Smart Home Care: Towards Supporting Elderlies in the Comfort and Safety of their (Smart) Homes

Igor Zavalyshyn[†], Axel Legay[†], Annanda Rath[‡], Etienne Rivière[†]
[†] ICTEAM, UCLouvain, Belgium [‡] SIRRIS, Belgium
{igor.zavalyshyn,axel.legay,etienne.riviere}@uclouvain.be, annanda.rath@sirris.be

***Abstract*—The aging of the population will be a major challenge in the coming years and will lead to massive changes related to aging peoples' safety, social inclusion, and well-being. The nature of the aid provided to elderly people is already changing, with a shift towards home care (assisted living) as compared to traditional care homes. In this position paper, we highlight the need for appropriate home automation and support systems that ensure the safety and well-being of aging occupants and maintain their social links with various people around them. Existing smart home systems do not meet all the requirements and safety features required for this purpose, in particular in terms of usability, privacy, and security. We describe the challenges the research community and the industry will need to address when designing smart home care systems and lay out a research agenda that we hope will stir more work in this important emerging area.**

***Index Terms*—access control, privacy, smart home care**

I. Introduction

The aging of the population will be a major challenge in the coming years. In Europe, the numbers of elderly people (aged 65 and over) is expected to rise from 61 million in 2000 to 103 million in 2050. The number of the very old (aged 80 and over) will triple in size over that period [1]. Globally, the total number of people aged 65 years and over is projected to more than double by 2050, while the number of very old people could triple in size [2]. Society needs to be prepared for a situation in which almost one-third of the population will be aged over 65 and one-tenth will be older than 80. Due to rapid increases in life expectancy more and more people live with chronic conditions, such as obstructive sleep apnea [3], that do not require immediate hospitalization but yet involve specific care and surveillance. At the same time, the current system where older people live in elderly care homes is increasingly considered as unsustainable at the scale of the aging population, with a lack of capacity in terms of infrastructure and personnel.

As a result, we already witness a major shift towards home care (assisted living) as an alternative to care homes [4]–[6]. Older people increasingly prefer to stay in the comfort of their homes and remain connected with their social network, e.g., family members, friends and neighbors, but also nursing personnel, service providers, doctors, etc., rather than go to a care home. However, a shift towards home care is associated with numerous challenges, such as ensuring autonomy and safety of the elderly person without a specially-trained personnel around at all times, as well as dealing with social isolation and loneliness issues. In order to address these challenges, it is essential to develop reliable, cost-effective and easy-to-use home care solutions. Recent advancements in smart home technologies offer a potential way to address these challenges. With various smart home sensors deployed in one's home it would be possible for instance for family members to stay connected with their loved ones, and for care professionals to monitor the health and well-being of the elderly and react to certain events without a need for constant physical presence.

However, existing smart home systems do not offer the properties required for smart home care. They were developed with home automation scenarios in mind and provide weak safety, security and availability guarantees, and at most offer a best-effort service [7]. Their configuration process often requires a companion smartphone app which does not take into account the usability and accessibility requirements of older people. Furthermore, the user interfaces of various smart home systems are often centered around a single user or a family, but offer a limited set of capabilities (if any) for sending event notifications and alerts to external members like neighbors and health professionals. The aspect of social isolation is rarely considered in the context of smart homes which makes it harder for older people and their families to adopt this technology. Finally, due to their limited technological literacy and experience older people tend to be unaware of and susceptible to various security and privacy risks posed by smart home systems [8], which results in either acting recklessly or avoiding a smart technology use completely.

In this paper, we lay out a research agenda towards making fair, dependable and open smart home care systems a reality. We highlight the challenges one might face when designing such systems and suggest potential research directions. While in this work we mostly focus on the technological side of the system design, we certainly agree that the effort towards effective and sustainable smart home care is intrinsically multidisciplinary, and there is still a lot to be done from the medical, business, and social sciences perspectives. Laying a foundation for smart home care systems requires collaborative effort from healthcare professionals, caregivers, legislators, engineers and, most importantly, representatives of the elderly.

