security in intelligent environments by blocking unauthorized network traffic. Likewise, [34] developed a firewall appliance for smart environments, called FANE, that can be configured with "generic security concepts". By monitoring the network traffic of IoT devices, this system is able to automatically learn and apply firewall rules. It is crucial to stress that many smart devices, such as security cameras, have well known vulnerabilities that can be exploited by attackers. We agree with [66] that firewalls are one of the most important tools for protecting networks against attackers.

Network segmentation is crucial for containing IoT devices and preventing the spread of potential threats. This involves blocking unnecessary data and redirecting potentially dangerous traffic. Thus, as mentioned by [66], one way to avoid information leaks is to implement the blocking of certain types of traffic at the firewall level and redirect them to a local server.

Another way to preserve data privacy is to use advanced encryption methods, such as the advanced encryption standard (AES) or public key cryptography (PKC). Unfortunately, due to hardware restrictions, most of the systems use lightweight symmetric cryptography algorithms (e.g. AES, Hummingbird, PRESENT, KLEIN, KATAN/KTANTAN, TEA, Curupira, DESL and Simon/Speck) [16].

2.2. Data privacy in assisted living environments

Ensuring data privacy in intelligent environments, such as smart homes or assisted living systems, is fundamental to protect the rights and dignity of their inhabitants. As advocated by [19], technology-rich environments must be implemented to respect the right of users to protect their privacy. Due to the amount of sensitive data collected by IoT devices, as well as by fall detection systems [23,32,50,51] and monitoring systems [6,12,35,48,58], a secure assisted living environment should be developed to avoid data leaks.

To ensure that sensitive data is not accessed by unauthorized users (e.g. curious administrators [40,55]), data collected about users' daily activities in their living environment should not be sent to external servers [19]. Sensitive information instead should reside on secure and private servers (a private cloud environment). As already proved by previous studies [18,19], it is possible to implement a private cloud infrastructure within an assisted living

environment using low-cost hardware, such as single board computers (e.g. Raspberry Pi, ZimaBoards, NVIDIA Jetson Nano, among others) or other small computers [19], and open source solutions [46].

Building a simple intelligent environment is relatively easy by integrating products from a variety of different companies such as Google, Amazon, Philips, Xiaomi, LG, Siemens, ABB, or Belkin. Most of these smart devices are compatible with smart speakers, also known as voice assistants, such as Google Home or Amazon Echo. A smart speaker is easy to use and serves as a home gateway, connecting to various home appliances. However, as described by [60], there are various situations in which certain smart speakers record private conversations without users consent.

As referred by [19], there are many assistive technologies, home appliances and fall detection systems [31] that use cloud based systems, such as Google Home and Amazon Echo, to do speech recognition, rising privacy concerns. Indeed, [60] proposed a system, called MicShield, that emits a jamming signal to protect private speech. Although the proposed system offers speech privacy protection against smart speakers, it has some limitations such as sensitivity of microphones and potential attacks on MicShield. As metioned by [60], their prototype supports wake word detection up to a range of 3 meters, but potential attackers may attempt to force other devices to emit inaudible words in order to bypass it.

It is relatively easy to build a simple smart environment using consumer products such as Philips HUE, Belkin Wemo, Wink, among others. However, creating a secure and user-friendly assisted living environment is a significant challenge. We argue that a smart environment can be implemented using low-cost technologies [19], but it is essential to have a profound knowledge about each product and its technologies. For instance, nowadays, nobody uses products based on X10 protocol, because it has an insecure protocol. Another example is products such as surveillance cameras and other IoT devices, which send sensitive data to manufacturers, allowing potential data breaches [66]. As mentioned in Section 2.1, a set of procedures should be implemented to prevent personal data leaks.

We advocate that it is essential to ensure that the inhabitants' privacy is protected. [9] conducted a study that demonstrated that even when IoT devices use encryption, any network observer can still analyze internet traffic to infer privacy-sensitive home-related activities. To mitigate this privacy issue, they analyzed several techniques (e.g. rate-shaping, blocking and tunneling) and concluded that traffic shaping can be an effective strategy to achieve it. They also concluded that, despite the common assumptions, implementing traffic shaping in smart homes can be done without compromising network performance or increasing data costs [9].

[5] also studied how passive network observers can use encrypted traffic from an intelligent environment to infer sensitive information. To achieve this, they proposed a novel multi-stage privacy attack. They concluded that an attacker can achieve an accuracy greater than 90% in inferring sensitive information. The effectiveness of these attacks raises serious privacy concerns. [5] also proposed a countermeasure based on generating spoofed traffic to mitigate privacy leaks. In other words, they presented a solution that generates false data packets at specific time intervals to deceive the attacker.

[63] developed a tool, called IoTMosaic, that generates signatures of diverse user activities from IoT network traffic. Their approximate matching algorithms and heuristic trimming strategy enable accurate inference of user activities from device event sequences, even when events are missing or out of order. Experimental results with thousands of user activities in a real-world smart home showed high levels of accuracy. [8] also proposed a new privacy attack that can be used by an out-of-network eavesdropper to identify various IoT devices and infer their working modes within 30 seconds. According to these studies, "*sensitive information leakage and privacy attacks constitute a genuine threat to intelligent environments*".

A technology-rich assisted living environment should be capable of recognizing each inhabitant, knowing their limitations, emotional state, medical history, and daily activities to assist them in their tasks. As a result, it should also be able to detect abnormal situations, such as falls and/or health problems, and alert health care services [19]. However, as described in [19], in order to preserve the privacy of the inhabitants, the system must have mechanisms to decide under what circumstances it should or should not emit alerts to health care services. This can be achieved through customizable settings that allow the inhabitants to set their own preferences for alerting health care services based on their individual needs and privacy concerns.

To the best of our knowledge, there is a privacy-related issue in intelligent environments that requires more research: When should information be shared with external entities and when should it remain private? The answer

to this question is indispensable to develop secure and technology-rich assisted living environments, allowing the algorithms to determine the appropriate actions to take without compromising the inhabitants' privacy. For instance, when the system detects a minor fall, it should be able to evaluate the severity and should only alert a family member without sharing any information with health care services. However, if a severe fall is detected, the system should be able to alert the health care services. In other words, the decision to share sensitive information with external entities should depend on (a) the severity of the situation and (b) the potential risks of not sharing the information.

Although a suitable intelligent environment should have mechanisms to allow each inhabitant to specify what kind of information they want to share with external entities, there are scenarios where it becomes complicated. For example, in case of a medical emergency, where the inhabitant is unable to provide an express consent, it may be necessary to disclose sensitive health information to health care services to provide appropriate care [43].

2.3. A summary of the literature

Intelligent environments, which combine different technologies, have been used to assist individuals with and without limitations in accomplishing their daily activities. Although many advances in this area have been made, with the development of alternative interaction methods [18,19,25,52,59] and monitoring systems [6,12,23,32,35,48,50,51,58], there are many challenges to overcome in developing a secure and safe assisted living environment. It is necessary to guarantee the privacy and data protection of the inhabitants in any intelligent environment to avoid disclosure or misuse of their sensitive information.

Unfortunately, although some researchers have proposed effective solutions to ensure the privacy [5,8,9,60,63] and data protection [2,21,28,34,37,38,53,56,57] of inhabitants and their guests, the heterogenity of devices and protocols presents a challenge for developing techniques to ensure privacy and data protection in intelligent environments [13]. Thus, further studies on privacy and data protection techniques are necessary to prevent the disclosure of sensitive information and protect the privacy of inhabitants. Additionally, implementing effective security mechanisms will ensure that intelligent environments are safe places to live, and inhabitants can trust that their personal information will remain confidential. Table 1 summarize the literature in this area, highlighting the advantages and disadvantages of the different proposals.

Overall, due to the heterogeneity of IoT devices as well as assistive technologies, it is not easy to design and implement a technology-rich assisted living environment that ensures privacy and data protection for its inhabitants. As observed in this brief literature review, some studies proposed solutions to enhance the security of intelligent environments, reducing their vulnerability to attacks and sensitive information leaks (see Table 1).

We believe that sensitive data should only be stored locally and that inhabitants should have the authority to decide which information is shared with external entities (e.g. health care services). In a technology-rich intelligent environment, it is crucial to incorporate best practices for privacy and data protection. Moreover, an assisted living environment should have the capability of identifying abnormal situations and notifying external entities, such as health care services, if the inhabitant is unconscious.

3. Meeting inhabitants' needs while ensuring privacy and data protection

The assisted living environment, originally described in [18], has been improved to provide its inhabitants with an exceptional user experience by integrating a wide range of innovative technologies that assist Paulo's family[4] with their daily tasks [19]. To achieve this, we followed established development and design principles in the field of HCI since 2013. Moreover, we have designed a multi-functional robotic solution that communicates with its environment to provide suitable assistance for its inhabitants. It adjusts environmental settings based on the emotional state of a given inhabitant and can alert health care services if it detects an abnormal situation (e.g. a fall or a health problem) [19].

We realized that a technology-rich intelligent environment, such as the one implemented to help Paulo and his family, deals with a vast amount of sensitive data, such as the activities of inhabitants, their preferences, emotional

[4]Paulo has cerebral palsy.

