Journal of Cybersecurity and Privacy

MDPI

Article

Security Perception of IoT Devices in Smart Homes

Lili Nemec Zlatolas *, Nataša Feher and Marko Hölbl

Faculty of Electrical Engineering and Computer Science, University of Maribor, 2000 Maribor, Slovenia; natasa.feher@student.um.si (N.F.); marko.holbl@um.si (M.H.)
* Correspondence: lili.nemeczlatolas@um.si

Abstract: IoT devices are used frequently in smart homes. To better understand how users perceive the security of IoT devices in their smart homes, a model was developed and tested with multiple linear regression. A total of 306 participants participated in the survey with measurement items, out of which 121 had already been using IoT devices in their smart homes. The results show that users' awareness of data breaches, ransomware attacks, personal information access breaches, and device vulnerabilities have an effect on IoT security importance. On the other hand, users often do not check their security settings and feel safe while using IoT devices. This paper provides an overview of users' perception of security while using IoT devices, and can help developers build better devices and help raise awareness of security among users.

Keywords: IoT; smart homes; security; privacy

Citation: Nemec Zlatolas, L.; Feher, N.; Hölbl, M. Security Perception of IoT Devices in Smart Homes. *J. Cybersecur. Priv.* **2022**, *2*, 65–73. https://doi.org/10.3390/jcp2010005

Academic Editors: Savio Sciancalepore, Giuseppe Piro and Nicola Zannone

Received: 12 January 2022
Accepted: 11 February 2022
Published: 14 February 2022

1. Introduction

Smart homes have been increasing in recent decades and refer to residences that allow devices connected to the Internet to manage and monitor appliances and systems at the residence. These devices are equipped with sensors that include software and process data and are referred to as the Internet of Things (IoT). Smart home devices were first used as a sort of remote on and off button but have evolved into devices that can control our homes according to predefined patterns or as required by the user [1].

Smart home architecture can be divided into three layers [2]: the Perception layer, the Network layer, and the Application layer. The Perception layer is responsible for collecting data gathered using physical devices. The collected data must then be transferred to the processing unit or application, and this is the responsibility of the Network layer. Finally, data reach the application via an interface entirely dependent on the end-user. The most common example of this interface is a smartphone or tablet. These layers could also be extended by privacy and security components [3].

Smart home devices are usually connected online and can, for instance, be controlled over an application on the phone. Although this is very comfortable for the user and can lower costs, it can also impose vulnerabilities. The users can usually also control and manage the security of these devices via a phone or desktop application.

Users are concerned about hackers, who can infiltrate smart devices and thereby cause damage, such as unlocking doors without permission or gaining insight into one's private life through cameras. Affordability is also a problem, as smart technologies can require significant amounts of money to install [2,4].

As part of our study, we conducted a survey on user habits regarding the configuration of smart devices and their use. In the survey, we included groups of the most used smart devices, which include:

1. A smart refrigerator (detects types of products (and their quantities and expiry dates), compiles shopping lists, and generates recipes based on the ingredients currently available);

2. Automatic A/C or heating systems (appliances can be switched on or off remotely, controlling energy consumption and thus providing the possibility to optimize and reduce costs);
3. Smart assistants (e.g., Google Home or Alexa, which are voice-controlled and allow users to search, find information, answer phone calls, and set different timers and reminders);
4. Smart lighting (the lights in the home can be turned on or off remotely);
5. Smart locks (can approve or reject visitors and have the possibility of unlocking the door automatically when the owner is nearby);
6. Smart alarms and sensors (inform users about dangerous situations such as gas leaks, house/apartment break-ins, etc., and help to take quick action in case of problems);
7. IP cameras (video from the camera is transmitted to registered devices and can be viewed remotely);
8. Smart washing machines and dishwashers (machines that dispense cleaning agents automatically and adjust the quantities according to different factors (e.g., dirtiness, weight) and allow remote switching on or off).

The motivation to start this study was a rapid increase in smart home device use in recent years, and we wanted to explore how much the users of such devices are aware of security and privacy.