II. Motivation

As a motivating example, consider a scenario in which an old lady lives alone in her own house. The lady has a son who lives separately with his own family but visits her several

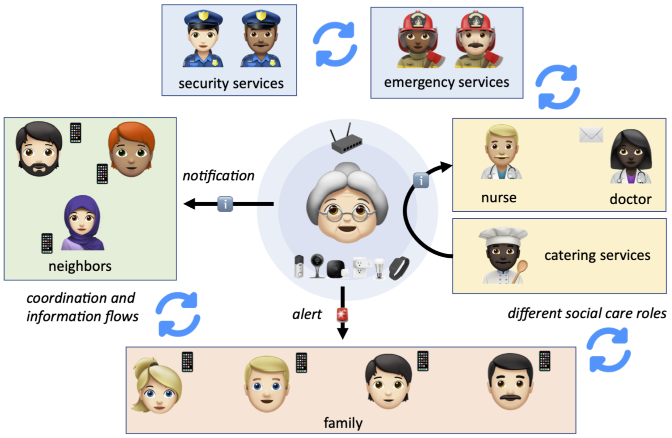

Fig. 1. Examples of interactions in smart home care.

times a week to bring groceries and spend time with her. While these visits are frequent, the son wants to have a better overview of his mother's health and well-being, as well as her daily activities and needs when he is not around. Given her old age, the lady may forget to take medicine or, worse, to turn off the gas stove, and the son wants to be aware of such things. He is also worried that his mother may fall or have a stroke in his absence and there will be no one to help her. Furthermore, the lady suffers from an obstructive sleep apnea – a breathing disorder which causes an occasional reduced or absent breathing during sleep. For proper diagnostics and treatment of this medical condition it is important to monitor various health parameters, such as pulse oximetry and blood oxygen saturation levels throughout the night. Such monitoring would be possible in a special care home, however, the lady preferred to stay in the comfort of her own home with regular visits of a nurse and a family doctor.

Since a care home is not an option, the son considers an alternative solution. One potential option is a smart home care system that would collect information from various connected smart home actuators and sensors, as well as medical devices in his mother's home, and provide insights into her health, well-being and daily activities. The system would send notifications and alerts to various interested parties. For instance, it will notify the son when his mother forgets to take her pills, prepare health and sleep quality reports for her doctor, or send an alert to emergency services when a fall is detected. The same system will connect the lady with her neighbors and professional caregivers who can help with daily activities and provide social support.

To set up such a system, the son wants to use off-the-shelf smart home devices that he can buy in the department store, as well as specialized medical sensors and monitors suggested by the doctor (e.g. a CPAP device for sleep apnea patients) that can be installed and configured by specialists. He does not want to create complex trigger-based rules for notifications and alerts on his own, and prefers to use applications that were specifically written for elderly care scenario. He only wants to define a set of people and/or services the system should be able to notify or alert (e.g. an SMS, an email or even a call) and the types of these alerts in each specific case.

A. System model

Following the motivating example we will now define a model of the system we envision for this specific use-case. As seen at Figure 1, in the center of the system is the lady who's health and well-being is being monitored. Such a central positioning is crucial since the system must be centered around the lady's needs, preferences and her social network which can be quite diverse. Within her social network we can define several distinct groups or *circles*: first, there are family members like her son who wants to keep an eye on his mother's life when he is away; then there are professional caregivers like doctors, nurses and representatives of various catering and cleaning services who offer regular medical checks and provide for basic needs; the neighbors and friends circle comprises all of the trusted people who are physically close to the lady and may offer help with day-to-day tasks and react quickly to critical events; finally, a circle of security and emergency services representatives offer emergency response.

Each member of a given social circle will receive notifications and alerts that are relevant for the offered service, e.g. the catering service will receive diet suggestions approved by the doctor and the emergency service will receive an alert when a fall is detected. Furthermore, the members of different social circles can interact with each other, coordinate their actions and suggest improvements. For instance, a doctor may recommend the lady's son to remind her about the pills. A catering service representative may inform the family members and a doctor about the lady's poor appetite. Finally, the son may ask lady's neighbors to help her with some daily tasks when the need arises, e.g. take out the garbage.