Table 1
Summary of privacy and data protection solutions

Proposed solution	Advantage	Disadvantage
Network operators should be responsible for controlling and maintaining the management layer of home automation networks [13,28].	Network operators can easily extend their services by controlling and maintaining the management layer of home automation networks [13], ensuring the data protection of their customers. Additionally, a distributed IDS [28], which combines the home gateway IDS with the network operator's IDS, aims to overcome limitations found in most smart devices and effectively detect attacks targeting smart homes.	External entities, such as public cloud services or network operators, are usually untrusted environments because a curious administrator [40,55] can eventually access sensitive information (see Section 2.2).
Intrusion detection systems for intelligent environments [21,28,37,38,53,57].	These systems are essential tools for securing IoT networks, also known as home automation networks [13], against different types of attacks. By detecting potential threats, it is possible to take proactive measures to minimize the risk of security incidents.	Detecting new threats is challenging due to the limited resources of most IoT devices. Fortunately, some researchers have proposed solutions that utilize artificial intelligence techniques to address this issue [21,37,38]. These systems do not primarily function as intrusion prevention systems to protect IoT devices from attacks.
IoT network security based on firewall and traffic monitoring mechanisms [2,34,56,66].	These systems are effective in protecting intelligent environments from unauthorized network traffic.	Configuring and maintaining these systems can be a challenge for less technologically savvy users.
Encryption methods [16].	These methods are crucial to ensure that all communications are encrypted and protected from hackers or other malicious agents.	Unfortunately, due to hardware restrictions, most of the systems use lightweight symmetric cryptography algorithms (e.g. AES, Hummingbird, PRESENT, KLEIN, KATAN/KTANTAN, TEA, Curupira, DESL and Simon/Speck).
Methods to prevent the inference of inhabitants' activities [5,8,9,63].	These methods generate false data packets at specific time intervals to mitigate the inference of inhabitants' activities by passive network observers [5].	The use of spoofed network traffic to mitigate the inference of inhabitants' activities may represent challenges in real scenarios, as many malicious agents employ spoofing attacks [3].

states and medical conditions. Thus, although his intelligent environment has been implemented using local services, we have also focused our research on understanding the privacy and data protection issues related to intelligent environments implemented to assist those who have limitations. Acquiring such knowledge is crucial for designing solutions that are both secure and appropriate for assisting people with limitations.

In our quest to acquire knowledge about issues related to privacy and data protection in intelligent environments, we conducted informal interviews to collect the opinions of a relatively small group of people. Additionally, we elaborated an online survey to gather a wider range of perspectives and insights. We also selected a small set of IoT devices, including surveillance cameras, to place inside a segmented network and analysed the traffic generated by them.

3.1. Towards privacy and data secure intelligent environments

Throughout the years we have been improving an assisted living environment, originally designed and implemented to assist Paulo and his family members in accomplishing their daily tasks. Lately we added features to increase the privacy and data protection of its inhabitants [18,19].

It is important to stress that the first implementation of this system, developed in 2013, used domotic devices based on the insecure and well-known X10 protocol. As previously described [18], we decided to use an inexpensive and widely used domotic technology because our primary goal was to propose a user-friendly interaction method that would enable Paulo and his wife to control their home appliances. However, as we used an iterative and user-centered approach to enhance their assisted living environment, we gradually updated the system to use more secure domotic protocols, namely Z-Wave and ZigBee.

Table 2
Characterization of individuals who participated in informal interviews, including their gender, education level, age and condition

Person	Gender	Education level	Age	Condition
Paulo	Male	Doctoral degree	43	Cerebral palsy
Wife	Female	High school	34	No limitations
Daughter	Female	Elementary school	10	No limitations
Friend #1	Female	Bachelor's degree	35	Cerebral palsy
Friend #2	Male	High school	42	No limitations
Friend #3	Female	Bachelor's degree	41	No limitations
Friend #4	Male	Bachelor's degree	53	Cerebral palsy
Friend #5	Female	Bachelor's degree	60	No limitations

Through the use of an iterative and non-traditional approach, in which we decided to implement and evaluate an assisted living environment in a real-life scenario rather than in a laboratory [18], we have constantly improved the proposed system to enable Paulo's family to perform their daily activities. We also evaluated novel assistive technologies, including a multi-functional robotic solution [19], in order to study how they can enrich intelligent environments. The collaboration with Paulo's family members, their friends, and the Portuguese Cerebral Palsy Association (APPC Faro) has been very important for the development and enhancement of the intelligent environment. Over time, we collected valuable knowledge regarding the design of intelligent environments for those with limitations through log files, usability tests, informal interviews and surveys.

To acquire knowledge about people's perceptions regarding privacy and data protection in assisted living environments, we initially conducted informal interviews with a small group of individuals (n = 8). Based on these interviews, we created an online survey that enabled us to collect more in-depth data and insights from a wider range of participants (n = 57).

3.1.1. Informal interviews

Four persons live at Paulo's home, namely Paulo, his wife, and their two children. Nevertheless, we were only able to obtain feedback from three inhabitants (Paulo, his wife, and their 10-year-old daughter) as their son was too young to participate in our study. We also gathered insights from five close friends of Paulo's family who frequently visit their home. Some of these friends also participated in previous studies [18,19]. In total, a small group of eight people, including individuals with cerebral palsy, shared their perceptions regarding privacy and data protection in intelligent environments. Table 2 shows the gender, education level, current age, and condition of each one of these persons.

Paulo's daughter grew up in the proposed assisted living environment and is familiar with using its various technologies, having been born the same year that it was implemented. As a result, she can effortlessly use IoT devices, robotic solutions, surveillance cameras, monitoring systems, and other assistive technologies, having been trained to use them while protecting her privacy.

With a good understanding of technology and its potential risks, Paulo and his wife revealed a growing concern regarding their privacy and data protection [19]. Over time, we have improved their assisted living environment to accomplish their preferences, needs, desires and limitations. In terms of privacy and data protection, Paulo's family demanded the following requirements:

- Use encryption methods to guarantee a secure communication between the application and home gateway.
- Replace all IoT devices based on unsecure communication protocols.
- Ensure that all services are self-hosted and that sensitive data is encrypted using the highest available standards.
- Implement the necessary measures to avoid, or at least minimize, any unsolicited communication between IoT devices and their manufacturers (e.g. segment the network and block traffic at firewall level).
- Avoid to use systems based on public cloud services (e.g. Alexa).

Note that Paulo's friends have become accustomed to his assisted living environment. In fact, some of them seem to enjoy observing our ideas (e.g. the development process of a robotic solution [19]). Nevertheless, during the initial phase of implementing this system, called *EasyHouse*, most of them expressed discomfort with certain features

that were implemented to ensure the well-being of Paulo and his family, namely surveillance cameras and motion sensors.[5] All of them agree that IoT devices and assistive technologies helped Paulo's family in accomplishing their daily tasks, facilitating his interaction with home appliances and other physical objects. However, since the initial stage of development of this system, they revealed that they are concerned about the potential security risks associated with these technologies. For instance, friend #5 asked if a smart lock system will be installed in Paulo's house and she expressed her fears regarding the reliability of such equipment. Such concerns regarding the reliability of some products are also shared by Paulo and his wife and they opted for a conventional lock system.

Like Paulo, two of his five friends – a female and a male – have cerebral palsy and mild coordination problems. Despite their physical limitations, Paulo and his friends have a high level of education, contribute to improving society with their work and use technological devices on a daily basis. They collaborated with us to design and improve the assisted living environment and other assistive technologies, testing the system and providing insights. As aforementioned, they also expressed concerns about potential hacker attacks and information leaks. In the early stages of developing the solution, Friend #1 asked Paulo and his wife how they were able to maintain their privacy with so many surveillance and monitoring systems.

In early 2020, Paulo and his wife met a couple – friend #2 and friend #3 – who also had children of similar ages, and the two couples developed a close friendship. Although they were not involved in the development process of Paulo's smart home, they indirectly used it as frequent visitors at Paulo's home. Being an employee of a large network operator, he is knowledgeable about significant privacy and data protection concerns, as the operator provides IoT solutions to other companies. He also helped us to improve the quality of Internet connection in terms of speed and reliability. Additionally, after several discussions with Paulo, friend #2 changed his opinion regarding cloud based services and now recognizes the benefits of self-hosted solutions.

Based on our knowledge about this small group and our previous research studies [18,19,30], over the last few months, in addition to designing and implementing novel interaction methods to enable Paulo and his family to have a more natural interaction with their environment, we conducted informal interviews to gain a better understanding of participants' concerns regarding the privacy and data protection risks of technologies used in intelligent environments.