The contribution of this study is the result of the statistical analysis, which can be used for further development of IoT devices for smart homes. It is important that users become more aware of the security and privacy of such devices.

1.1. Literature Review

The number of IoT-connected devices had already reached around 11 billion in 2020, and this is expected to increase to 30 billion by 2025 [5]. The increase in the use of smart devices has, consequently, also led to an increase in the amount of private data typically uploaded to the cloud. The pace of development of smart home devices is much faster than the development of protection techniques that could protect these devices and the data collected from them. Given the high risks of devices and their connection to everyday life, understanding the threats and challenges posed by these devices and how this relates to our privacy is of the utmost importance. To understand this area better, we need to understand the terms "security" and "privacy." The term "security" refers to the protection of devices and the networks they are connected to [6]. "Privacy" is defined as a personal boundary regulation process to regulate the levels of privacy with others, depending on the context [7].

Security is one of the most important aspects of any system, as it protects against any internal or external risks [8]. Security attacks on smart homes are divided into passive and active. Passive attacks attempt to obtain useful information without affecting system resources and also include attacks in the form of traffic analysis. These attacks are difficult to detect, as they do not modify data. Hence, the focus should be on prevention rather than detection in these types of attacks. Active attacks are those that attempt to modify or falsify data and influence the operation of devices. These include masquerading, where an intruder pretends to be a legitimate entity to gain privileges. Then a message modification attack, where the attacker intercepts the message passively, partially modifies it and gains unauthorized access by resending it. There are also malware attacks to exploit internal vulnerabilities to modify, destroy, or steal information and gain unauthorized access to system resources.

A study found that users usually lack trust in smart home assistants and lack knowledge on the security of smart home assistants [9]. Another study found that users assume that their privacy while using IoT is protected but are often unaware of the potential for revealing sensitive information. That is why it is important that privacy notifications be improved and more user-friendly settings be presented [10]. Often, users also transfer responsibilities for their privacy protection while using the IoT to manufacturers, not to

ourselves, which should also be improved with better support and adoption of smart home technologies [11]. In another study, it was found that users' security risk perception has an effect on their intentions to use smart home devices [12]. Although smart home devices bring many vulnerabilities, they can often reduce costs or eliminate danger, and they are on the rise. It is expected that a lot of homes will be using these devices in the future.

Another crucial factor in the security of smart home devices is the human aspect. Previous research found that the human aspects need to be accounted for when performing risk analysis of IoT devices in smart homes [13,14].

The rest of the paper is organized as follows. The research model and methods for measuring the model are presented in Section 2. The data analysis and the results are presented in Section 3. In Section 4, we present a discussion of the results and the conclusion.

2. Research Model and Methods

This section describes the developed research model and presents the data collection and samples of the demographic results. We also present the measures used in the regression model.

2.1. Research Model

In Figure 1, we have presented a research model where four variables affect IoT security importance for the users. The model was built based on a previous literature review presented in Section 1.1. and self-created variables, measured using a 5-point Likert scale [14]. The model will be tested with multiple linear regression.

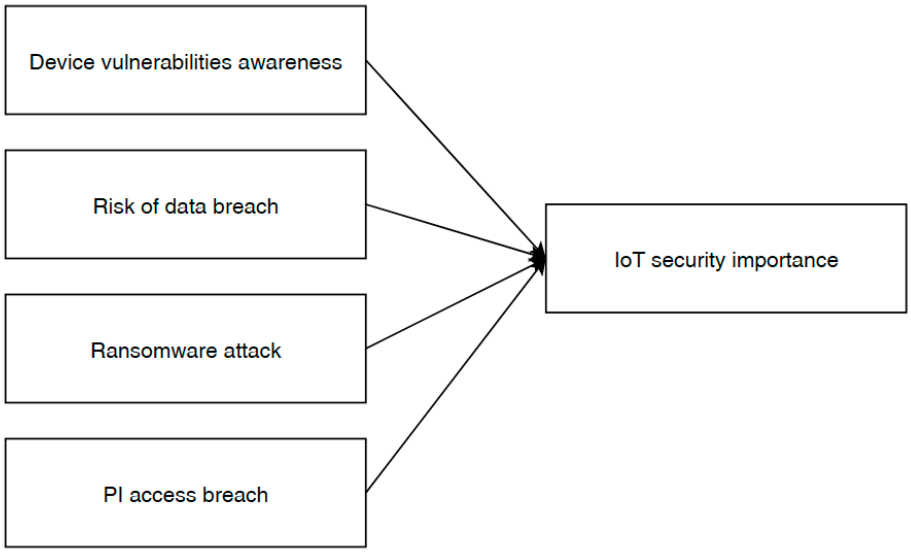

Figure 1. Research model.

