ELEKTROTEHNIŠKI VESTNIK 86(5): 267–273, 2019
ORIGINAL SCIENTIFIC PAPER

Adoption of smarthome devices: Blinded by benefits, ignoring the dangers?

Egzona Lutolli[1], **Simon L. R. Vrhovec**[1,*]

[1] *University of Maribor, Faculty of Criminal Justice and Security*
Kotnikova 8, 1000 Ljubljana, Slovenia

[*] *E-mail: simon.vrhovec@um.si*

Abstract. Smarthomes aim to facilitate everyday tasks of their residents. To achieve this, a substantial amount of data is being collected and analyzed in smarthome systems. Smarthomes are comprised of a myriad of individual smart devices (e.g., sensors, home appliances), control centers (e.g., smart TVs) and even systems (e.g., cooling system). Since these devices are connected to the internet (e.g., for remote management through mobile apps integrated into a manufacturer's cloud), they are threatened by cyberattacks and other dangers to security and privacy of smarthome residents. In the paper we try to determine which factors influence the adoption of smarthomes. A survey is conducted among internet users using convenience sampling (N = 120). Findings suggest that the use of smart devices is associated with benefits and knowledge of smarthomes but not with the perceived dangers nor presence of smarthomes. A probable explanation is that the benefits of smarthomes outweigh their dangers when individuals are deciding to adopt them.

Keywords: smart home, internet of things, IoT, cyber security, cybersecurity, privacy, adoption, acceptance, use

Sprejemanje naprav v pametnih domovih: Zaslepljenost s koristmi, ignoriranje nevarnosti?

Cilj pametnih domov je olajšati vsakodnevna opravila stanovalcev. Da bi to dosegli, se v sistemih pametnih domov zbira in analizira velika količina podatkov. Pametne domove sestavljajo številne posamezne pametne naprave (npr. senzorji, gospodinjski aparati), nadzorni centri (npr. pametni televizorji) in celo sistemi (npr. hladilni sistem). Ker so te naprave povezane z internetom (npr. za oddaljeno upravljanje prek mobilnih aplikacij, integriranih v proizvajalčev oblak), jim grozijo kibernetski napadi ter druge nevarnosti za varnost in zasebnost stanovalcev v pametnih domovih. V prispevku poskušamo ugotoviti, kateri dejavniki vplivajo na sprejemanje pametnih domov. Med uporabniki interneta je bila izvedena anketa z uporabo priročnega vzorčenja (N = 120). Ugotovitve nakazujejo na to, da je uporaba pametnih naprav povezana s koristmi in poznavanjem pametnih domov, ne pa tudi z zaznanimi nevarnostmi ali prisotnostjo pametnih domov. Verjetna razlaga je, da koristi pametnih domov prevladajo nad njihovimi nevarnostmi, ko se posamezniki odločajo za njihovo sprejemanje.

1 INTRODUCTION

Automation of home systems dates back to 1975 when the Scottish company Pico Electronic developed a special solution that allowed devices to communicate over the electrical network at homes. At that time, devices made it possible to simply switch off lights in another room using the code number that the transmitter communicated to the receiver. Today, one can communicate with cameras, motion sensors and other devices facilitating and simplifying their everyday tasks through an internet connection, e.g., by using smart phones [1]. Smarthomes are equipped with smart devices, such as sensors and transmitters, that collect and analyze data in order to be able to respond to a changing situation at home [2]. They enable residents to remotely monitor and control their homes as well as automatically adjust the living conditions according to the situation (e.g., adjusting heating and lighting for late-night visitors). Due to their ability to facilitate everyday tasks, smarthomes are also important for people with disabilities, limited mobility and other limitations [3].

Besides various benefits, smarthomes also pose various dangers to their residents. Smarthome devices process and store a significant amount of data of smarthome residents' everyday activities and routines. Since this data is typically sent to providers of smarthome devices, this gives them an insight into the privacy of smarthome residents. Besides, smarthome devices may lack the needed security mechanisms that would ensure adequate data protection due to their limited capabilities (e.g., battery life, processing power). Smarthome devices are also exposed to cyberthreats, such as hacker intrusions or malware infections, due to their connection to the internet [4].