Through these interviews, we concluded that all of the participants are well aware about the potential risks related to use of domotic technologies, including surveillance and monitoring systems.[6] They expressed concerns about potential hacker intrusions and information leaks related to the use of these technologies. Thus, although the proposed solution allows Paulo and his family members to turn on/off all systems, they suggested that we should design a mechanism that would allow both inhabitants and visitors to activate a temporary privacy mode, in which all sensitive technologies are deactivated.[7]

Some of Paulo's friends revealed that, before they became more familiar with his environment, they had no special concerns about IoT devices and monitoring systems based on public cloud services. Nevertheless, their perspective changed and they expressed serious concerns about the use of such systems. Friend #4 said that "*our personal data should not be shared with unknown people, since there is no guarantee that they respect our privacy*" and "*now, I understand Paulo's concerns about the risks related to systems based on public cloud services. I agree with him that self-hosted services are good and affordable alternatives*". Friend #2 also said that "*unfortunatelly, many technologies only work based on cloud services and, now, I realize that this is a real threat for privacy and data protection*". Friend #5 revealed that Paulo helped her to set up a small homelab, specifically created to enable her to perform backups from her business systems. She also disclosed that someone had offered her an Alexa, but she had avoided installing it due to privacy and data protection concerns.

Our group also showed serious concerns about privacy and data protection regarding IoT devices and their manufacturers, due to certain features that require unsolicited communication between each device and its manufacturer.

[5]The use of these technologies might have been seen as an intrusion into their privacy. Furthermore, Paulo's friends might have also been afraid that such devices could be misused or hacked.

[6]Please note that this group may not be a representative sample of the entire population due to their previous knowledge regardings certain risks related to use of IoT devices, acquired through their contact with Paulo's family.

[7]Such functionality would be integrated with our proposed robotic solution, allowing anyone to be able to control that mechanism.

Despite implementing segmentation and blocking traffic at the firewall-level to deny any unsolicited communication [2,34,56,66], the participants believed that there is no valid reason for a manufacturer to establish communication with devices installed in real assisted living environments. Paulo thinks that some manufacturers may claim that the communication feature is implemented to enable users to control their devices remotely using the provided applications. However, this argument is invalid because an intelligent environment can integrate technologies from various manufacturers. It is impractical to use a specific application to control each manufacturer's devices, as this creates potential security breaches. Moreover, Paulo argued that "*users need a unique and easy-to-use application that enables them to control all of their heterogeneous domotic technologies*".

We also made an effort to understand the perspective of our participants regarding a very important question: when and in which situations a system should share data with external entities (e.g. health care services)? All of them agreed that a technology-rich intelligent environment should have mechanisms to detect if an inhabitant is unconscious and, in such cases, request help by alerting external entities. Nevertheless, it is a very complex topic and an extensive research is needed because there are many ethical and moral aspects to address. Overall, an intelligent environment should always respect an inhabitant's privacy preferences, but it should also ensure that assistance is requested in case of detecting a serious fall or health problem.

These informal interviews provided us with an opportunity to learn about the participants' concerns regarding privacy and data protection in assisted living environments. These concerns are listed below:

- Sensitive information leaks.
- Unauthorized access.
- Untrusted IoT systems.[8]
- Physical security threats.
- Lack of solid policies to share sensitive data with external entities.

This group of people appear to be technologically savvy and well informed of the risks of exposing personal data. However, due to their deeper knowledge about domotic technologies and computer networks, we elaborated an online survey to obtain a wider perspective of the users' concerns regarding privacy and data protection in intelligent environments.

3.1.2. Online survey

Potential participants were informed about the main goals of this online survey, the way to contact the principal researcher, and the assurance of their privacy being ensured. Therefore, they could provide their informed consent or decline participation in this research study [39].

We elaborated an online questionnaire to gather people's perceptions of privacy and data protection in intelligent environments. The questionnaire was divided into four main sections, designed to help us (a) characterize the participants, (b) comprehend how individuals without disabilities perceive the challenges faced by those with limitations and how IoT devices can enhance their quality of life, (c) gain a deeper insight into the participants' knowledge of IoT devices and domotic technologies, and (d) understand all participants' perspectives on privacy and data protection in intelligent environments

A total of 57 persons, both with and without limitations, filled out our online questionnaire, with 37 females and 20 males. Of these, 13 persons reported having some sort of disability, while the remaining 44 did not.

As shown in Table 3, 36.8% of participants had a range of ages between 40 and 49 years old. Considering participants that had a range of ages between 30 and 39 years old (29.8%), we concluded that the large majority of participants (66.6%) in our survey were aged between 30 and 49 years old. 15.8% of participants had a range of ages between 50 and 59 years old, and 12.3% of participants were under the age of 30. Only 5.3% of participants were aged over 60 years old. Unfortunately, the number of older adults participating in our online survey was limited, despite their significance as a target group for our study.

Most participants have a higher education level, namely 42.1% of them have an undergraduate degree, 15.8% have a master degree and 3.5% have a doctoral degree. 33.3% of participants have the 12th grade, 3.5% have the

[8] All domotic technologies that may put inhabitants at risk of data leaks, unauthorized monitoring activities, privacy violations and physical security threats.

Table 3
Distribution of participants by age range

Age range	% of participants
Under 20	1.8
20–29	10.5
30–39	29.8
40–49	36.8
50–59	15.8
60–69	5.3
Over 70	0

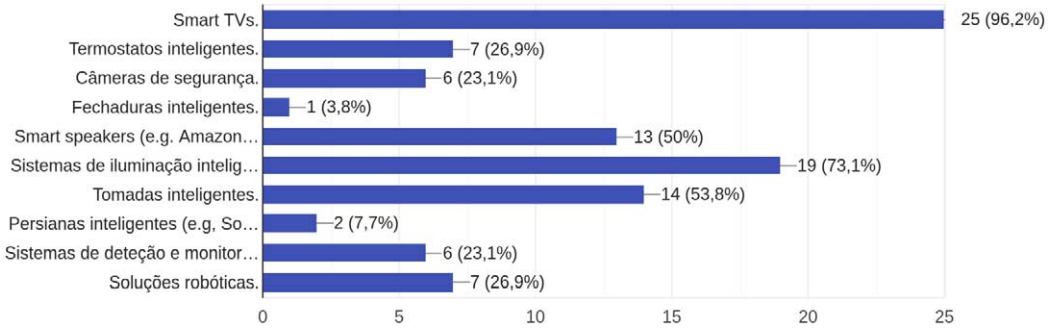

Fig. 1. The bar chart displays the responses in Portuguese to the question: "*Which IoT devices do you use?*"

9th grade and 1.8% of participants only have the 4th grade. Thus, we concluded that most people who answered our questionnaire are well instructed and have a strong general culture. Moreover, as the majority of participants were aged under 50 years old, they should have a reasonable familiarity with information and communication technologies, including their advantages and disadvantages.

An interesting observation is that 97.7% of the participants without disabilities reported that they knew someone with disabilities. All of them answered that IoT devices and/or domotic solutions can improve the quality of life of those who have limitations. 84.1% of them recognized that these technologies can have a major impact in promoting the autonomy of people with disabilities and/or older adults, while the rest of them believed that it can still have an impact, but not to the same degree. Such results are similar to the ones presented in a previous study [19], showing that overall people believe that the design and development of technology-rich assisted living environments contributes to improving the quality of life of people with limitations.

With the goal of understanding participants' perception about privacy and data protection in intelligent environments, we also tried to perceive their familiarity with IoT devices. Thus, we asked participants if they use these devices or domotic solutions. 54.4% of participants reported not using them, while 45.6% confirmed using them in their daily routine. From those who use these technologies, only 23.1% of them used an unique application to control their home appliances, sensors and actuators. A large part of them used different solutions to accomplish the same task, possibly one for each brand. The majority of them (76.9%) used IoT devices on their main network, but they failed to implement two essential measures to protect their equipment against attacks: Network segmentation and traffic control at the firewall-level. Overall, most people appear to have no concerns regarding their primary network security, ignoring threats such as Mirai [2].

Figure 1 shows the answers in Portuguese to the question: "*Which IoT devices do you use?*" Most used devices reported by participants were smart TVs (96.2%), followed by smart lighting solutions (73.1%), smart plugs (53.8%), smart speakers (50%), smart thermostats (26.9%), robotic solutions (26.9%), surveillance cameras (23.1%), detection and monitoring systems (23.1%), smart curtains (7.7%), and smart locks (3.8%).

The majority of participants (68.4%) answered that they believed that IoT devices were secure, providing privacy and data protection for their users. All participants were asked to classify, on a scale of 1 (none) to 4 (high), which is the level of privacy and data protection provided by these devices to their users. While most participants believed

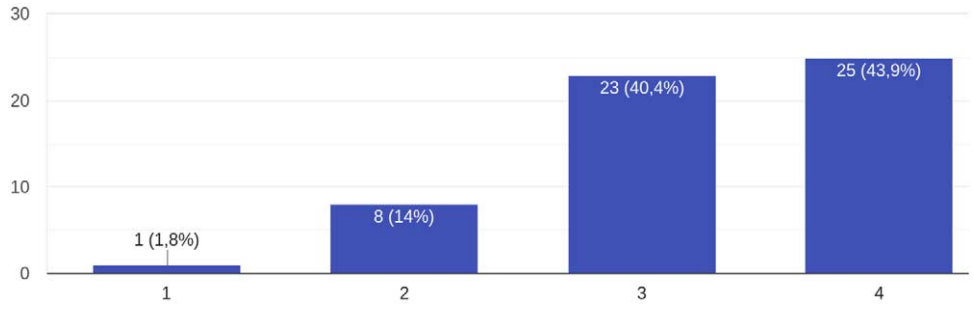

Fig. 2. The bar chart displays the responses in Portuguese to the question: "*On a scale of 1 to 4, how do you rate the sensitivity of the data collected, processed, and stored by these systems?*"

that these devices were secure, only 5.3% of them answered that the level of privacy and data protection provided by IoT devices was high. In fact, most of them (64.9%) selected 3 on the scale, with 22.8% and 7% choosing 2 and 1, respectively. The results showed that while people do not have complete confidence in the level of privacy and data protection offered by most of these products, they still want to trust that technologies are developed with these features in mind. This suggests that most users assume that any technology is implemented with privacy and data protection issues in mind. Moreover, since 59.6% of people answered that they did not read terms and conditions or privacy policies, it could be an alarming indication that users are not aware of many details about how their data is treated and stored by companies.