Device vulnerability awareness measures users' awareness of the vulnerabilities of smart home IoT devices connected online. Next, *Risk of data breach* measures participants' worries of a cybercriminal being able to access their data in their IoT device in their smart home. *Ransomware attack* measures how worried the participants of the study are that an attacker might enter their network via an IoT device in their smart home to blackmail the user and demand a ransom for the re-establishment of the home system. Personal information (*PI*) *access breach* measures how worried users are that someone might access their personal information shared with a smart home assistant. *IoT security importance* is a dependent variable and measures the importance of security and the protection of smart devices in participants' homes.

This study proposes the following hypotheses:

1. Device vulnerability awareness has a positive impact on IoT security importance.
2. Risk of data breach has a positive impact on IoT security importance.

3. Ransomware attack has a negative impact on IoT security importance.
4. PI access breach has a positive impact on IoT security importance.

2.2. Data Collection

The study used an online questionnaire that was designed to test the hypotheses. There were 34 questions in the survey in total. The research targeted the Slovenian population and used a convenience sampling method. Due to the convenience sampling method, the study cannot be generalized to Slovenian users of the IoT or to all IoT users, but it is a method often used in research. After a complete screening of the results was done, 306 cases were valid. A detailed sample of the demographics for valid cases is presented in Table 1. Most of the participants in the study were aged between 18 and 34 years.

Table 1. Sample of demographics (n = 306).

Variable	Sample Results
Age	18–24 years (46.7%) 25–34 years (32.7%) 35–44 years (12.1%) 45–54 years (5.2%) 55–64 years (2.0%) 65+ years (1.3%)
Gender	Male (60.5%) Female (38.9%) Other (0.70%)
Status	Employed (48.4%) Student (45.1%) Unemployed (3.6%) Retired (1.6%) Other (1.3%)
Type of housing	House (70.3%) Apartment building (29.7%)
Area of living	Rural (51.0%) Urban (49.0%)

2.3. Measures

Particular survey questions were only asked of the users who had at least one IoT device at home, which were 121 participants in the study. Among these questions, five survey questions measuring variables were constructed and measured by a 5-point Likert scale, ranging from (1) strongly disagree to (5) strongly agree:

1. Security and protection of smart devices in my home is very important (*IoT security importance*).
2. I am aware of the dangers and vulnerabilities of smart devices connected to the Internet (*Device vulnerability awareness*).
3. I am worried that a cybercriminal might be able to access data on my smart device in my home (*Risk of data breach*).
4. I am worried that a hacker may enter my network via a smart device in order to blackmail/demand a ransom for the system to work again (*Ransomware attack*).
5. I am worried that someone might be able to access personal information (e.g., passwords, financial information) that is shared with a smart assistant (such as Google Home or Alexa) (*PI access breach*).

3. Data Analysis and Results

3.1. IoT Device Use

The participants were asked whether they were familiar with IoT devices like smart refrigerators, automatic A/C or heating systems, smart assistants, smart lighting, smart

locks, smart alarms and sensors, IP cameras, and smart washing machines and dishwashers. They were also asked whether they owned any of these devices, and 40% of the participants reported owning at least one IoT device. Later on, participants were asked whether they wished to own any of these devices. The detailed statistics are presented in Table 2.

Table 2. Familiarity with IoT devices and use.