Smarthomes are being gradually adopted and little

Received 8 August 2019
Accepted 25 November 2019

research has been done on the security- and privacy-related factors affecting it. In this paper, we try to address this gap by focusing on factors affecting the adoption of smarthome devices. In particular, we study how the perceived benefits and threats of smarthome devices affect their adoption and how the knowledge and the perceived presence of smarthomes contribute to adoption of smarthome devices.

The paper is structured as follows. Section 2 presents smarthomes and the related research. Section 3 develops a research model. Section 4 presents research methods. Section 5 presents results of a survey data analysis. Section 6 discusses the results, draws conclusions and gives suggestions for the future work.

2 Theoretical Background

In this section, we first define and present smarthomes focusing on their relation to smart devices. Then, we discuss the smarthome benefits and threats to both smarthomes and their residents.

2.1 Smarthomes

The rapid development of the internet of things and smart devices has led to a boom in a variety of applications in smart systems in which people and things are interconnected [5]. The great deployment of communication networks, increased availability of networked sensors, and data analysis tools have enabled the emergence of smart systems, such as smart health, smart agro, smart transportation, smart cities, smart buildings, smarthomes and others [5], [6], [7], [8], [9], [10].

A home needs to fit three basic criteria to be considered as a *smarthome* [11], [12]. First, it needs to have an internal network of any kind (e.g., wired, wireless, cable) [11], [12]. Next, it needs to enable intelligent monitoring of devices connected to the internal network [11], [12]. Finally, it needs to enable home automation (i.e., control of electronic devices with a lowered human interaction) [11], [12]. Additionally, it can include internal sensor systems that provide residents the ability to monitor, control and remotely manage a smarthome by accessing smart devices from anywhere in the world [13]. One of the goals of smarthomes may therefore be to provide the owners the ability to control a smarthome no matter where they are located [14].

Smarthomes are made up of devices capable of communicating with each other, thus forming an interconnected ecosystem. It comprises of a set of a connected evolving technology and intelligent systems with technologically demanding functions, such as voice management. Smarthomes may be operated through mobile applications and devices that typically enable an access to individual smarthome devices, a central unit, such as smart TV or smart fridge, or dedicated interfaces (e.g., on the wall) [2]. Smarthomes increasingly include smaller smart devices that make it easier for a user to manage the day-to-day tasks. Their use is simplified if they are connected to a common system that independently manages them. In order not to overload the residents with micromanaging smarthomes, management of smarthome devices is being increasingly automated with the use of artificial intelligence, and machine learning in particular. Individual smarthome devices therefore provide comfort, security, energy efficiency, etc., and smarthomes as smart systems learn residents' preferences and adapt to them [13], [15]. Smarthomes can be set up for a fully independent operation, direct user interaction or a combination of both [16].

With the aging population, the human resources and space needed for providing adequate healthcare are becoming scarce. Smarthomes may help find ways that would enable the elderly and people with disabilities a more independent life while preserving and perhaps even enhancing the level of provided healthcare service [17]. Smarthomes may be integrated with smart hospitals which aim to expand the boundaries of classical hospitals. For example, smart devices for automatic monitoring of health and remote administering of medications may help transform smarthomes into an extension of a smart hospital. Smarthomes may provide a better quality of life for the elderly, patients and people with disabilities just because they would be located in the home environment. These kinds of systems include a technology that allows, for example, automatic illumination of the light with the motion sensor, control of the blinds, changing of the room temperature, opening and closing doors and windows, etc. [18].

There are several ways to construct a smarthome. Smarthomes can be either new buildings with a standardized base system and optional additional components according to the requirements of the owner, or existing buildings that have been subsequently upgraded (e.g., during reconstruction, installation of a smart system) [12]. In principle, preplanned smarthomes tend to be more homogeneous. This is however rarely the case due to the rapid evolution of technologies used in smarthomes. Already during the construction of a smarthome, some of the planned smarthome devices or technologies may become outdated (e.g., cable-connected devices). This is even more evident afterwards as smarthomes are being used for decades after construction. Therefore, we can consider smarthomes as heterogeneous smart systems which are composed of devices from different manufacturers, capabilities, and eras.