The participants also answered a set of five questions designed to understand their main concerns about privacy and data protection in relation to solutions based on public cloud services. First of all, when they were asked regarding their concerns about the fact that most IoT devices depend on cloud-based services to operate, the majority (40.4%) answered that they had not thought about it, while 36.8% and 22.8% answered yes and no, respectively. When asked to classify the level of privacy and data protection provided by solutions based on public cloud services on a scale of 1 (insecure) to 4 (very secure), the majority of participants (56.1%) selected 3 on the scale, while 29.8% chose 2, 12.3% selected 1 and only 1.8% chose 4. They were also asked to rate the measures implemented by the main cloud providers using some scale. Most participants selected 3 on the scale, while a percentage of 19.3% chose 2, 14% selected 4, and 5.3% chose 1. When participants were asked about the possibility of a curious administrator to have access to their personal data, 42.1% answered to be probable and 21.1% affirmed to be very probable. Moreover, a large majority of participants (71.9%) reported a preference for using local servers to store data related to their daily activities, rather than cloud-based services.

The answers above revealed that people want to trust cloud-based services. However, as expressed by our participants, they consider these services untrustworthy. The majority of participants believed that a system administrator could access their data. They also revealed a preference for using systems based on local services, or self-hosted services, over the ones based on public cloud services. Moreover, according to the survey results, 56.1% of participants reported trusting devices' brands, but only 5.3% claimed to have the highest level of trust in these companies. Additionally, 78.9% of participants emphasized the importance of privacy and data protection.

Almost all participants answered that they believed that the implementation of fall detection and monitoring systems improves the quality of life of inhabitants of intelligent environments, especially those with limitations. In fact, only 1.8% of survey respondents affirmed that they did not believe that the installation of these technologies improves the quality of life of inhabitants. 98.2% of participants indicated that these systems, as well as emotional recognition systems, should have mechanisms to ensure guests' privacy. When asked to classify the level of data sensitivity collected and processed by this kind of systems on a scale of 1 (little sensitive) to 4 (very sensitive), the majority of participants (43.9%) selected 4 on the scale, while 40.4% chose 3, 14% selected 2 and only 1.8% chose 1 (see Fig. 2).

An interesting observation is that the majority of participants, when asked about their level of confidence in external entities (e.g. health care services), reported that they had none or little confidence, while 42.1% of them admitted having confidence. Nonetheless, 70.2% of participants answered that if the intelligent environment detects

a user in a critical situation, it should be capable of overriding the user' settings and call for external assistance. In contrast, only 29.8% revealed that the system should respect users' preferences.

We concluded that people believe that IoT devices, as well as other monitoring systems and assistive technologies, can improve the quality of life of people, especially those with limitations. Although the majority of participants showed concerns regarding their privacy and data protection, this study suggests that they did not know about some risks associated with it. The results revealed that they tend to trust in brands and big technological companies. However, some of their fears were noticed and are listed below:

- Many participants expressed concern that communication between IoT devices and their manufacturers could be a violation of privacy.
- Although many participants hadn't thought about these devices depending on cloud-based services to operate, most expressed a desire to create an intelligent environment that runs on a local server.
- The majority of participants considered that it is possible for a system administrator to have access to their data.
- Only one participant revealed that they own a smart lock, which suggests that most participants don't trust these kinds of systems for their physical security.

Like Paulo's family and friends, many people have serious concerns about sensitive information leaks, unauthorized access, and physical security threats. However, unlike the first group, participants who are less technologically savvy may be more inclined to trust that companies will ensure their privacy and data protection.

The results showed that people use various IoT devices to improve their lives, automating many daily tasks and accessing a wide range of multimedia contents.

3.1.3. Discussion

According to the survey results, we conclude that people highly prioritize their privacy and data protection. They have concerns about sensitive data leaks and malicious attacks and prefer to store their information on local servers. Moreover, we also conclude that many individuals use consumer and inexpensive devices to build their intelligent environments. Unfortunately, they may not have the necessary knowledge to use open-source tools, such as Home Assistant,[9] to design secure and user-friendly environments. On the one hand, it is a positive sign that people are utilizing low-cost technologies to facilitate their daily activities, which aligns with our goal to develop secure and cost-effective assisted living environments [18,19]. On the other hand, it is concerning that many individuals appear to have a limited understanding of basic home automation systems.

People generally have little confidence in sharing sensitive data with external entities, such as health care services. However, they also defend that if an assisted living environment detects any emergency situation it should be able to alert these entities, having appropriate mechanisms to overcome users' preferences in extreme cases (e.g. when users are unconscious).

Overall, despite many people's lack of knowledge regarding certain limitations of IoT devices, both informal interviews and online surveys showed that people have real concerns regarding sensitive data leaks, unauthorized access, physical security threats and lack of clear policies to share sensitive information with external entities.

Some researchers have suggested that network operators should control and maintain the management layer of home automation networks [13,28], but we disagree. We believe that users should be informed and empowered to configure their own settings. Since many people have trust issues with external entities, it does not make sense to delegate their security to a network provider. We also argue that developers should implement integrated solutions, while keeping the following security requirements in mind:

- Use secure communication protocols to ensure that users' data is protected against potential security breaches.
- Design and develop methods to prevent the inference of inhabitantes' activities [5,8,9,63].
- Segment and isolate the IoT network to block any unauthorized communication between these devices at the firewall-level [2,34,56,66]. It is also crucial to prevent communications with other network segments and external entities.

[9]This software is available at https://www.home-assistant.io/ (accessed on May 2, 2023).

- Implement secure gateways to enable communication between a wide range of devices, ensure a secure channel of communication between user interfaces and the system, and provide mechanisms for detecting and preventing possible intrusions.
- Explore artificial intelligence techniques to build models that enable assisted living environments to decide if a user needs external assistance.

We started a long term study to understand the real interaction between Paulo's family and their home appliances and implement a technology-rich assisted living environment [18,19]. While our research has primarily concentrated on designing and developing interaction methods and assistive technologies to improve the user experience of inhabitants, our concerns regarding privacy and data protection have grown in recent times. Although the original assisted living environment has been enhanced to meet various well-known data security requirements, the initial prototype used a Raspberry Pi acting as a gateway. All communication established between the gateway and different user interfaces, especially the one developed for mobile devices, was encrypted using the AES algorithm to protect inhabitants from potential attacks.

Over time, we proposed several interaction methods and an assistive robotic solution to facilitate interaction between inhabitants and their environment. Additionally, we implemented a more robust encryption method that combines RSA and AES algorithms to protect communication and data stored in the gateway from potential data leaks and hacker attacks. We also created a specific network to isolate all IoT devices from other networks, blocking all unknown traffic at the firewall-level. From May 2018 to December 2019, this network was protected with Snort IDS configured on a PFSense firewall, but Paulo changed their router and it no longer has that functionality.

We studied ways to comply with users' needs, desires and limitations, improving the mechanisms to protect their privacy and avoid data leaks. Overall, as described in Section 2, to the best of our knowledge we have already implemented the most advanced techniques in order to increase privacy and data protection in Paulo's intelligent environment. However, there are still many aspects to be explored and improved, For instance, although we developed a robotic solution that recognizes each inhabitant, their emotions, their pose, and detects falls or abnormal situations, it is not able to call for external help without the user's explicit consent. According to feedback from participants in both informal interviews and an online survey, it would be interesting to explore deep learning techniques to build a model that can detect if a user is unconscious, evaluate the situation, and call for assistance, without considering the user's privacy preferences.

To evaluate the network traffic generated by specific consumer devices, we implemented a small intelligent environment using a few inexpensive IoT devices.

3.2. Analyzing network traffic generated by consumer and inexpensive IoT devices

We created a segmented and isolated network to analyze the traffic generated by a small set of devices: a Philips Hue kit and three TP-Link TAPO C200 cameras (see Fig. 3). Our goal was to study the behavior of these widely popular devices without interfering with Paulo's family's daily tasks. After installing the devices, we captured all network traffic generated by them to a .cap file and analyzed it using a tool called Wireshark.[10]

We decided to use these two brands because they offer a wide range of well-known home automation solutions in recent years, and their products are economically accessible. These two well-known brands offer high-quality devices that are relatively more expensive than those available from anonymous brands. Unfortunately, most of the time, anonymous brands do not provide any kind of technical support or firmware updates for their devices, causing them to become obsolete within a short period of time. On other hand, the well-known brands, perhaps for commercial reasons, still pay attention to basic data security and provide firmware updates, along with appropriate technical support for their products for at least several years. Therefore, we have strong evidence to believe that if security and privacy flaws were to be encountered within well-known home automation solutions, anonymous solutions would have even more flaws. To reinforce our point of view, a study revealed that users prefer to buy well-known smart solutions rather than products from anonymous brands [68]. This suggest that they consider high-quality products such as Philips Hue to be more reliable and trustworthy.