B. Desired system guarantees

The envisioned smart home care system has to provide a set of essential guarantees:

Privacy guarantees: sensitive data collection and processing has to comply with the privacy expectations and preferences of the monitored person (the lady) and her relatives (the son). The notifications and alerts generated by the system have to contain only minimal amount of information required for the desired purpose (e.g., according to the purpose limitation principles of regulations such as the EU GDPR [9] or the upcoming update of California's CCPA [10]) and respect appropriate usability/privacy tradeoffs.

Reliability (or dependability) guarantees: the system may signal the occurrence of critical and potentially life-threatening events (e.g., a detected fall) which need to be processed in a timely and efficient manner. A failure to notify an emergency contact or delay such a notification may result in serious injury or even death and have irreversible consequences. At the same time, for some other events a delay of several minutes or even hours may be acceptable, e.g., a daily physical activity report sent to a doctor. To this end, the system must be working in a ‘mixed criticality’ mode in which critical workloads are co-located with non-critical ones. At the system level, there must be a sufficient performance isolation so that critical workloads can never be blocked by non-critical ones, even when the latter try to exhaust systems resources.

Usability guarantees: the system will be used by the people who might have different levels of technological literacy and experience with smart devices. The system must therefore be designed in a way that considers these differences and provides an easy-to-use and more importantly convenient interface to all kinds of its users.

Flexibility guarantees: the members of various social circles can be represented by real people, e.g., neighbors or family members, or services, e.g., emergency or nursing services. The system must be easily extendable and provide the means to connect to and interact with existing or future third-party services. Such a flexible design allows providers of specific solutions (e.g. a monitoring system for a certain disease, or novel ML-based solutions for dementia signs detection, or personalized menu suggestions of catering service, etc.) to offer new services built on top of such system.

C. Inadequacy of existing smart home systems

Following a generalized system model description and a set of guarantees it must provide we will now examine existing smart home systems to determine if they could form the basis for a smart home care ecosystem.

Cloud-based smart home systems, such as Amazon Alexa or Samsung SmartThings, have a wide range of supported devices and a collection of home automation applications, or *apps*, available out-of-the-box, but their cloud-first design requires sending all of the sensitive sensor data to the cloud servers outside of user control, which conflicts with our privacy requirement. Fully local and open-source home automation systems, such as OpenHAB and Home Assistant, allow their users to collect and process sensor data locally but do not prevent data leaks through alerts sent by the system.

In terms of reliability, none of the existing smart home systems proved to be suitable for emergency and life-threatening scenarios [11], [12]. Moreover, these systems do not take into account the criticality of the events they process and offer no way for the users to specify the priorities for favoring certain events over the others. While priority-based approaches to smart home data processing have been previously proposed in academia [13]–[15], commercial systems still lag behind [16].

Usability-wise existing smart home systems are not suitable for a smart home care scenario either due to their excessive use of mobile apps as command and control interfaces, or their high expectations regarding user’s ability to be aware of and comprehend the internal structure and interactions within one’s smart home. Voice-controlled interfaces are more natural and convenient to use but without a proactive interaction model they still require active user engagement to operate.

Finally, smart home systems generally consider a scenario in which only a single user (or only the members of one household with equal capabilities) interact with the system. This contrasts with the system flexibility required in a smart home care scenario. Some of the alerts or notification may need to be shared with external parties, such as a family doctor or a nurse. Furthermore, the access control mechanisms used by smart home systems are often too coarse-grained and can only allow or block access to certain device events.

