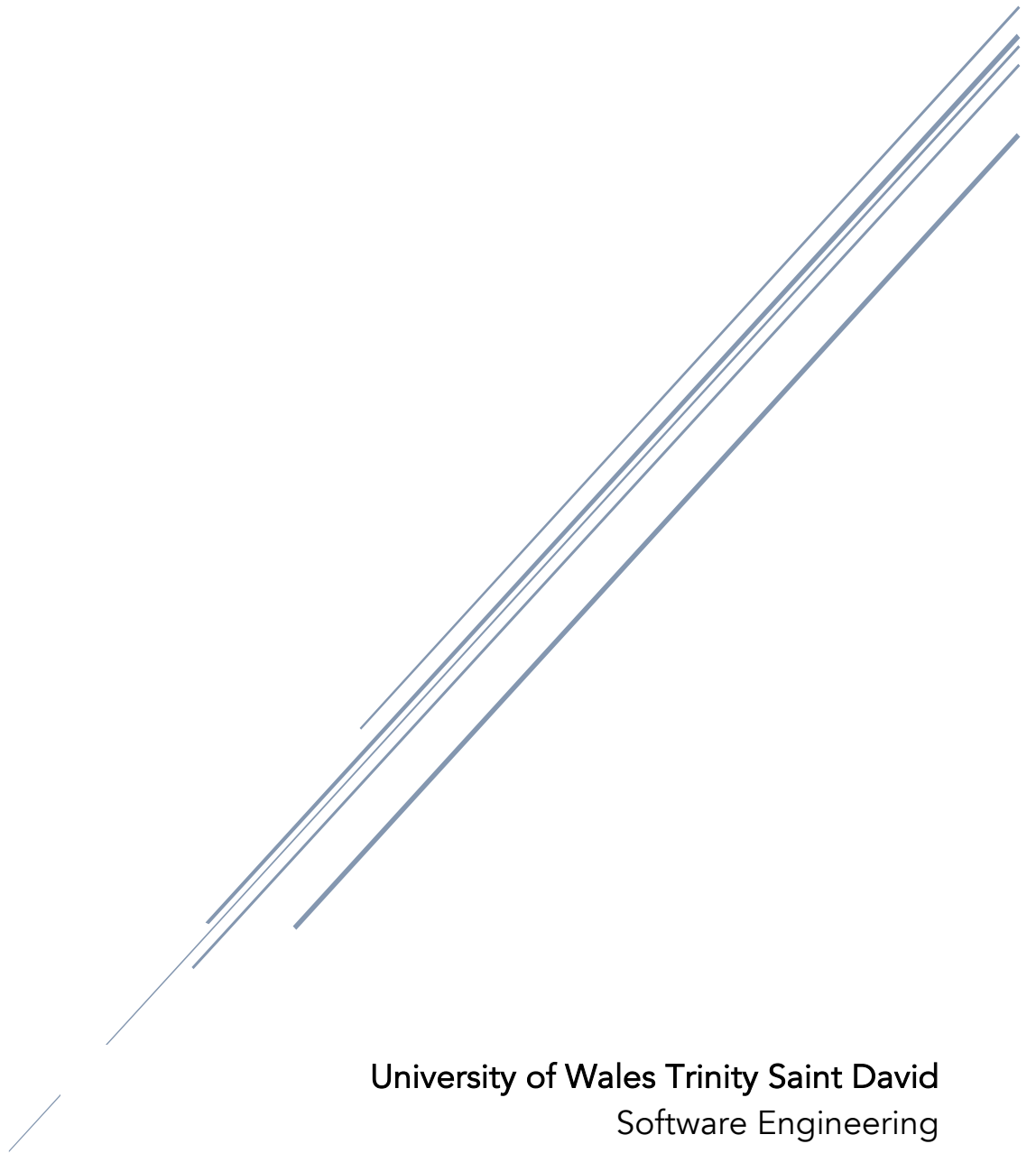


Design and Implementation of Smart Home

Smart and Connected Devices I



University of Wales Trinity Saint David
Software Engineering

Siobhan Stephens - 1800709

Abstract

The rise in smart home devices has sparked concerns for the security and privacy of their users. Smart home and home automation has allowed the house to become more interactive to the needs of its occupants and aims to simplify the daily routine and provide increased convenience for the process of managing electrical appliances within the home, whilst also being able to personalise the home and improve safety. This report outlines some common smart home devices, their security risks and vulnerabilities, and ways to protect against them.