[10] Wireshark is a well-known network protocol analyzer, which can be found at https://www.wireshark.org/ (accessed on May 2, 2023).

Fig. 3. A photo of devices used to create the small network.

The Philips Hue lighting system uses the ZigBee communication protocol[11] and requires a hub, known as the Philips Hue Bridge, to enable control of various lighting devices through the WIFI network. The TP-Link, a well-known manufacturer of network devices, also offers many solutions for home automation, including lighting systems and smart plugs, based on WIFI protocol.[12]

Although we used the Wireshark application to analyze the network traffic, we also utilized shell commands such as "nslookup" and "whois" to gather more detailed information about the servers used by these IoT devices. Figure 4 shows the utilization of these shell commands.

The network traffic analysis showed that TP-Link TAPO C200 cameras tried to resolve certain subdomains, namely rtsp-dcipc.tplinknbu.com, euw1-relay-dcipc.i.tplinknbu.com, n-device-api.tplinkcloud.com, and n-deventry-dcipc.tplinkcloud.com. We ran the following Linux shell commands to collect more detailed information about these domains: *whois tplinknbu.com* and *whois tplinkcloud.com*. We found that both domains were registered in Hong Kong and pointed to Amazon's name servers, while not employing Domain Name System Security Extension (DNSSEC).[13] After running the "nslookup" command for both domains, we also realized that they were pointing to servers located on Amazon Web Services (AWS).

The cameras tried to establish a secure TCP connection, through port 443, with the servers located on AWS. Overall, we concluded that TP-Link has developed solutions with mechanisms to prevent interceptation of users' data by hackers and other malicious agents. Nonetheless, we found certain vulnerabilities that can be exploited by bad actors, for instance, through DNS spoofing attacks. We also concluded that this brand uses third-party services, such as AWS, to implement its own cloud-based services. While less technologically savvy users may believe that their data are being treated and stored on TP-Link's datacenter, in reality their data flows inside the Amazon' data centers.

We also performed an identical analysis to identify the network traffic generated by Philips Hue Bridge and determine whether this specific solution ensures inhabitants' privacy and data protection. This equipment tried to resolve the subdomains ws.meethue.com and diagnostics.meethue.com, which point to one specific IP address of a server located on Google Cloud. Just like TP-Link, Philips contracted a third-party company to manage and maintain its servers, maximizing its profits and reducing its costs. Our analysis revealed that the Philips main domain is also vulnerable to DNS spoofing attacks due to the lack of DNSSEC implementation. The Philips Hue Bridge tried to establish both secure and insecure TCP connections with the server using ports 443 and 80, respectively. Although sensitive data were transmitted through the secure connections, insecure connections may leave inhabitants exposed

[11] The ZigBee protocol uses the AES-128 encryption algorithm to ensure that all information exchanges are protected against hacker attacks [64].

[12] Although integrating WIFI-based solutions into existing networks is easy, they consume more energy than devices based on other protocols [19].

[13] Overall, DNSSEC increases the security by providing a mechanism to digitally sign and authenticate DNS responses. It is essential to prevent DNS spoofing attacks.

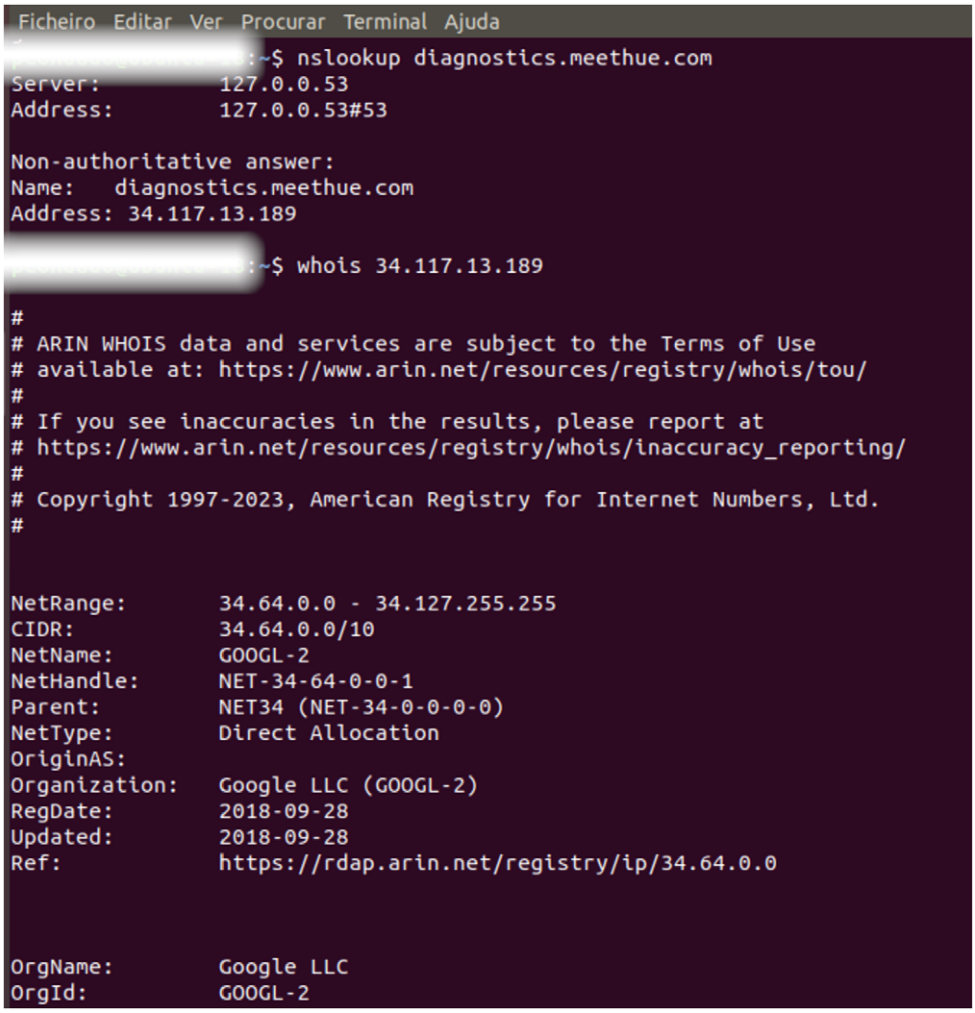

Fig. 4. Using nslookup and whois commands in a Linux shell.

to malicious agents, facilitating attackers' tasks. Nowaday, it is both unnecessary and poor practice to design products that use insecure communication channels.

Public cloud services should be considered untrustworthy systems because users are unaware of their implementation and whether a curious administrator can access their data [40,55]. As both Philips and TP-Link have opted to use third-party data centers (Google and Amazon), users are also depositing their trust in these third-party companies to protect their privacy and data. Assuming that both Philips and TP-Link own their servers on third-party data centers and encrypt all data using asynchronous encryption methods, it's possible that Google and Amazon administrators are unable to access the data. However, without further details on these systems' implementation, we cannot confirm this hypothesis, which means that these services may be implemented without these security measures, leading to an increased risk of data breaches.

The network traffic analysis also revealed that both brands have used domains without implementing DNSSEC, leaving their cloud-based services vulnerable to DNS spoofing attacks. This is an important issue that manufacturers of IoT devices should address to offer more robust solutions.

This analysis also showed that both brands have their servers located outside the member states of the European Union (EU), more specifically in the United States (US). Nevertheless, two of the four subdomains from TP-Link point to AWS servers located in Ireland (EU). It could indicate that TP-Link, a Chinese company with its main

domains registered in Hong Kong, is trying to comply with the GDPR and avoid sending personal data of European citizens to third countries. On the other hand, Philips, a Dutch company, is undoubtedly sending all the data to servers located in the US.

The GDPR defines that, "*under certain circumstances*", if personal information needs to be transmitted outside the protected area (EU and the three member states of the European Economic Area), the destination country must provide data protection at a level "*essentially equivalent*" to the protected area [44]. Nonetheless, data transfers to the US have been a problematic question. In 2020, the Court of Justice of the European Union decided to invalidate the 2016 EU-US Privacy Shield, which had previously allowed data transfers to certified companies [41]. As announced on the European Commission website,[14] "*the European Commission adopted its adequacy decision for the EU-US Data Privacy Framework*" on July 10, 2023.

Our research led us to conclude that the major manufacturers of IoT devices attempted to implement some security measures to protect users' privacy and data. Nonetheless, as developers have prioritized improving user interfaces, there are still certain security questions that must be addressed to improve users' privacy and data protection. Although some IoT devices have limited resources and do not support more robust security methods (as discussed in Section 2), the advances in technology will increase their memory and processing power.

Many home automation solutions suffer from security flaws, as pointed out in David Bombal's recent video "*Hacking IoT devices with Python (it's too easy to take control)*"[15,16]. Despite these issues, we still argue that it's important to empower both people with and without limitations to build their own intelligent environments using low-cost products. However, we also believe that users should be properly informed regarding the weaknesses of these technologies in order to implement effective security measures.