Variable	Have Heard of It (n = 306)	Own a Device (n = 121)	Wish to Have a Device but Do Not Own Any Yet (n = 185)	Wish to Have a Device and Has at Least One Already (n = 121)
Smart refrigerator	201	7	27	49
Automatic A/C or heating systems	240	67	56	39
Smart assistants (Google Home, Alexa)	230	49	17	27
Smart lighting	196	54	32	41
Smart locks	202	21	50	49
Smart alarms and sensors	244	43	48	41
IP cameras	231	45	36	42
Smart washing machines and dishwashers	166	38	33	34

In Figure 2, a percentage of participants in each of the four sections has been cumulated into a percentages scale. As can be seen from Table 2, the least owned devices were smart refrigerators and smart locks, and on the other hand, these were also the most wished for devices among participants who already had at least one IoT device. Users who did not have any IoT devices yet most wanted to use automatic A/C or heating systems and smart locks.

We also asked the participants why they did not use IoT devices. The frequencies of this analysis are presented in Table 3. Mostly, the participants did not feel the need to use such devices, or the costs of installment were too high. Not a lot of participants were concerned about the security of IoT devices.

Table 3. Sample of demographics (n = 185).

Reasons for Not Using IoT Devices	Frequency
Excessive cost of installment	60
Unfamiliarity with smart home devices	22
Do not feel the need to use such devices	95
Concerns about the security of IoT devices	35
Resistance to new technologies	8

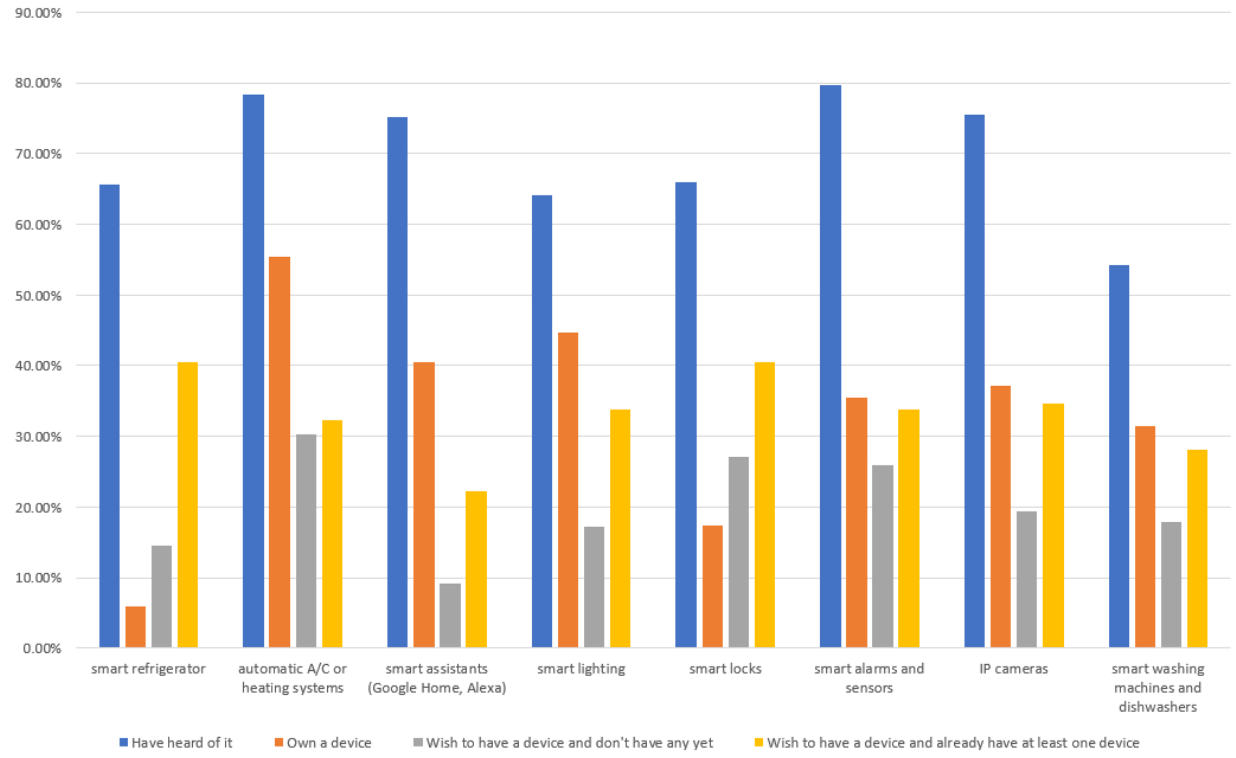

Figure 2. Ownership and familiarity with IoT devices.