D. Lack of appropriate security mechanisms

IoT systems, and smart home ones in particular, have received a tremendous amount of attention from researchers over the last 5 years, mainly due to the numerous flaws found in either device software [17], [18], communication protocols [19]–[21], third-party apps [22]–[26], and cloud platforms [27]–[30]. In particular, Fernandes *et al.* investigated the problem of overprivileged apps in commercial smart home platforms [22] and proposed mechanisms for effective data flow tracking and privacy policy enforcement [23]. The same authors later pointed out the limitations of a permission-based model commonly used in IoT systems suggesting it is too coarse grained and leaves the end users at risk for potential security and privacy violations. They proposed alternative context-dependent access control policies for multi-user environments [30]. Celik *et al.* investigated the potential of static taint analysis to detect sensitive information misuse by IoT apps [24] and possible conflicts between the apps operating in the same environment [25], [26]. However, common across all of the proposed systems is the assumption that a smart home platform provider and all of the platform components including a hub and cloud servers are trusted and may not act maliciously. Such an assumption is a dangerous one and other researchers have pointed out its inadequacy, as well as suggested ways to minimize the amount of sensitive data sent to the platform provider’s cloud [31]. While there is a large body of work in the area of smart home privacy and security, most existing approaches are not directly applicable to home care scenario due to limitations of their access control mechanisms, app programming models or trust models used.

For a smart home care system to be secure, there is a need for a dynamic, fine-grained and context-aware access control system which restricts alerts and notifications to authorized social circles’ only. Traditional role- [32], [33] or attribute-based [34], [35] access control systems may be a viable option but would need to be customized to allow for the members of the same social circle to receive different types of alerts and notifications and with different information contained in those.

When it comes to specifying one’s expectations and preferences regarding sensor data processing and sharing, existing smart home systems lack flexibility and often provide a limited set of control knobs. The control options are usually ‘binary’ in a sense that they either allow or block a certain app action, which is not suitable when the action depends on the context or type of shared data. Several alternative privacy policy specification mechanisms have been proposed [36]–[38], however, they all fall short at offering mechanisms to set policies in an intelligible manner that considers the granularity and sensitivity of the shared information, the context in which

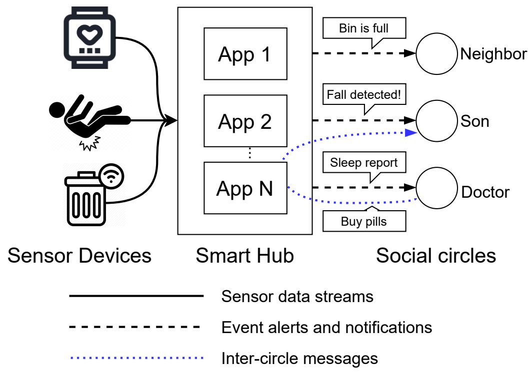

Fig. 2. A bird's-eye view of smart home care system.

the sharing takes place, and, most importantly, the social circle involved in such sharing.

The usability and privacy aspects of smart systems have been rarely discussed in the context of their use by older people [8], [39]–[41]. Frik *et al.*, in semi-structured interviews with 46 adults aged over 65, identified a range of usability and risk assessment issues that stem from limited technical knowledge, experience as well as a decline of their physical abilities [8]. These issues often lead to poor security and privacy choices or instead become a barrier to wide technology adoption. The results of this study only prove an urgent need for mechanisms and interfaces allowing non-expert users to understand and define privacy and security policies using intelligible notions of social circles and scenarios. Gaspar *et al.* [41] performed a systematic analysis of various participatory methods used to design future home care systems for elderly, and suggested a concept of *'personas'* to identify and characterize different users of the system, such as caregivers, relatives and neighbors. In our system model we define such personas as members of various *social circles*.

Finally, the idea of mixed-criticality systems that prioritize certain events processing over others have been discussed for a while [42], [43]. However, while this research has been widely applied in industrial IoT, in the area of smart care and in smart homes in general the idea of mixed-criticality processing has yet to be adopted.

III. Proposed architecture

Considering that none of the existing smart home systems can fully satisfy the requirements of a smart home care scenario, we now present our vision for the design of such a system and highlight its essential features.