4. Summary and conclusion

Our comprehensive research, including a literature review, informal interviews, and an online survey, provided valuable insights for designing technology-rich assisted living environments that prioritize the privacy and data protection of their inhabitants. Although many IoT devices have limited memory and processing power, researchers have proposed various methods to protect inhabitants and their guest from malicious agents and information leaks, including intrusion detection systems [21,28,37,38,53,57], encryption methods [16], network security mechanisms [2,34,56,66], and methods to prevent the inference of inhabitants' activities [5,8,9,63]. Like [13], we believe that users may not have the necessary skills to control and manage the management layer of IoT networks. However, we disagree with the idea that network operators should be responsible for these tasks, as they are untrustworthy and have the potential to access users' sensitive information [40,55]. Instead, we argue that users should be informed on the potential threats of using IoT devices and how to implement measures to protect their intelligent environments.

According to our study, both informal interviews and an online survey revealed that people prefer to store sensitive information on self-hosted services, indicating a lack of confidence in external entities. To achieve this goal, people need to learn how to install open-source solutions such as Home Assistant, which can run on a local machine and promise to put "*local control and privacy first*". It is understandable that inhabitants want to keep control over information collected by environmental sensors (e.g. temperature, humidity, presence) and activity monitoring systems, protecting their own privacy. While we developed several solutions to assist Paulo and his family in accomplishing their daily tasks, we used low-cost hardware[17] to run self-hosted services, encrypt, and store all data generated by the proposed solution. Nevertheless, these systems do not provide a complete protection against data leaks, as they cannot block traffic generated by IoT devices at the firewall-level.

[14] The information is available at https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3721 (accessed on July 26, 2023).

[15] David Bombal is a well-known instructor, author, and YouTuber who develops and publishes training material on a wide range of topics related to network security, including Ethical Hacking, Python Programming, Linux, CCNA, and many others.

[16] The video is available at https://youtu.be/o9rlLuUpYxo (accessed on May 2, 2023).

[17] In the first stage, a Raspberry Pi acted as a gateway and stored all generated data. Currently, Paulo's family uses a low-power computer to perform this task.

As shown in Section 2.1, many IoT solutions available on the market establish connections with cloud-based services to offer a set of features to their customers. Although this would be useful for less technologically savvy users, as they can control their devices from anywhere using manufacturer applications, it means that users need to deposit their trust in these companies. Moreover, since certain manufacturers use third-party data centers to host their services, users are indirectly trusting in these third-party companies. To protect the privacy and data of Paulo's family, we designed the proposed solution to have its own isolated and segmented networks, blocking all traffic generated by devices at the firewall-level (curiously, a solution similar to the one proposed by [2] was implemented by us in late 2013).

There is no an easy-to-use solution to ensure that IoT devices, such as surveillance cameras, do not transmit sensitive data related to inhabitants' activities to their manufacturers. Setting up an isolated network for IoT devices can be a complex process for less technologically savvy users, representing a challenge for them to configure routers, switches, and access points. Moreover, building firewall rules to block network traffic from untrusted devices adds another layer of difficulty. We advocate that network manufacturers, some of them also produce IoT devices (e.g. TP-Link), should to develop all-in-one routers/firewalls to enable users to configure their intelligent environments and networks through an easy-to-use user interface. Therefore, users will be able to configure, control, and maintain their different networks without needing support from network operators or other external entities. Certain brands are making efforts to enable users to run Docker containers on their routers,[18] but it remains a non-trivial process and cannot be performed for less technologically savvy users. We believe that in the near future other brands will follow a similar path to develop secure, robust and easy-to-use home gateways.

Our online survey results showed that, unlike the participants in our informal interviews, many respondents believed that home automation devices are designed to ensure users' security. However, there are several products on the market that do not use encryption algorithms to protect their communications. For instance, there are many devices available on the market that use the X10 protocol. Initially, these insecure products were used to implement the first prototype that was used by Paulo's family. Fortunately, over time, we replaced these old devices with ones based on technologies that use lightweight symmetric cryptography algorithms [18,19].

This study also revealed that developing secure and easy-to-use assisted living environments is a complex process due to the various hardware limitations associated with home automation devices. Additionally, there are questions regarding how the use of cloud-based services can ensure users' privacy and data protection. Despite the positive impact of technology-rich assisted living environments on the autonomy of people with limitations, the existing literature highlights the need for further research to adequately protect sensitive user information, including medical data, from breaches.

During the last years, we developed technologies that enable Paulo's environment to recognize each inhabitant, their emotional state, their daily activities, and any abnormal situation (e.g. a fall or a critical health condition). Given the sensitive nature of this data, it is essential that developers and researchers adopt measures to protect both data and communications. Furthermore, it is crucial to develop models that enable intelligent environments to determine when external entities should be called upon for assistance.

The development of intelligent environments must take into account both the best practices used in HCI, such as user-centered design and an iterative development process, and the most recent security measures to guarantee privacy and data protection. Additionally, further studies are necessary to improve the protection of inhabitants' data. As these systems become even more capable of assisting people using artificial intelligence techniques, it is vital to conduct comprehensive research that examines certain actions that intelligent environments should take without human intervention and discusses ethical and moral aspects related to the use of these mechanisms.[19]

Based on our literature review, and to the best of our knowledge, there is a lack of in-depth research on the circumstances under which data collected by various systems should be shared with external entities such as health care services. To address these issues in our proposed solution, we adopted a simple approach that allows each inhabitant to define their own privacy settings. However, since there may be instances in which an inhabitant is unable

[18] It is possible to install Home Assistant onto the most recent version of RouterOS with containers – this information is available at https://community.home-assistant.io/t/installing-home-assistant-on-your-mikrotik-router-with-containers/522428 (accessed on May 2, 2023).

[19] The current version of our proposed assisted living environment can only call for external assistance if the inhabitant's preferences allow for it. Unfortunately, if the inhabitant is unconscious, the system does not have the capability to override their settings to provide better assistance.

to make decisions, such as in the event of a serious fall or heart attack, it is essential for intelligent environments to have mechanisms to evaluate the situation and take appropriate actions. And even here, the user should give consent beforehand, that in case the system finds him/her to be in an unconscious or dangerous state, to call for external assistance. We suggest that further studies should be conducted to explore the ethical and moral aspects of building models that enable machines to make decisions on behalf of unconscious inhabitants. While the majority of people who answered our online survey indicated that an intelligent environment should include mechanisms for providing appropriate assistance to unconscious inhabitants, many also noted the ethical and moral considerations involved.

The proposed environment has been designed to support Paulo and his family to perform their daily activities, avoiding to cause harm to anyone. Thus, based on the ethical framework proposed by [42] and explained in Section 2, the principles of non-maleficence and beneficence are observed as well as the principle of multi-user group, once the system is able to recognize each inhabitant and their needs, desires and limitations. Nonetheless, as mentioned above, our simplistic approach of allowing each inhabitant to define the system's action in case it finds him/her to be in an unconscious or danger state can lead us to a conflict of ethical principles. On one hand, the principles of privacy, data protection, and transparency are respected, allowing inhabitants to specify their privacy levels, define the levels of information-sharing or disclosure, and be aware of data processing, monitoring and surveillance [42]. On the other hand, due to individual privacy settings, the system may be unable to call for external assistance in order to help an inhabitant in a dangerous state, Once again, it is essential to balance various ethical issues and make trade-offs with some principles [42] to design systems for helping users to perform their daily activities, respecting their needs, preferences and ambitions.

Overall, the current version of our proposed assisted living environment follows the basic ethical principles described by [42]. The system has been developed to provide equality of access, since it uses low-cost hardware and we designed an easy-to-use user interface that allows both people with and without limitations to use it. Our assisted living environment also enhances the autonomy of those who have limitations by assisting them in their daily activities and improving their interaction with the surrounding world. This is very important to reduce their dependency on others and increase social inclusion. It is also essential to stress that our system has been designed to be transparent to users, allowing them to be clearly informed of the features offered by the assisted living environment, including data processing, surveillance, monitoring and the use of artificial intelligence. On the other hand, as already described, the proposed solution has also been developed to protect the privacy of inhabitants and their personal data. Therefore, the system protect inhabitants and their personal data, collecting and storing data on local servers rather than use public cloud-based solutions.

This research is a starting point for improving the security of intelligent environments through the analysis and study of mechanisms to protect inhabitants' data. To enable assisted living environments to share data with external entities, such as health care services, while protecting the privacy and data of the residents, we are building models using artificial intelligence techniques. A suitable model must be capable of detecting exceptional situations and requesting external assistance. Nonetheless, we are also trying to gain a better understanding of potential model failures (false positives) and the degree to which inhabitants are willing to tolerate them. We are also developing alternative interaction methods, as well as exploring augmented reality technology, to provide immersive experiences for inhabitants. We also designed user interfaces that facilitate the interaction of inhabitants with their environment and enable them to define their privacy settings in a simple way.

As a side note, we also plan to use our robotic platform to create an immersive robotic telepresence system, which will enable inhabitants to interact with a remote environment and feel as though they are actually there. As mentioned in [19], to the best of our knowledge, this has not been done before.