Since smarthome devices are often lacking adequate security mechanisms, attempts have been made to transfer security to the entire system level and not just individual devices [19]. Various kinds of protocols for se-

curing communications aim to provide the data integrity and privacy [20], [21]. Although the use of cryptography is highly encouraged, there are severe obstacles to its adoption due to poor specifications of a high share of smarthome devices [22]. Residents may help secure smarthomes up to a certain point with certain security measures, such as regularly updating smart devices and systems, backing up data, using antivirus solutions, etc. [23], [24], [25], [26]. This may be however hindered by factors that residents have no control over, e.g., if the device manufacturer does not provide updates, goes out of business, does not have a privacy-friendly data policy, etc.

2.2 Dangers of smarthomes

Smart devices collect and store huge volumes of data [27], [28]. Devices that are directly connected to the internet are most at risk as they are exposed to cyberattacks although the heterogeneity of smart systems widens the attack surface [29], [28]. Even though cyberattacks were recently more or less associated only with the theft and misuse of data, a cyberattack on a smarthome device or system may cause a material damage in the real world, personal injury or even death (e.g., disabling a carbon monoxide monitor in the garage). In addition to cyberattacks, there are also other threats to smarthomes such as the ones presented below [30].

Physical attacks. These attacks are related to having a physical access to smarthome devices, such as the destruction and theft of smarthome devices, relocation or removal from their original location, direct infection with malware and extraction of stored data [31].

Catastrophes. Catastrophes are divided into *natural disasters* (e.g., earthquakes, floods, avalanches) which are consequences of natural forces and are devastating to people and the infrastructure, and *environmental catastrophes* (e.g., fires, explosions, releases of toxic substances). A smarthome can be threatened just by its location (e.g., floods). Catastrophes may lead to losing communication links with and within a smarthome which causes a full smarthome failure.

Eavesdropping and interception. Smarthome devices often use wireless communication which enables anyone with a good enough receiver to eavesdrop and intercept it. Since wireless communication is often not encrypted, attackers may pick up sensitive data that can be later misused (e.g., for planning an intrusion into a smarthome when its residents are away, blackmailing the residents) [32], [33].

Unintentional and accidental damages. Complex sensor networks in smarthomes collect sensitive data about residents and could disclose more data than residents would want to disclose. Not using an adequate security software and communication encryption or failing to appropriately configure it increases the probability of accidental data leaks. The number of connections to external servers also increases (i.e., multiplies) the possibility of data leaks [34].

Sensitive data loss. A vast amount of sensitive data is collected and stored in smarthomes. This poses a variety of threats that result in leaking sensitive data due to various reasons from intrusions and malware infections to smarthome device manufacturers selling this data, e.g., for advertising purposes. These leaks may have serious consequences for smarthome residents if misused [2].

Loss and destruction of devices, media and documents. Although the information security and privacy best practices prescribe personal and sensitive data to be encrypted at rest, this is rarely the case. Data breaches may therefore still occur, e.g., when a smarthome device is stolen or lost. If remote data wiping is enabled, the procedure needs to be performed as soon as possible after an incident has been detected. Data also needs to be wiped before selling or disposing of a smarthome device to prevent unwanted data retrieval [35].

Faults and errors. Smarthomes are complex systems that depend on many different devices and are therefore exposed to a variety of faults and errors that are considered one of the best entry points for attackers. Identifying and exploiting these weaknesses represent the first steps towards eavesdropping, intercepting and acquiring sensitive data [34], [36]. Errors may also occur due to poor maintenance, failure of interfaces or unintended cut of fiber optics [37]. Consequently, the data flow may be impaired and some data may be lost.

Outages. Communication may be interrupted or broken down due to various reasons, such as power outages, failures of the local network or issues with the internet connectivity.

Misuse. Misuse stems from the continuous availability and integration of smarthome devices into information networks, and collecting and analyzing data from devices that enable management of devices in the real world [38]. For example, entertainment devices can collect audio and video data and share intimate data with others [39].

Cyberattacks. These attacks comprise all attacks taking advantage of the cyberspace. Smarthome devices may not only be targets of cyberattacks (e.g., malware that deliberately causes a physical damage or targets a certain function) but may also be used to attack others (e.g., distributed denial-of-service (DDoS) attacks) [40], [41].