Table of Contents

- 1. Introduction 0
- 2. Research into Smart Home and Home Automation Devices 1
 - 2.1. Smart Thermostat 1
 - 2.2. Smart Lighting..... 1
 - 2.3. Smart Home Security 2
 - 2.4. Virtual Personal Assistant 3
- 3. Security Risks 3
- 4. Measures to Secure Smart Devices..... 5
- 5. Conclusion 7
- 6. References 8

1. Introduction

Smart home and home automation has allowed the home space to become more interactive to the needs of its occupants, and aims to simplify the daily routine and provide increased convenience for the process of managing electrical appliances within the home, whilst also being able to personalise their home and improve safety [1].

IoT devices often contain sensors that continually monitor the fine details of their user and environment [2], and allow their users to control them remotely over the internet. By means of low-cost computing, big data, the cloud and mobile technologies, everyday objects such as kitchen appliances, home locks, doorbells, can all be connected to create a seamless connection between people, processes, and things [3].

Over the last decade, IoT has become increasingly popular and can be found in a substantial number of households worldwide. According to Statista (figure 1), worldwide consumer spending on smart home systems from 2014 to 2023 is set to increase to 157 billion USD in 2023 [4]. They also state that UK household penetration will be 16.5% in 2020 and is expected to hit 44.8% by 2024 [5].

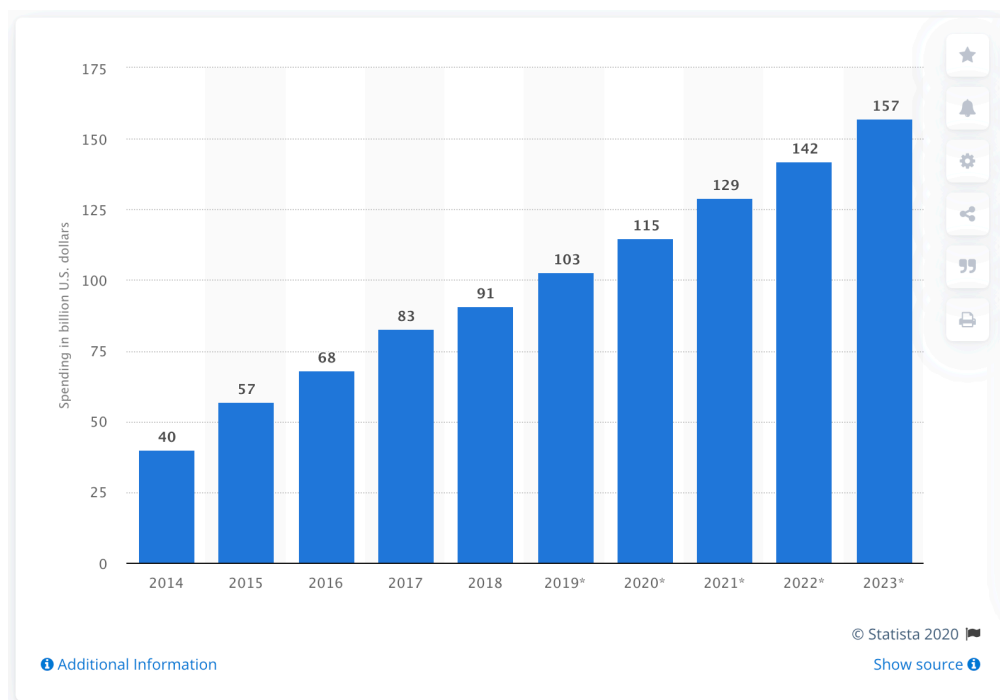


Figure 1. Smart Home Spending Worldwide - Statista [4]

However, these devices can be manipulated by attackers to cause financial, physical and psychological harm [6].