Our envisioned architecture of a smart home care system is shown in Figure 2. Its central component is a *smart hub*. This hub collects sensor data from the connected *sensor devices* and allows to process it locally in a privacy-aware manner without the need to share sensitive information with external cloud services or third-parties. This is essential to enforce privacy guarantees and maintain control over the flows of sensor data. The hub provides an execution environment for various *apps* that compute on and analyze sensor data, and generate alerts and notifications to the selected *social circles* if needed. These apps are offered by various third-party organizations, such as those providing nursing, food delivery or social services, as well as medical hospitals and polyclinics. Through such apps all of these organizations can have an up to date information about the health, well-being and needs of the elderly person, and thus can offer a more tailored services. The apps may be installed at the hub by the system administrator – a tech-savvy family member or a professional who installs the system.

Social circles constitute the groups of people who are responsible for the health and well-being of a monitored person. Affiliation with a given circle limits the amount, type and granularity of notifications and alerts one might receive. For instance, a members of an emergency services circle will receive notifications based on certain devices' data only, e.g., a gas sensor or a fall detector, while the other circles will have a much broader range of notifications and alerts. At the same time, the content of notifications will also differ from circle to circle. Coming back to our motivating example in Section II, the son being a family member would have full access to his mother's daily physical activity and sleep quality, while her doctor should only receive aggregated daily statistics.

Various social circles can also communicate between each other through on of the installed apps at the hub. For instance, a doctor after looking at the latest sleep quality report may decide to prescribe new sleeping pills and leave a message for a lady's son to buy those for her (see Figure 2). Such a communication mimics real-world interaction between the caregivers and the family members.

The exact list of members for each social circle can be defined by the monitored person herself or a hub administrator (e.g., a son). For each member a contact information, e.g., a phone number or an e-mail, has to be provided which is later used to send notifications about pre-configured events. Alternatively, the notifications can be sent through a third-party SMS or push messaging service connected to the hub.

A. Smart Hub Internals

After a general overview of our proposed architecture for the smart care system, we will now provide more details about the internals of the hub and their intended purpose.

Device Drivers: Device drivers implement software interfaces to various devices connected to the hub. They abstract away the complexity of the communication protocols or specific hardware characteristics and instead offer a simple way to interact with device functions and collect sensor readings. A smart hub may come with a set of default drivers for interacting with Zigbee, Z-Wave and BLE devices commonly used in smart home scenarios.

Middleware: A smart hub implements a middleware layer that serves as a proxy between the sensor data provided by the connected devices and the smart apps requesting access to this data. This middleware layer interacts with the devices using the corresponding device drivers installed on the hub, and offers an API for the apps to access the device data, trigger certain device actions, or send notifications and alerts to various social circles or external services. The apps run in sandboxes that restrict apps' activities to curated API calls only. The runtime environment closely monitors sensitive data flows between the sensor devices and various social circles instantiated by the apps, and verifies if these flows comply with the privacy and security preferences of the monitored person.

API: An API exposed by the middleware to the installed apps provides access to sensor data in two modes: a history-based and a reactive one. A history-based mode is suitable for batch processing of sensor data collected in the past over a specified time period, for example, when computing an average daily room temperature. A reactive mode fits the trigger-based nature of IoT apps that act in response to a given trigger event, e.g. send an emergency message when fall is detected. In this mode a device state change event is immediately sent to all the apps that subscribed to this event.

App Types: Apps implement passive monitoring functions: they act upon device state changes but do not trigger those themselves. Their logic differs from app to app but generally falls into one of two categories: *analytical* apps or *reactive* apps. Analytical apps are more suitable for monitoring the health and well-being parameters in retrospective mode. Such apps may, for instance, compute the average daily physical activity of the person, analyze her sleep quality or hygiene routines. The amount of data these apps usually have access to is measured in data points spread across hours, days or even weeks. Their outputs are either aggregated values computed for a given period of time or raw values that might be useful for further analysis done by any of the social circles. Following our motivating example, this is a case for the app that shares aggregated statistics on lady's sleep quality with a doctor.

The reactive apps act upon the immediate events. They react to a set of critical and potentially life-threatening events, such as a gas leak or a detected fall. The goal of reactive apps is to notify the specified social circles when a given event occurs in real time. Hence, the data available to these apps is limited to the last data point generated by a given device. The output of reactive apps is either a textual notification, a raw device state (e.g., *fall: detected*) or a combination of both. An app that notifies an emergency service about the detected fall event is an example of a reactive app.