3 Research Model

In this section we present a developed research model shown in Figure 1.

People consider the benefits of things before using them. Benefits of smarthome devices may vary for different people. For example, automatic lighting may

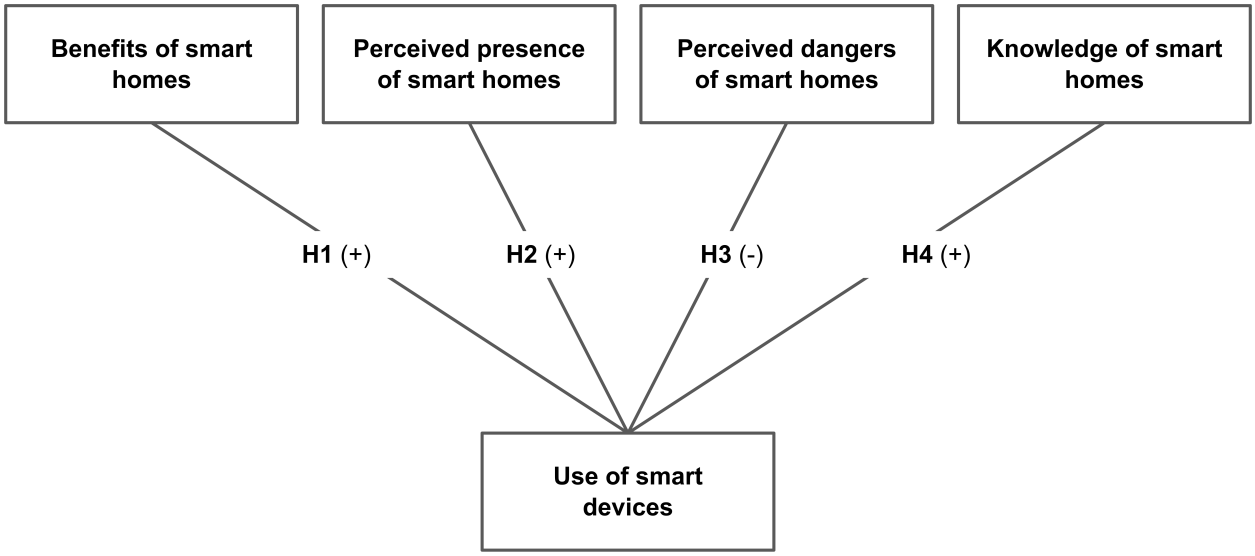

Figure 1. Research model.

be considered a benefit for some people but a drawback for others who prefer to use a standard light switch. Adoption of smarthome devices may therefore be affected by their perceived benefits. We thus propose the following hypothesis:

Hypothesis H1: The perceived smarthome benefits are positively correlated with the use of smart devices.

The technology adoption life cycle indicates several groups of people according to when they decide to adopt new technology: innovators, early adopters, early majority, late majority and laggards. The more widely used a certain technology is perceived to be by people, the more likely it will be used by them. Therefore, we propose the next hypothesis:

Hypothesis H2: The perceived smarthome presence is positively correlated with the use of smart devices.

Adoption may be hindered if people perceive the new technology being adopted as dangerous. In this paper, dangerous is defined as posing a threat to smarthome residents either by invading their privacy or by simply being insecure and prone to exploiting. Based on these assumptions, we suggest the following hypothesis:

Hypothesis H3: The perceived smarthome dangers are negatively correlated with the use of smart devices.

People may want to learn more about the new technology that they adopt or aim to do so. Since people who are more knowledgeable about smarthomes are more inclined to use smarthome devices, we propose our final hypothesis:

Hypothesis H4: The knowledge of smarthomes is positively correlated with the use of smart devices.

4 METHODS

To test our hypotheses, we conducted an online survey among internet users. Invitations for taking part in the survey were distributed through e-mail and Facebook. A total of 120 respondents completed the survey. The demographic characteristics of the respondents are given in Table 1.