2. Research into Smart Home and Home Automation Devices

The concept of home automation, or smart home, covers a range of functionality and processes, from home assistants, automatic lighting, home security and even pouring your morning coffee. The practicality of home automation allows the user to eliminate repetitive tasks and respond to the surrounding environment by making decisions based on sensor inputs and set tolerances.

The following sub-sections discuss some of the common devices and uses of home automation.

2.1. Smart Thermostat

One of the most common smart home devices used today are smart thermostats/climate control. These devices work through the use of temperature and humidity sensors to monitor the environment and react by turning on/off heating devices to increase or decrease temperature when the environment crosses the required temperature or humidity values. These thermostats can either be used as a standalone device, e.g. for home heating, which allows the user to set the temperature remotely, or can be found within other home devices such as ovens and refrigerators.

These devices have many advantages, firstly - convenience. The heating can be set remotely, as a set schedule, or even by using the user's geo-location. Users are able to ensure their home is to their ideal temperature before they arrive home or throughout the day. The heating can be turned off automatically when the user leaves their home, saving money on heating bills and also benefitting the environment by reducing emissions and carbon footprint.

If geo-location is used, the algorithms are able to learn the user's routine and aim to set the home temperature without user interaction. They also often have better tolerances than conventional home controls, for a more accurate temperature setting.

There are however disadvantages to smart thermostats, and if there is often a person at home, there would likely be no need for a smart thermostat as it would not need to adjust to schedules and would not be cost effective. Smart thermostats are costly to install and are not compatible with all heating appliances. Smart Thermostats have also been used maliciously. In 2019, a couple in Wisconsin had their home heat turned up to 90 degrees F by a hacker, due to a leaked password [7].

2.2. Smart Lighting

Smart lighting is an umbrella term for many different types of devices, from single smart bulbs, bulbs connected in a series, LED strips, smart switches or whole light modules. These smart bulb/light devices often contain built-in sensors, and can communicate either through

a smartphone app, remote, or a switch, often over Wi-Fi networks, to receive commands of control for brightness and colour. Smart switches allow normal light bulbs and fittings to act as smart lights, in order to control them remotely, again through the use of a smartphone app.

Smart plugs may also be used to control lighting. They once again use a smartphone app to remotely control the switch on or off and allow the user to set schedules to trigger the switch. Many of these devices also work with smart home assistants such as Alexa, allowing the user to say phrases such as “turn the hall light on”, however, integration is not always the smoothest and are often glitchy. As there are many brands of smart lighting all with their own smartphone apps, users are either forced to stay loyal to a brand or have multiple apps. Also, phone apps are often only compatible with the latest versions of smartphone such as Apple or Android, which limits the use for some users.

These devices have many benefits, firstly, to save energy consumption – a user may set up switches to turn off on weekdays after they have left for work. They can also be used for security – for example if a user is going on holiday, setting lamps to turn on in the evening as normal could trick a potential burglar into thinking they are at home. Another use is to simply personalise the home for a set mood – for example a movie night might suit a dimmer bulb, or a house party an RGB disco bulb.

However, smart lighting can be very costly, and can be unreliable. If there is an issue with the Wi-Fi network, the bulb may not be responsive. Also, if you decide to use the original light switch and turn the bulb off, it will not respond to any of the smart demands.

2.3. Smart Home Security

There are many types of devices that come under smart home security, one of them is smart door locks. Smart locks contain built-in modules which receive wireless ZigBee or Z-Wave commands to allow users to unlock or lock their doors. The keyless entry can be done remotely through the use of a smartphone app, allowing access to permitted visitors without a key if required, other devices require a card. Another useful feature is geo-fencing, which automatically locks the door once your smartphone leaves a defined location/area. Many devices have tamper alarm and monitor who has been entering and leaving the house in real time – with the option to turn on alerts to your smart phone.