3.2. Regression Model Analysis

A regression analysis was built with the 5-point Likert scale survey questions presented in Section 2.3. The descriptive statistics for these variables are presented in Table 4.

Table 4. Descriptive statistics of variables (n = 121).

Variable	Mean	Std. Deviation
IoT security importance	4.01	1.004
Device vulnerability awareness	3.54	1.000
Risk of data breach	3.03	1.245
Ransomware attack	2.79	1.238
PI access breach	3.11	1.395

Multiple linear regression was used to test whether the four independent variables predicted one dependent variable significantly. We chose this method because it is well founded and widely used in various scientific fields [15]. We tested the hypotheses with multiple linear regression (what effect the independent variables have on the dependent variable). Although the Likert scale is often perceived as an ordinal scale, it can also be used as an interval scale in cases where scores are considered to have even spacing between them, and can therefore be used in multiple linear regression [16]. The fitted regression model was *IoT security importance* = 1.82 + 0.44 × *(Device vulnerability awareness)* + 0.19 × *(Risk of data breach)* − 0.07 × *(Ransomware attack)* + 0.08 × *(PI access breach)*.

The overall regression was statistically significant (R^2 = 0.226, F(4,116) = 8.452, p = 0.000). The summary of the multiple linear regression analysis is presented in Table 5. It was found that *Device vulnerability awareness* significantly predicted *IoT security importance* (β = 0.436, p = 0.000) and *Risk of data breach* significantly predicted *IoT security importance* (β = 0.238, p = 0.069). It was found that *Ransomware attack* did not significantly predict *IoT security importance* (β = −0.083, p = 0.528), and *PI access breach* did not significantly predict *IoT security importance* (β = 0.108, p = 0.321).

Table 5. Summary of multiple linear regression analysis (standardized coefficients).

Independent Variable	Standardized β	t-Value (*p*-Value)
Device vulnerability awareness	0.436	5.084 (0.000 ***)
Risk of data breach	0.238	1.833 (0.069)
Ransomware attack	−0.083	−0.633 (0.528)
PI access breach	0.108	0.996 (0.321)

[1] * $p < 0.05$. ** $p < 0.01$. *** $p < 0.001$.

Device vulnerability awareness and *Risk of data breach* had a higher impact on *IoT security importance* perception than *Ransomware attack* and *PI access breach*, but together all variables formed a significant model. However, there was a risk of multicollinearity in the model, which means that some of the independent variables could have been correlated. Although the statements used in the model were independent, collaborators in the survey could have seen similarities in the statements, which could pose a risk to the interpretation of the results.

3.3. IoT Devices and Security

Further on, the users of IoT devices were asked questions regarding security concerns. The frequency of the results is presented in Table 6. The results show that the majority of users changed their security settings after more than 12 months, or never. On the other hand, they had never been a victim of cyberattacks. Some reports show that there are over 12,000 cyberattacks a week in smart homes [17]. Although people are not concerned about the security of their IoT devices, cyberattacks on smart homes are on the rise and awareness about the issues is lacking among users.

Table 6. Questions regarding the security of IoT devices (n = 121).

Variable	Frequency
Do you think the usefulness of smart devices outweighs concerns about their security?	Yes (47.1%) No (47.1%)
Have you changed your security settings (passwords, codes) after purchasing smart devices?	Yes (73.6%) No (26.4%)
How often do you change the security settings of your smart devices?	Every 2 months (1.7%) Every 3–6 months (11.6%) Every 6–12 months (11.6%) After more than 12 months (20.7%) Never after the first use (28.1%)
Have you ever been the victim of a cyberattack involving IoT devices in your home?	Yes (0.00%) No (100.00%)

4. Discussion and Conclusions

In this study, we proposed four hypotheses that were tested using multiple linear regression. The results of the hypothesis are presented here.