The survey questionnaire was designed to measure five constructs: benefits of smarthomes (Benefits), perceived presence of smarthomes (Presence), perceived dangers of smarthomes (Dangers), knowledge of smarthomes (Knowledge), and use of smart devices (Use). The survey items were self–developed for the research. Each construct consisted of three survey items. All items were measured using a five-point Likert scale from 1 (I strongly disagree) to 5 (I strongly agree).

The reliability of the questionnaire was assessed by using the Cronbach's alpha (CA) coefficient. The CA values range from 0 to 1 and the higher values generally mean a better reliability. The acceptable values range from 0.60 to 0.95 with the preferred values above 0.70. The values exceeding 0.95 suggest that items are too similar to each other. If the CA values fall below or above the recommended thresholds, the reliability may be improved by excluding individual items.

Table 1. Demographic characteristics

Characteristic	N	Percent
Gender		
Male	33	27.5
Female	75	62.5
Not specified	12	10.0
Age		
16–25 years	96	80.0
26–35 years	9	7.5
46–55 years	3	2.5
Not specified	12	10.0
Education		
Less than bachelor's degree	50	41.7
Bachelor's degree	54	45.0
Master's degree	3	2.5
Not specified	13	10.8
Living area		
Rural	31	25.8
Urban	77	64.2
Not specified	12	10.0

Table 2. Reliability analysis (Cronbach's alpha = CA).

Construct	CA
Benefits of smarthomes	0.750
Perceived presence of smarthomes	0.708
Perceived dangers of smarthomes	0.584
Knowledge of smarthomes	0.649
Use of smart devices	0.658

5 RESULTS

The research instrument was first validated by calculating CA for each construct. In our study, the CA values for Benefits, Knowledge and Use were above the 0.60 threshold. CA for Presence and Dangers were 0.244 and 0.486, respectively. Therefore, we considered excluding individual items from both constructs. After excluding Presence1, CA for Presence increased to 0.708. We therefore decided to exclude it from further analysis. Similarly, CA for Dangers increased to 0.584 after excluding Dangers2. Since CA was very close to the threshold value of 0.60 and significantly above the threshold value of 0.4 for exploratory studies (e.g., surveys with newly developed items), we decided to keep Dangers1 and Dangers3 for further analysis. The results of reliability analysis after excluding Presence1 and Dangers2 from our analysis are presented in Table 2.

Next, we aggregated items into construct variables and tested the new variables for normality. Since all construct variables appeared to follow the normal distribution, we calculated the Pearson's correlation coefficients to test the hypotheses. The results are shown in Figure 2.

There is a strong positive statistically significant ($p < 0.001$) correlation between Benefits and Use supporting hypothesis **H1**. Next, the correlations between Presence and Dangers, and Use are not statistically significant. Therefore, we cannot neither confirm nor reject hypotheses **H2** and **H3**. Finally, there is a statistically significant ($p < 0.05$) positive correlation between Knowledge and Use supporting hypothesis **H4**.

6 DISCUSSION AND CONCLUSION

In the paper, we study which factors affect the adoption of smarthomes. Even though this is an exploratory study, several implications can be provided as well as directions for future research. First, we confirm our assumption that the perceived benefits affect adoption of smarthomes. This is in line with the well-established research on adoption of new technologies that consistently associate usefulness and behavioral intentions to use new technology.

Next, we also confirm our assumption that knowledge of smarthomes is associated with their use. However, we do not study whether respondents are knowledgeable because of adoption or are more inclining to adopt because of their knowledge of smarthomes. Our future work will focus on the causal relationship between these two constructs, e.g., by employing qualitative research methods or longitudinal studies.

Our study shows no association between the perceived presence of smarthomes and their use. This may suggest that the respondents do not consider the presence when adopting smarthome devices. Including descriptive norms (i.e., what the respondents believe the others are doing) may be considered in future research to determine whether there is some kind of social influence on adoption as recent research suggests.

Finally, it appears that the respondents do not consider strongly the perceived dangers of smarthomes when adopting them. This non-finding appears to be quite puzzling and various explanations can be provided. For example, the respondents might simply ignore the dangers when adopting smarthomes because of the benefits provided by them. Alternatively, a significant share of the respondents may not be aware of the dangers of smarthomes influencing the results. Studying the determinants of the perceived dangers may be highly beneficial in solving this puzzle.