However, many smart locks are powered by batteries which will run out – this could potentially leave you unable to enter your house until you replace the battery. There are also more sinister dangers for some smart locks. A security flaw was discovered in the KeyWe smart lock, allowing hackers to exploit the device and gain access to homes. The smart lock is unable to receive firmware updates, leaving owners with no choice but to remove the lock [8].

Other smart security devices include motion sensors, door and window sensors, alarms and security cameras. These devices often connect to your home router and continually monitor

the environment. If suspicious movement is detected, SMS or push notifications are sent to your mobile. They can also be used to trigger lights, door locks and alarms.

Smart alarms allow you to trigger an alarm remotely, to discourage an intruder, along with the use of smart security cameras which allow you to watch the video feed on your smartphone or internet enabled device remotely. Internet connected smart cameras pose many potential threats especially inside the home, if a hacker was to access the footage.

2.4. Virtual Personal Assistant

Many smart devices can be linked together through a virtual personal assistant or smart hub, such as Amazon's Alexa or Google's Home or Nest. These can be used as a central point to control your smart home devices through a smartphone app or voice commands. They also contain their own features, such as playing music and querying the internet for response to questions you ask it.

However, these pose many threats, as if a hacker gains access to this device, they can potentially control many of the appliances in your home, from security cameras, lights, even smart refrigerators and ovens.

3. Security Risks

IoT-based smart homes face security and privacy challenges that span all layers of the IoT architecture [9], in terms of the confidentiality, authenticity, and integrity of the data sensed, collected, and exchanged by the IoT devices [10].

As discussed, despite having many advantages, smart devices are often vulnerable to attacks. These vulnerabilities may lie in the devices themselves or the protocols that operate between those devices, such as the two most common – Z-Wave and ZigBee [6]. As smart home devices are such a growing market, many companies are getting involved, including non-IT based companies, such as the physical security sector. As a result, most companies do not consider the full security of these devices in their services and leave them vulnerable. As stated by Sivaraman et al, "Users purchasing IoT devices for their smart-home assume that the manufacturer has embedded appropriate privacy/security safeguards in the devices. As we have shown in the previous section, this is not the case – indeed many of these devices can be compromised with very little effort on the part of the attacker." [11].

There have been many instances of exposed vulnerabilities in smart devices, an example being where Fernandes et al. were able to exploit framework design flaws in Samsung's SmartThings to construct four proof-of-concept attacks that: (1) secretly planted door lock codes; (2) stole existing door lock codes; (3) disabled vacation mode of the home; and (4) induced a fake fire alarm [6]. All of the above attacks expose a household to significant harm—break-ins, theft, misinformation, and vandalism [6]. Also, in a framework written by

Denning et al., a number of serious threats to smart homes were outlined, which included threats of eavesdropping, illegal physical entry, privacy violations and data destruction [12].

Passive network observers such as internet service providers could analyse IoT traffic to infer sensitive details about users [13]. Apthorpe et al. found that network traffic rates from IoT devices can reveal sensitive user interactions even when the traffic is encrypted, indicating that IoT-specific concerns should be considered in ISP data collection and usage policies [13].

Consider the following security breaches - it is possible for cybercriminals to access your home network through an IoT device, and perform a ransomware attack, demanding money for return of data with no promise. Smart thermostat data could be accessed to work out whether an occupant is at home or on vacation. Data shared with smart assistants could be accessed, discovering sensitive passwords, financial information and user routines, along with potentially sensitive conversations [14]. In fact, according to the 2017 Internet Security Threat Report by Symantec, the average IoT device was attacked once every two minutes [15].

IoT devices are vulnerable for many reasons, including the lack of security consideration, no mechanism for updating software – therefore not allowing for patches to be made, and default or hardcoded passwords which hackers are able to exploit [14].