IV. Research Challenges

When designing a smart care system one needs to overcome a number of significant challenges concerning access control, usability, privacy and security. While some of these challenges have been previously addressed in a smart home scenario, there is no one-fits-all solution that can be easily applied to a home care scenario. Hence, we will now summarize key challenges and potential research directions specific to this use-case.

Challenge 1: Fine-grained access control. A smart home care system needs a flexible access control system that is able to determine the sensitivity of the shared data and the context in which this sharing takes place to enforce proper restrictions for each social circle. For instance, a physical activity log may be shared with family members in a raw form, while only an aggregated and anonymized summary can be shared with the doctor. One potential way to achieve this goal would be to expose so-called *data bleachers* – API functions that dynamically degrade the sensitivity of the shared data through aggregation or obfuscation – and enforce their usage for the generation of notifications or alerts for specific social circles.

Challenge 2: Usability issues for elderly. The end-users of smart home care systems have limited technical knowledge and experience with smart home technologies. Designing an effective and easy-to-use system interface that accounts for older users' physical and mental abilities, as well as their data privacy and security perceptions and preferences requires a significant research effort [8], [44], [45]. One potential research direction lies in exploring the capabilities of a smart and proactive voice assistant to setup and configure a smart home care system. Such an approach removes the technology barrier for the elderly and allows to interact with the system with voice commands in natural language.

Challenge 3: Third-party software security. Third-party software components of the hub, such as apps, have access to both sensor data and network resources which can result in sensitive data leaks. While various smart home systems have been previously reported to contain serious security and privacy vulnerabilities [22]–[24], the smart home care systems may suffer from the same issues. Therefore it is important to inspect and continuously monitor at runtime the smart care apps' activities when accessing and sharing sensitive sensor data. Combining both static and dynamic app code analysis can be a potential research direction.

Challenge 4: Resources management. Apps running side by side at the hub inevitably have to compete for the computing resources. To this end, there is a need for a mechanism to control the distribution of computing resources which ensures that apps processing critical or life-threatening events can always execute successfully and on time. Such a mechanism could be driven by a pre-defined policy instructing how resources should be prioritized between apps that process critical events and those that do not.

V. Conclusion

In this position paper we presented our vision for smart home care systems. We highlighted the requirements such a system must satisfy and explained why available smart home systems are unable to do so. As an alternative, we provided a high-level design overview of a smart home care system consisting of several key components: a set of sensor devices, a central hub for sensor data processing, and, finally, a number of social circles that may be notified about the health and well-being of a monitored person. We listed several challenges that we believe the scientific and industrial community will have to overcome when designing such a system and pointed out potential research directions.

Acknowledgments

This work was supported by the Brussels Institute for Research and Innovation (Innoviris) under project "Smart and Social Home Care".

References

[1] G. Carone, D. Costello, N. Diez Guardia, G. Mourre, B. Przywara, and A. Salomäki, "The economic impact of ageing populations in the EU25 member states," *Directorate general for economic and financial affairs European economy economic working paper*, 2005.

[2] U. Nations, "United nations department of economic and social affairs, population division. world population ageing 2015," *Online Edition UN DESA, New York*, 2015.

[3] S. Gomez-Cantarino, P. Dominguez-Isabel, B. Espina-Jerez, M. C. Bouzas-Mosquera, M. T. A. Ortuño, M. d. l. M. de Dios, M. C. R. F. Chaves *et al.*, "Formal and informal care: Home care in the elderly with obstructive sleep apnea," in *Noninvasive Ventilation Technologies and Healthcare for Geriatric Patients*, 2020.

[4] M. Lillo-Crespo and J. Riquelme, "From home care to care home: a phenomenological case study approach to examining the transition of older people to long-term care in spain," *Journal of Research in Nursing*, 2018.