As with any other exploratory research, this study has a number of limitations that the readers should note. First, convenience sampling (i.e., a non-probability sampling technique) is employed which substantially affects the generalizability of the findings. Future research employing random sampling may be needed to further validate the findings of this study. Next, the respondents are mostly young people who most likely use internet

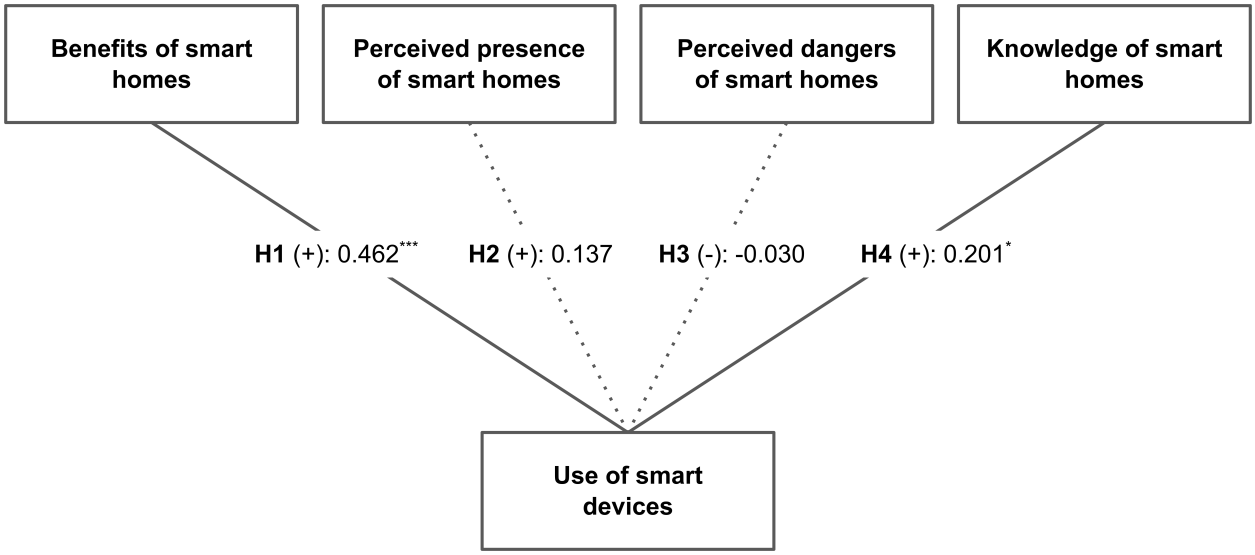

Figure 2. Hypotheses testing results ($^{*}p < 0.05, ^{**}p < 0.01, ^{***}p < 0.001$).

frequently though smarthomes are also intended for the elderly and the disabled. Future research targeting them through different communication channels (e.g., face-to-face or land phone lines) would be beneficial. Finally, the survey instrument is newly developed for this particular research. Further validation and extension of the survey instrument may be needed to improve its reliability and validity.

Smarthomes are quickly developing and are being used by an increasing number of people. It is hard to draw a clear line between a non-smart and a smarthome as more and more smart devices are being developed covering more and more of our everyday needs. For example, is a smart phone part of a smarthome or not – the difference may be a single mobile application that lets a smarthome resident check what is available in a fridge while shopping. With the increasing number of interconnected devices comprising smarthomes and their inherently questionable security and privacy, a strong focus should be put on providing smarthome residents with the same degree of privacy and security as they expect from the non-smart homes.

REFERENCES

[1] M. Edmonds, "How Smart Homes Work," 2008. [Online]. Available: http://home.howstuffworks.com/smart-home.htm

[2] C. Wilson, T. Hargreaves, and R. Hauxwell-Baldwin, "Benefits and risks of smart home technologies," *Energy Policy*, vol. 103, pp. 72–83, 2017.

[3] G. Demiris and B. K. Hensel, "Technologies for an Aging Society: A Systematic Review of "Smart Home" Applications," *Yearbook of Medical Informatics*, vol. 17, no. 01, pp. 33–40, 2008.