1. Device vulnerability awareness had a positive impact on IoT security importance.

This hypothesis was confirmed and was significant with a t-value of 5.084. This shows that the users who feel that they are aware of IoT device vulnerabilities also believe that the security and protection of IoT devices are important.

2. Risk of data breach had a positive impact on IoT security importance.

The second hypothesis was not significant, meaning that if the user is worried that a cybercriminal might access data on their smart device, it does not necessarily mean that the security of their IoT devices is important to the user.

3. Ransomware attack had a negative impact on IoT security importance.

The third hypothesis was also not significant but showed a slightly negative impact of *Ransomware attack* on *IoT security importance*. This shows that if the user is worried that someone might demand a ransom after obtaining control over their system, it does not mean that IoT device security is important to them.

4. PI access breach had a positive impact on IoT security importance.

The fourth hypothesis was also not statistically significant. Suppose a user is worried that someone could access their personal information over a smart assistant. In that case, it does not mean that the security and protection of IoT are important to the user.

Overall, the multiple linear regression model was confirmed and was significant, with a coefficient of determination of 22.6%. All four independent variables predicted the dependent variable and presented a model that was statistically significant. Still, the independent variable *Device vulnerability awareness* also had a significant effect on the dependent variable in this model.

Further on in our analysis, we also found that the least owned devices were smart refrigerators and smart locks, and on the other hand, these were also the most wished for devices among participants who already had at least one IoT device. Users who did not have any IoT devices wanted to use mainly automatic A/C or heating systems and smart locks.

The users who did not use IoT devices most often did not feel the need to use such devices, or the costs of installment were too high. On the other hand, not many participants were concerned about the security of IoT devices. In another study, it was also found that the perceived security risk had an effect on intentions to use smart home devices [12].

Some studies have already researched users' perceptions of security IoT devices and found a lack of users' knowledge on systems and not being aware of threats [9].

4.1. Limitations and Future Research Directions

This study has some limitations. Due to the convenience sampling method, the study cannot be generalized to Slovenian users of IoT or to all IoT users. Future research should strive to collect a larger and more representative sample.

The next limitations are the variables in the regression model. Potential variables might have been left unselected, and further variables could have had an effect. There is also a risk of multicollinearity in the linear regression model. For future research, more Likert-type questions should be used, and a SEM model could be built. Future studies may need to develop a measurement scale specific to IoT users.

4.2. Conclusions

This study established a survey to measure a developed model with IoT users in smart homes. Altogether, 306 participants collaborated in the survey, out of whom 121 already used IoT devices in their smart homes. Among those who did not use any IoT devices at home, most wished they had automatic A/C or heating systems or smart locks at home. Those already using IoT devices wished they had devices like smart refrigerators or smart locks. We also developed a model tested with multiple linear regression, where the results were significant. The independent variables *Device vulnerability awareness*, *Risk of data breach*, *Ransomware attacks*, and *PI access breach* had an impact on *IoT security importance*. We also found that the users often did not feel that the security or privacy of IoT devices in their homes was very important. Most users were not using IoT devices due to expense and not because of security issues. Users who were using IoT devices in their smart homes rarely checked their security settings. It was also found that none of the respondents had been a victim of a cyberattack involving IoT devices in their homes. It is important that users be made aware of the privacy risks associated with their devices and the approaches in place to protect and minimize the risks. This paper also provides an overview of users'

perception of security while using IoT devices and help developers build devices with security settings that are easier to set up.

Author Contributions: Conceptualization, N.F.; data curation, N.F.; formal analysis, L.N.Z.; funding acquisition, M.H.; investigation, N.F.; methodology, L.N.Z.; resources, M.H.; supervision, M.H.; validation, L.N.Z.; writing— original draft, L.N.Z. and N.F.; writing—review & editing, L.N.Z. and M.H. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the European Union's Horizon 2020 Research and Innovation Program CONCORDIA grant number [830927] and CyberSec4Europe grant number [830929]. Research was also funded by the Slovenian Research Agency grant number [P2-0057].