[5] L. Bennett, M. Honeyman, and S. Bottery, "New models of home care," *London, UK: The King's Fund*, 2018.

[6] R. M. Compton, A. O. Owilli, V. Caine, C. Berendonk, D. Jouan-Tapp, S. Sommerfeldt, D. J. McPhee, and D. Walz, "Home first: exploring the impact of community-based home care for older adults and their family caregivers," *Canadian Journal on Aging*, 2020.

[7] S. Liao, "Samsung's SmartThings smart home hub has been down since yesterday for some users." [Online]. Available: https://www.theverge.com/circuitbreaker/2018/3/13/17115624

[8] A. Frik, L. Nurgalieva, J. Bernd, J. Lee, F. Schaub, and S. Egelman, "Privacy and security threat models and mitigation strategies of older adults," in *Proc. of SOUPS*, 2019.

[9] E. Commission, "General data protection regulation art. 5: Principles relating to processing of personal data." [Online]. Available: https://gdpr-info.eu/art-5-gdpr/

[10] S. of California, "Senate bill no. 1121: California consumer privacy act." [Online]. Available: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1121

[11] M. S. Ardekani, R. P. Singh, N. Agrawal, D. B. Terry, and R. O. Suminto, "Rivulet: A fault-tolerant platform for smart-home applications," in *Proc. of USENIX Middleware*, 2017.

[12] A. Sengupta, T. Leesatapornwongsa, M. S. Ardekani, and C. A. Stuardo, "Transactuations: where transactions meet the physical world," in *Proc. of USENIX ATC*, 2019.

[13] C. Dixon, R. Mahajan, S. Agarwal, A. Brush, B. Lee, S. Saroiu, and P. Bahl, "An operating system for the home," in *Proc. of NSDI*, 2012.

[14] D. Retkowitz and S. Kulle, "Dependency management in smart homes," in *Proc. of DAIS*, 2009.

[15] S. B. Ahsan, R. Yang, S. A. Noghabi, and I. Gupta, "Home, safehome: smart home reliability with visibility and atomicity," in *Proc. of EuroSys*, 2021.

[16] S. Mare, L. Girvin, F. Roesner, and T. Kohno, "Consumer smart homes: Where we are and where we need to go," in *Proc. of HotMobile*, 2019.

[17] Y. Chen, X. Yuan, J. Zhang, Y. Zhao, S. Zhang, K. Chen, and X. Wang, "Devil's whisper: A general approach for physical adversarial attacks against commercial black-box speech recognition devices," in *Proc. of USENIX Security*, 2020.

[18] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis *et al.*, "Understanding the Mirai botnet," in *Proc. of USENIX Security*, 2017.

[19] E. Ronen, A. Shamir, A.-O. Weingarten, and C. O'Flynn, "IoT goes nuclear: Creating a ZigBee chain reaction," in *Proc. of IEEE S&P*, 2017.

[20] P. Morgner, S. Mattejat, Z. Benenson, C. Müller, and F. Armknecht, "Insecure to the touch: attacking ZigBee 3.0 via touchlink commissioning," in *Proc. of WiSec*, 2017.

[21] W. Wang, F. Cicala, S. R. Hussain, E. Bertino, and N. Li, "Analyzing the attack landscape of Zigbee-enabled IoT systems and reinstating users' privacy," in *Proc. of WiSec*, 2020.

[22] E. Fernandes, J. Jung, and A. Prakash, "Security analysis of emerging smart home applications," in *Proc. of IEEE S&P*, 2016.

[23] E. Fernandes, J. Paupore, A. Rahmati, D. Simionato, M. Conti, and A. Prakash, "Flowfence: Practical data protection for emerging iot application frameworks," in *Proc. of USENIX Security*, 2016.

[24] Z. B. Celik, L. Babun, A. K. Sikder, H. Aksu, G. Tan, P. McDaniel, and A. S. Uluagac, "Sensitive information tracking in commodity IoT," in *Proc. of USENIX Security*, 2018.

[25] Z. B. Celik, P. McDaniel, and G. Tan, "Soteria: Automated IoT Safety and Security Analysis," in *Proc. of ATC*, 2018.