[4] H. Lin and N. W. Bergmann, "IoT privacy and security challenges for smart home environments," *Information (Switzerland)*, vol. 7, no. 3, 2016.

[5] D. Alulema, J. Criado, and L. Iribarne, "A Cross-Device Architecture for Modelling Authentication Features in IoT Applications," *Journal of Universal Computer Science*, vol. 24, no. 12, pp. 1758–1775, 2018.

[6] R. Souza, J. Lopes, C. Geyer, A. Cardozo, A. Yamin, and J. Barbosa, "An Architecture for IoT Management Targeted to Context Awareness of Ubiquitous Applications," *Journal of Universal Computer Science*, vol. 24, no. 10, pp. 1452–1471, 2018.

[7] C.-Y. Lin, K.-H. Liao, and C.-H. Chang, "An Experimental System for MQTT/CoAP-based IoT Applications in IPv6 over Bluetooth Low Energy," *Journal of Universal Computer Science*, vol. 24, no. 9, pp. 1170–1191, 2018.

[8] A. Sebastian and S. Sivagurunathan, "Multi DODAGs in RPL for Reliable Smart City IoT," *Journal of Cyber Security and Mobility*, vol. 7, no. 1, pp. 69–86, 2018.

[9] D. Žagar, "Avtonomna plovila in bodoča vloga posadke / Unmanned ships and future role of crew members," *Elektrotehniški vestnik / Electrotechnical Review*, vol. 85, no. 1-2, pp. 69–74, 2018.

[10] E. M. Ghourab, E. Samir, M. Azab, and M. Eltoweissy, "Trustworthy Vehicular CommunicationEmploying Multidimensional Diversificationfor Moving-target Defense," *Journal of Cyber Security and Mobility*, vol. 8, no. 2, pp. 133–164, 2018.

[11] V. S. Gunge and P. S. Yalagi, "Smart Home Automation: A Literature Review," *International Journal of Computer Applications*, pp. 975–8887, 2016.

[12] N. King, "Smart Home – a Definition," *Health (San Francisco)*, pp. 1–6, 2003.

[13] M. Kumar, A. Basu, S. Dass, and S. Kumar, "Technical report M2M/IoT enablement in Smart Homes," Ministry of Communications, Government of India, Tech. Rep., 2017.

[14] A. S. Dicarlo, "Smart Homes–home automation," in *Livable New York*. New York State Office for the Aging, 2011, pp. 1–8.

[15] Univerza v Ljubljani, "Seminar: Inteligentne Hiše," 2002. [Online]. Available: http://luks.fe.uni-lj.si/sl/studij/SUIS/seminarji/nartnikm/

[16] B. Kerbel, "Pametni dom za samostojno in kakovostno bivanje starejših ljudi," *AR Arhitektura, raziskave*, no. 2, pp. 15–22, 2011.

[17] A. Reissner, "Nove tehnologije kot pomoč starejšim," ZDUS, Tech. Rep., 2012.

[18] M. Kušar, "Mnenje uporabnika: Napredne rešitve za lažje bivanje," 2017. [Online]. Available: http://www.rtvslo.si/dostopno/novica/726