Acknowledgements

The authors acknowledge and thank the support given to CENSE by the Portuguese Foundation for Science and Technology (FCT) through the strategic project UIDB/04085/2020.

Paulo Condado's work was also sponsored by the Portuguese Foundation for Science and Technology, FCT/MCTES, under grant CEECIND/00578/2017.

Conflict of interest

None to report.

References

[1] J. Abascal, Ambient intelligence for people with disabilities and elderly people, in: *Proceedings of the ACM's Special Interest Group on Computer-Human Interaction (SIGCHI)*, Ambient Intelligence for Scientific Discovery (AISD) Workshop, 2004.

[2] S.G. Abbas, M. Husnain, U.U. Fayyaz, F. Shahzad, G.A. Shah and K. Zafar, IoT-sphere: A framework to secure iot devices from becoming attack target and attack source, in: *Proceedings of the 2020 IEEE International Conference on Trust, Security and Privacy in Computing and Communications*, IEEE, 2020, pp. 1402–1409.

[3] N.M. AbdelAzim, S.F. Fahmy, M.A. Sobh and A.M.B. Eldin, A hybrid entropy-based DoS attacks detection system for software defined networks (SDN): A proposed trust mechanism, *Egyptian Informatics Journal* **22**(1) (2021), 85–90. doi:10.1016/j.eij.2020.04.005.

[4] R.H. Abiyev and M. Arslan, Head mouse control system for people with disabilities, *Expert Systems* **37**(1) (2020). doi:10.1111/exsy.12398.

[5] A. Acar, H. Fereidooni, T. Abera, A.K. Sikder, M. Miettinen, H. Aksu, M. Conti, A.-R. Sadeghi and S. Uluagac, Peek-a-boo: I see your smart home activities, even encrypted!, in: *Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, 2020, pp. 207–218. doi:10.1145/3395351.3399421.

[6] S. Alam, M.S. Mahmud and M. Yeasin, Toward building safer smart homes for the people with disabilities, 2020, arXiv preprint arXiv:2006.05907.

[7] W. Alrajhi, D. Alaloola and A. Albarqawi, Smart home: Toward daily use of BCI-based systems, in: *Proceedings of the 2017 International Conference on Informatics*, Health & Technology (ICIHT), IEEE, 2017, pp. 1–5.

[8] M. Alyami, I. Alharbi, C. Zou, Y. Solihin and K. Ackerman, WiFi-based IoT devices profiling attack based on eavesdropping of encrypted wifi traffic, in: *Proceedings of the 2022 IEEE Annual Consumer Communications & Networking Conference (CCNC)*, IEEE, 2022, pp. 385–392.

[9] N. Apthorpe, D. Reisman, S. Sundaresan, A. Narayanan and N. Feamster, Spying on the smart home: Privacy attacks and defenses on encrypted iot traffic, 2017, arXiv preprint arXiv:1708.05044.

[10] J.C. Augusto, V. Callaghan, D. Cook, A. Kameas and I. Satoh, Intelligent environments: A manifesto, *Human-centric Computing and Information Sciences* **3** (2013), 1–18. doi:10.1186/2192-1962-3-12.

[11] Ç. Bakır, Single label model for confidentiality in big data, in: *Proceedings of the 6th International Conference on Computer Science and Engineering (UBMK)*, IEEE, 2021, pp. 10–14.

[12] M. Bassoli, V. Bianchi and I.D. Munari, A plug and play IoT wi-fi smart home system for human monitoring, *Electronics* **7**(9) (2018), 200. doi:10.3390/electronics7090200.

[13] J.M. Batalla, A. Vasilakos and M. Gajewski, Secure smart homes: Opportunities and challenges, *ACM Computing Surveys (CSUR)* **50**(5) (2017), 1–32. doi:10.1145/3122816.

[14] E. Bertino, Data privacy for IoT systems: Concepts, approaches, and research directions, in: *Proceedings of the 2016 IEEE International Conference on Big Data (Big Data)*, IEEE, 2016, pp. 3645–3647. doi:10.1109/BigData.2016.7841030.

[15] H.F. Chinchero, J.M. Alonso and H. Ortiz, LED lighting systems for smart buildings: A review, *IET Smart Cities* **2**(3) (2020), 126–134. doi:10.1049/iet-smc.2020.0061.

[16] L. Colorado, Security in 1-wire system: case study: Home automation, Master's thesis, Universidad Tecnológica de Bolívar, 2017.

[17] P.A. Condado and F.G. Lobo, EasyVoice: Breaking barriers for people with voice disabilities, in: *Proceedings of the 11th International Conference on Computers Helping People with Special Needs*, Lecture Notes in Computer Science, Vol. 5105, Springer, Berlin, Heidelberg, 2008, pp. 1228–1235. doi:10.1007/978-3-540-70540-6_185.

[18] P.A. Condado and F.G. Lobo, A system for controlling assisted living environments using mobile devices, in: *Proceedings of the 17th International ACM SIGACCESS Conference on Computers & Accessibility, ASSETS'15*, ACM Press, New York, NY, USA, 2015, pp. 33–38. doi:10.1145/2700648.2809839.

[19] P.A. Condado, F.G. Lobo and T. Carita, Towards richer assisted living environments, *SN Computer Science* **3**(1) (2022), 1–13. doi:10.1007/s42979-021-00983-0.

[20] G. Cortellessa, F. Fracasso, A. Sorrentino, A. Orlandini, G. Bernardi, L. Coraci, R. De Benedictis and A. Cesta, ROBIN, a telepresence robot to support older users monitoring and social inclusion: Development and evaluation, *Telemedicine and e-Health* **24**(2) (2018), 145–154. doi:10.1089/tmj.2016.0258.

[21] A. Cosson, A.K. Sikder, L. Babun, Z.B. Celik, P. McDaniel and A.S. Uluagac, SENTINEL: A robust intrusion detection system for IoT networks using kernel-level system information, in: *Proceedings of the International Conference on Internet-of-Things Design and Implementation*, 2021, pp. 53–66. doi:10.1145/3450268.3453533.

[22] C. De Terwangne, Council of Europe convention 108+: A modernised international treaty for the protection of personal data, *Computer Law & Security Review* **40** (2021), 105497. doi:10.1016/j.clsr.2020.105497.

[23] J. Ding and Y. Wang, A WiFi-based smart home fall detection system using recurrent neural network, *IEEE Transactions on Consumer Electronics* **66**(4) (2020), 308–317. doi:10.1109/TCE.2020.3021398.

[24] M. Duraipandian and R. Vinothkanna, Cloud based Internet of things for smart connected objects, *Journal of ISMAC* **1**(02) (2019), 111–119.