[26] Z. B. Celik, G. Tan, and P. McDaniel, "IoTGuard: Dynamic Enforcement of Security and Safety Policy in Commodity IoT," in *Proc. of NDSS*, 2019.

[27] Y. J. Jia, Q. A. Chen, S. Wang, A. Rahmati, E. Fernandes, Z. M. Mao, and A. Prakash, "ContexIoT: Towards providing contextual integrity to appified iot platforms." in *Proc. of NDSS*, 2017.

[28] E. Fernandes, A. Rahmati, J. Jung, and A. Prakash, "Decoupled-IFTTT: Constraining privilege in trigger-action platforms for the internet of things," *arXiv preprint arXiv:1707.00405*, 2017.

[29] E. Fernandes, A. Rahmati, and J. Jung, "Decentralized action integrity for trigger-action IoT platforms." in *Proc. of NDSS*, 2018.

[30] W. He, M. Golla, R. Padhi, J. Ofek, M. Dürmuth, E. Fernandes, and B. Ur, "Rethinking access control and authentication for the home internet of things (IoT)," in *Proc. of USENIX Security*, 2018.

[31] H. Chi, Q. Zeng, X. Du, and L. Luo, "Pfirewall: Semantics-aware customizable data flow control for home automation systems," in *Proc. of NDSS*, 2021.

[32] E. J. Coyne, H. Feinstein, R. Sandhu, and C. E. Youman, "Role-based access control models," *IEEE Computer*, 1996.

[33] P. Samarati and S. C. de Vimercati, "Access control: Policies, models, and mechanisms," in *Proc. of FOSAD*, 2000.

[34] Y. Zhu, D. Huang, C.-J. Hu, and X. Wang, "From RBAC to ABAC: constructing flexible data access control for cloud storage services," *IEEE Transactions on Services Computing*, 2014.

[35] G. Batra, V. Atluri, J. Vaidya, and S. Sural, "Enabling the deployment of ABAC policies in RBAC systems," in *Proc. of DBSec*, 2018.

[36] M. Yahyazadeh, P. Podder, E. Hoque, and O. Chowdhury, "Expat: Expectation-based policy analysis and enforcement for appified smart-home platforms," in *Proc. of SACMAT*, 2019.

[37] Y. Tian, N. Zhang, Y.-H. Lin, X. Wang, B. Ur, X. Guo, and P. Tague, "Smartauth: User-centered authorization for the internet of things," in *Proc. of USENIX Security*, 2017.

[38] W. Ding and H. Hu, "On the safety of IoT device physical interaction control," in *Proc. of CCS*, 2018.

[39] D. Hornung, C. Müller, I. Shklovski, T. Jakobi, and V. Wulf, "Navigating relationships and boundaries: Concerns around ict-uptake for elderly people," in *Proc. of CHI*, 2017.

[40] B. Knowles and V. L. Hanson, "Older adults' deployment of 'distrust'," *ACM Transactions on Computer-Human Interaction (TOCHI)*, 2018.

[41] R. de Podestá Gaspar, R. Bonacin, and V. P. Gonçalves, "Designing iot solutions for elderly home care: a systematic study of participatory design, personas and semiotics," in *Proc. of UAHCI*, 2018.

[42] T. Carpenter, J. Hatcliff, and E. Y. Vasserman, "A reference separation architecture for mixed-criticality medical and IoT devices," in *Proc. of SafeThings*, 2017.

[43] J. Takalo-Mattila, J. Kiljander, F. Pramudianto, and E. Ferrera, "Architecture for mixed criticality resource management in internet of things," in *Proc. of TRON*, 2014.

[44] A. Olwal, D. Lachanas, and E. Zacharouli, "Oldgen: Mobile phone personalization for older adults," in *Proc. of SIGCHI*, 2011.

[45] J. Hayes, S. Kaushik, C. E. Price, and Y. Wang, "Cooperative privacy and security: Learning from people with visual impairments and their allies," in *Proc. of SOUPS*, 2019.