[19] P. Rubens, *The Do-It-Yourself Security Audit*. Jupitermedia, 2008.
[20] T. Mendes, R. Godina, E. Rodrigues, J. Matias, and J. Catalão, "Smart Home Communication Technologies and Applications: Wireless Protocol Assessment for Home Area Network Resources," *Energies*, vol. 8, no. 7, pp. 7279–7311, jul 2015.
[21] J. Bugeja, A. Jacobsson, and P. Davidsson, "On Privacy and Security Challenges in Smart Connected Homes," in *2016 European Intelligence and Security Informatics Conference (EISIC)*. IEEE, aug 2016, pp. 172–175.
[22] Synopsys, "Cryptography," 2019. [Online]. Available: https://www.synopsys.com/software-integrity/resources/knowledge-database/cryptography.html
[23] N. Lord, "101 Data Protection Tips: How to Keep Your Passwords, Financial & Personal Information Safe in 2019," 2019. [Online]. Available: https://digitalguardian.com/blog/101-data-protection-tips-how-keep-your-passwords-financial-personal-information-safe
[24] C. Howard, "Clark Howard: Free virus, spyware and malware protection guide," 2019. [Online]. Available: https://clark.com/technology/clark-howards-virus-spyware-and-malware-protection/
[25] Privacy Rights Clearinghouse, "Securing Your Computer to Maintain Your Privacy," 2018. [Online]. Available: https://www.privacyrights.org/consumer-guides/securing-your-computer-maintain-your-privacy
[26] Federal Communications Commission, "Cybersecurity for Small Business," 2019. [Online]. Available: https://www.fcc.gov/general/cybersecurity-small-business
[27] P. I. Shah, P. A. Shah, S. Yasmin, Z. Ur-Rehman, A. Ahmad, Y. Nam, and S. Rho, "Crumbling Walls Log Quorum System-based Name Resolution Routing for CCN based IoT," *Journal of Universal Computer Science*, vol. 24, no. 9, pp. 1282–1305, 2018.
[28] M. Sepehri, A. Trombetta, and M. Sepehri, "Secure Data Sharing in Cloud Usingan Efficient Inner-Product ProxyRe-Encryption Scheme," *Journal of Cyber Security and Mobility*, vol. 6, no. 3, pp. 339–378, 2018.
[29] S. Prabavathy, K. Sundarakantham, and S. M. Shalinie, "Design of Cognitive Fog Computing for Autonomic Security System in Critical Infrastructure," *Journal of Universal Computer Science*, vol. 24, no. 5, pp. 577–602, 2018.
[30] H. M. O'Brien, "The Impact of the Smart Home Revolution on Product Liability and Fire Cause Determinations," Wilson Elser, Tech. Rep., 2016.
[31] D. Desai and H. Upadhyay, "Security and Privacy Consideration for Internet of Things in Smart Home Environments," *International Journal of Engineering Research and Development*, vol. 10, no. 11, pp. 73–83, 2014.
[32] R. Eržen, "Review of main security threats in Smart Home networks," Mednarodna podiplomska šola Jožefa Štefana, Tech. Rep., 2012.
[33] BSI Standards, "Threats Catalogue - Elementary Threats," British Standards Institution, Tech. Rep., 2012.
[34] E. C. Damiani, C. A. C. Ardagna, F. C. Zavatarelli, E. E. Rekleitis, and L. E. Marinos, *Big Data Threat Landscape and Good Practice Guide Big Data Threat Landscape and Good Practice Guide About ENISA Big Data Threat Landscape and Good Practice Guide*. ENISA, 2015.
[35] Government of Ontario, *Disposal, Loss and Incident Reporting of Computerized Devices & Digital Storage Media*. Government of Ontario, 2014.
[36] C. Lévy-Bencheton and G. Dufay, *Security and Resilience of Smart Home Environments*. ENISA, 2015.
[37] S. Nelakuditi, S. Lee, Y. Yu, Z. L. Zhang, and C. N. Chuah, "Fast local rerouting for handling transient link failures," *IEEE/ACM Transactions on Networking*, vol. 15, no. 2, pp. 359–372, 2007.
[38] L. Toms, "Data And Identity Theft in the IoT," 2016. [Online]. Available: https://www.globalsign.com/en/blog/identity-theft-in-the-iot
[39] K. Irkal and S. Irkal, "Identity theft and protection using IoT," *International Journal of Innovative Research in Science, Engineering and Technology*, vol. 6, no. 12, pp. 97–100, 2017.
[40] S. Kodra, "Smart Home Hacking," Ph.D. dissertation, University of Tartu, 2016.
[41] W. E. Wong and V. Debroy, "Malicious Code," *IEEE Transactions on Reliability*, vol. 58, no. 2, pp. 249–251, 2009.

Egzona Lutolli received her B.Sc. degree in Information Security from the University of Maribor in 2018. Her research interests are in security of advanced technology, human-computer interaction, healthcare service.

Simon L. R. Vrhovec is an Assistant Professor at the University of Maribor. He received his PhD degree in Computer and Information Science from the University of Ljubljana in 2015. He co-chaired the Central European Cybersecurity Conference (CECC) in 2018 and 2019. His research interests are in human factors in cybersecurity, agile methods and secure software development, resistance to change, and medical informatics.