[25] G. Edlinger, C. Holzner and C. Guger, A hybrid brain-computer interface for smart home control, in: *Proceedings of the 14th International Conference on Human-Computer Interaction. Interaction Techniques and Environments*, Springer, Berlin, Heidelberg, 2011, pp. 417–426.
[26] K.A. Faraj, M. Mojahid and N. Vigouroux, BigKey: A virtual keyboard for mobile devices, in: *Proceedings of the 13th International Conference on Human-Computer Interaction. Part III: Ubiquitous and Intelligent Interaction*, Lecture Notes in Computer Science, Vol. 5612, Springer, Berlin, Heidelberg, 2009, pp. 3–10.
[27] I.B. Fink, M. Serror and K. Wehrle, Extending MUD to smartphones, in: *Proceedings of the 2020 IEEE Conference on Local Computer Networks (LCN)*, IEEE, 2020, pp. 353–356. doi:10.1109/LCN48667.2020.9314782.
[28] M. Gajewski, J.M. Batalla, G. Mastorakis and C.X. Mavromoustakis, A distributed IDS architecture model for smart home systems, *Cluster Computing* **22**(1) (2019), 1739–1749. doi:10.1007/s10586-017-1105-z.
[29] K.Z. Gajos, J.O. Wobbrock and D.S. Weld, Automatically generating user interfaces adapted to users' motor and vision capabilities, in: *UIST'07: Proceedings of the 20th Annual ACM Symposium on User Interface Software and Technology*, ACM Press, New York, NY, USA, 2007, pp. 231–240. doi:10.1145/1294211.1294253.
[30] R. Godinho, P.A. Condado, M. Zacarias and F.G. Lobo, Improving accessibility of mobile devices with EasyWrite, *Behaviour & Information Technology* **34**(2) (2015), 135–150. doi:10.1080/0144929X.2014.981584.
[31] S. Greene, IoT development for healthy independent living, Master's thesis, University of Kentucky, 2017.
[32] S. Greene, H. Thapliyal and D. Carpenter, IoT-based fall detection for smart home environments, in: *Proceedings of the 2016 IEEE International Symposium on Nanoelectronic and Information Systems (iNIS)*, IEEE, 2016, pp. 23–28. doi:10.1109/iNIS.2016.017.
[33] T. Guerreiro, H. Nicolau, J. Jorge and D. Gonçalves, NavTap: A long term study with excluded blind users, in: *ASSETS'09: Proceedings of the 11th International ACM Conference on Computers and Accessibility*, ACM Press, New York, NY, USA, 2009, pp. 99–106. doi:10.1145/1639642.1639661.
[34] C. Haar and E. Buchmann, FANE: A firewall appliance for the smart home, in: *Proceedings of the 2019 IEEE Federated Conference on Computer Science and Information Systems*, IEEE, 2019, pp. 449–458. doi:10.15439/2019F177.
[35] R.A. Hamad, A.S. Hidalgo, M.-R. Bouguelia, M.E. Estevez and J.M. Quero, Efficient activity recognition in smart homes using delayed fuzzy temporal windows on binary sensors, *IEEE journal of biomedical and health informatics* **24**(2) (2019), 387–395. doi:10.1109/JBHI.2019.2918412.
[36] D. He, X. Li, S. Chan, J. Gao and M. Guizani, Security analysis of a space-based wireless network, *IEEE Network* **33**(1) (2019), 36–43. doi:10.1109/MNET.2018.1800194.
[37] R. Heartfield, G. Loukas, A. Bezemskij and E. Panaousis, Self-configurable cyber-physical intrusion detection for smart homes using reinforcement learning, *IEEE Transactions on Information Forensics and Security* **16** (2020), 1720–1735. doi:10.1109/TIFS.2020.3042049.
[38] I. Idrissi, M. Azizi and O. Moussaoui, Accelerating the update of a DL-based IDS for IoT using deep transfer learning, *Indonesian Journal of Electrical Engineering and Computer Science* **23**(2) (2021), 1059–1067. doi:10.11591/ijeecs.v23.i2.pp1059-1067.
[39] M. Jefford and R. Moore, Improvement of informed consent and the quality of consent documents, *The lancet oncology* **9**(5) (2008), 485–493. doi:10.1016/S1470-2045(08)70128-1.
[40] D.N. Jha, G. Lenton, J. Asker, D. Blundell and D. Wallom, Trusted platform module-based privacy in the public cloud: Challenges and future perspective, *IT Professional* **24**(3) (2022), 81–87. doi:10.1109/MITP.2022.3147968.
[41] G. Johnson, Economic research on privacy regulation: Lessons from the GDPR and beyond, 2022, National Bureau of Economic Research Working Paper.
[42] S. Jones, S. Hara and J. Augusto, eFRIEND: An ethical framework for intelligent environment development, in: *Proceedings of the 7th International Conference on PErvasive Technologies Related to Assistive Environments*, 2014, pp. 1–4.
[43] T.E. Jost, Privacy Management for Cyber-Physical Systems – a System-of-Systems Architecture Based on Digital Twins, Master's Thesis, Johannes Kepler Universität, Linz, 2021.
[44] B.A. Juliussen, E. Kozyri, D. Johansen and J.P. Rui, The third country problem under the GDPR: Enhancing protection of data transfers with technology, *International Data Privacy Law* (2023), ipad013. doi:10.1093/idpl/ipad013.
[45] M. Kasmi, F. Bahloul and H. Tkitek, Smart home based on Internet of things and cloud computing, in: *Proceedings of the 2016 International Conference on Sciences of Electronics, Technologies of Information and Telecommunications (SETIT)*, IEEE, 2016, pp. 82–86.
[46] P. Kokkinos, T.A. Varvarigou, A. Kretsis, P. Soumplis and E.A. Varvarigos, Cost and utilization optimization of Amazon ec2 instances, in: *Proceedings of the 2013 IEEE International Conference on Cloud Computing*, IEEE, 2013, pp. 518–525.
[47] S. Miniaoui, S. Atalla and K.F.B. Hashim, Introducing innovative item management process towards providing smart fridges, in: *Proceedings of the 2nd International Conference on Communication Engineering and Technology (ICCET)*, IEEE, 2019, pp. 62–67.
[48] J. Park, K. Jang and S.-B. Yang, Deep neural networks for activity recognition with multi-sensor data in a smart home, in: *2018 IEEE 4th World Forum on Internet of Things (WF-IoT)*, IEEE, 2018, pp. 155–160. doi:10.1109/WF-IoT.2018.8355147.
[49] R. Pottier and J.-M. Menaud, Privacy-aware data storage in cloud computing, in: *CLOSER*, 2017, pp. 377–384.
[50] M.T. Pourazad, A. Shojaei-Hashemi, P. Nasiopoulos, M. Azimi, M. Mak, J. Grace, D. Jung and T. Bains, A non-intrusive deep learning based fall detection scheme using video cameras, in: *Proceedings of the 2020 International Conference on Information Networking (ICOIN)*, IEEE, 2020, pp. 443–446. doi:10.1109/ICOIN48656.2020.9016455.
[51] Z. Qian, Y. Lin, W. Jing, Z. Ma, H. Liu, R. Yin, Z. Li, Z. Bi and W. Zhang, Development of a real-time wearable fall detection system in the context of Internet of things, *IEEE Internet of Things Journal* **9**(21) (2022), 21999–22007. doi:10.1109/JIOT.2022.3181701.
[52] R. Raj and N. Rai, Voice controlled cyber-physical system for smart home, in: *Proceedings of the Workshop Program of the 19th International Conference on Distributed Computing and Networking*, 2018, pp. 1–5.
[53] E. Rodríguez, P. Valls, B. Otero, J.J. Costa, J. Verdú, M.A. Pajuelo and R. Canal, Transfer-learning-based intrusion detection framework in IoT networks, *Sensors* **22**(15) (2022), 5621. doi:10.3390/s22155621.

[54] C. Ryngaert and M. Taylor, The GDPR as global data protection regulation?, *American Journal of International Law* **114** (2020), 5–9.
[55] C. Sahin and A. El Abbadi, Data security and privacy for outsourced data in the cloud, in: *Proceedings of the 2018 IEEE International Conference on Data Engineering (ICDE)*, IEEE, 2018, pp. 1731–1734. doi:10.1109/ICDE.2018.00225.
[56] M. Serror, M. Henze, S. Hack, M. Schuba and K. Wehrle, Towards in-network security for smart homes, in: *Proceedings of the 13th International Conference on Availability, Reliability and Security*, 2018, pp. 1–8.
[57] V. Simadiputra and N. Surantha, Rasefiberry: Secure and efficient Raspberry-Pi based gateway for smarthome IoT architecture, *Bulletin of Electrical Engineering and Informatics* **10**(2) (2021), 1035–1045. doi:10.11591/eei.v10i2.2741.
[58] D. Singh, E. Merdivan, S. Hanke, J. Kropf, M. Geist and A. Holzinger, Convolutional and recurrent neural networks for activity recognition in smart environment, in: *Towards Integrative Machine Learning and Knowledge Extraction*, A. Holzinger, R. Goebel, M. Ferri and V. Palade, eds, Springer, Berlin, Heidelberg, 2017, pp. 194–205. doi:10.1007/978-3-319-69775-8_12.
[59] U.V. Solanki and N.H. Desai, Hand gesture based remote control for home appliances: Handmote, in: *Proceedings of the 2011 World Congress on Information and Communication Technologies*, IEEE, 2011, pp. 419–423. doi:10.1109/WICT.2011.6141282.
[60] K. Sun, C. Chen and X. Zhang, "Alexa, stop spying on me!": Speech privacy protection against voice assistants, in: *Proceedings of the 18th Conference on Embedded Networked Sensor Systems*, 2020, pp. 298–311. doi:10.1145/3384419.3430727.
[61] K. Vertanen and P.O. Kristensson, Parakeet: A continuous speech recognition system for mobile touch-screen devices, in: *Proceedings of the 14th International Conference on Intelligent User Interfaces, IUI'09*, ACM Press, New York, NY, USA, 2009, pp. 237–246.
[62] M. Vretta, The new EU General Data Protection Regulation (GDPR) in medical data and clinical research, Master's thesis, International Hellenic University, 2019.
[63] Y. Wan, K. Xu, F. Wang and G. Xue, IoTMosaic: Inferring user activities from IoT network traffic in smart homes, in: *IEEE INFOCOM 2022 – IEEE Conference on Computer Communications*, IEEE, 2022, pp. 370–379. doi:10.1109/INFOCOM48880.2022.9796908.
[64] Y. Wang, C. Chen and Q. Jiang, Security algorithm of Internet of things based on ZigBee protocol, *Cluster Computing* **22** (2019), 14759–14766. doi:10.1007/s10586-018-2388-4.
[65] J. Wobbrock and B. Myers, Trackball text entry for people with motor impairments, in: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, CHI'06*, ACM Press, New York, NY, USA, 2006, pp. 479–488. doi:10.1145/1124772.1124845.
[66] C. Ye, P.P. Indra and D. Aspinall, Retrofitting security and privacy measures to smart home devices, in: *Proceedings of the 2019 IEEE International Conference on Internet of Things: Systems, Management and Security*, IEEE, 2019, pp. 283–290.
[67] R.N. Zaeem and K.S. Barber, The effect of the GDPR on privacy policies: Recent progress and future promise, *ACM Transactions on Management Information Systems (TMIS)* **12**(1) (2020), 1–20.
[68] S. Zheng, N. Apthorpe, M. Chetty and N. Feamster, User perceptions of smart home IoT privacy, in: *Proceedings of the 2018 ACM on Human-Computer Interaction 2(CSCW)*, 2018, pp. 1–20.