Acknowledgments: The authors acknowledge the financial support from the European Union's Horizon 2020 Research and Innovation Program under the CONCORDIA project (GA No. 830927) and CyberSec4Europe project (GA No. 830929). The research was also supported financially by the Slovenian Research Agency (Research Core Funding No. P2-0057).

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Schiefer, M. Smart Home Definition and Security Threats. In Proceedings of the 2015 Ninth International Conference on IT Security Incident Management & IT Forensics, Magdeburg, Germany, 18–20 May 2015; pp. 114–118.
2. Yassein, M.B.; Hmeidi, I.; Shatnawi, F.; Mardini, W.; Khamayseh, Y. Smart Home Is Not Smart Enough to Protect You—Protocols, Challenges and Open Issues. *Procedia Comput. Sci.* **2019**, *160*, 134–141. [CrossRef]
3. Tawalbeh, L.A.; Muheidat, F.; Tawalbeh, M.; Quwaider, M. IoT Privacy and Security: Challenges and Solutions. *Appl. Sci.* **2020**, *10*, 4102. [CrossRef]
4. Zielonka, A.; Woźniak, M.; Garg, S.; Kaddoum, G.; Piran, M.J.; Muhammad, G. Smart Homes: How Much Will They Support Us? A Research on Recent Trends and Advances. *IEEE Access* **2021**, *9*, 26388–26419. [CrossRef]
5. Internet of Things (IoT) and non-IoT Active Device Connections Worldwide from 2010 to 2025. Available online: https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide/ (accessed on 11 January 2022).
6. Seliem, M.; Elgazzar, K.; Khalil, K. Towards Privacy Preserving IoT Environments: A Survey. *Wirel. Commun. Mob. Comput.* **2018**, *2018*, 1032761. [CrossRef]
7. Altman, I. *The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding*; Brooks/Cole Pub. Co.: Pacific Grove, CA, USA, 1975.
8. Komninos, N.; Philippou, E.; Pitsillides, A. Survey in Smart Grid and Smart Home Security: Issues, Challenges and Countermeasures. *IEEE Commun. Surv. Tutor.* **2014**, *16*, 1933–1954. [CrossRef]
9. Abdi, N.; Ramokapane, K.M.; Such, J.M. More than smart speakers: Security and privacy perceptions of smart home personal assistants. In Proceedings of the Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019), Santa Clara, CA, USA, 12–13 August 2019; pp. 451–466.
10. Zheng, S.; Apthorpe, N.; Chetty, M.; Feamster, N. User Perceptions of Smart Home IoT Privacy. *Proc. ACM Hum.-Comput. Interact.* **2018**, *2*, 1–20. [CrossRef]
11. Haney, J.; Acar, Y.; Furman, S. "It's the Company, the Government, You and I": User Perceptions of Responsibility for Smart Home Privacy and Security. In Proceedings of the 30th USENIX Security Symposium (USENIX Security 21), Online, 11–13 August 2021.
12. Klobas, J.E.; McGill, T.; Wang, X. How perceived security risk affects intention to use smart home devices: A reasoned action explanation. *Comput. Secur.* **2019**, *87*, 101571. [CrossRef]
13. Jacobsson, A.; Boldt, M.; Carlsson, B. A risk analysis of a smart home automation system. *Future Gener. Comput. Syst.* **2016**, *56*, 719–733. [CrossRef]
14. Ali, B.; Awad, A.I. Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes. *Sensors* **2018**, *18*, 817. [CrossRef] [PubMed]
15. Andrews, D.F. A robust method for multiple linear regression. *Technometrics* **1974**, *16*, 523–531. [CrossRef]
16. Hair, J., Jr.; Babin, B.; Money, A.; Samouel, P. *Essentials of Business Research Methods*; Johns Wiley & Sons. Inc.: Hoboken, NJ, USA, 2003.
17. Coker, J. Smart Home Experiences Over 12,000 Cyber-Attacks in a Week. *Info Secur.* 2 July 2021. Available online: https://www.infosecurity-magazine.com/news/smart-home-experiences-cyber/ (accessed on 11 January 2022).