These IoT devices are susceptible to Man-in-the-middle attacks, where an attacker breaches, interrupts or spoofs communications between the two systems [16]. For example, a hacker could intercept and spoof temperature or activity data from an IoT device in order to disable sensors or a critical alarm system, or could intercept sensitive data from a personal assistant, which could be major if not encrypted.

Data and identity theft are also possible due to the mass amount of data shared with IoT devices, including personal habits and schedules, passwords, addresses and contact information, and personal messages. This data could be exploited for fraudulent transactions and identity theft [17]. Alongside this, device hijacking is possible, where a hacker assumes control of a device, allowing them to potentially infect the whole network and all other smart devices connected to it. This suggests that a hacker could gain access to a less critical device, such as a smart light bulb, and use it to gain access to the network and later control a critical device such as a smart door lock, security alarms or security cameras and their footage.

IoT devices are vulnerable to permanent and distributed denial of service (PDos and DDoS) attacks, as described by Koliadis et al in "DDoS in the IoT: Mirai and Other Botnets" [18]. According to Norton Security [14], on October 12th 2016, hundreds of thousands of compromised IoT devices were used as a botnet named Mirai, harnessing the processing power of these devices to launch a large scale cyberattack, taking down websites including Spotify, Netflix and PayPal temporarily [18]. The number and frequency of DDoS attacks are rising rapidly, primarily due to the lack of security in IoT Devices [19]. Another example of PDos is BrickerBot, which started in March 2017. BrickerBot utilises the assault procedure, Telnet brute force, which is also utilised by Mirai botnet. In its first four days, Bricker bot 1 infected 1,895 IoT devices [11].

4. Measures to Secure Smart Devices

Despite the many vulnerabilities that may lie in IoT devices, there are ways to secure them.

Building a more secure smart home begins with the Wi-Fi router, the gateway to the internet, and what connects all of your IoT devices. Firstly, consider renaming the router so that it does not contain any identifiers including its provider or manufacturer [20]. The router should also be set to use a strong encryption method such as WPA2. Most importantly, ensure strong, complex and unique passwords are used for the router account. It is also recommended that passwords are changed frequently [20].

Ensure that a firewall is set up on your home router to block unsolicited incoming network traffic. Consider allocating static IP addresses to your devices instead of using DHCP, or use MAC address filtering for each IoT device on the network, so that a hacker cannot join the network or manipulate DHCP to allocate themselves a network address [20].

Next, are the smart devices and their providers. Privacy and security are key aspects when choosing these devices, consider their privacy policies, how the provider will store your data, if the provider will sell your data to a third party, and how updates to the IoT devices will occur. There may be settings such as if you agree to sending data to the manufacturer – it is best to disable this to improve privacy.

As stated by Balliu et al, one of the most important steps to remember is keep any smartphone app or operating system up to date, as these are often access points for IoT devices with remote access [21]. It is also through these apps that IoT device updates take place. These updates often contain security patches, which is why they are so essential.

In order to further improve security, if the smart device providers allow for two-factor authentication (2FA), make sure it is enabled. This makes it more difficult for a hacker to gain access to the account. As well as this, do not ever remotely access any IoT devices whilst using a public Wi-Fi network. Whilst on this network, communications may be susceptible to attacks such as man-in-the-middle. If a public network must be used, a VPN should be used to increase security [11]. A VPN is beneficial even when on a home network.

In order to best protect a home network and IoT devices, two separate routers and networks should be used, one for home devices, and another for IoT devices, however if this isn't possible, creating a secondary 'guest' type network to isolate the IOT devices is recommended, as stated by Lin et al [22]. The reason for this, is if one network was to be compromised, such as the IoT device network due to a security flaw in a device, all home devices are secure and cannot be breached. The other network can be dealt with, hopefully without any harm to personal data.

Another way to further secure IoT devices, if possible, is to disable all unused features. An example of this would be to disable the microphone on your home assistant and use the smartphone app, due to concerns of them recording personal conversations, as discussed by

Lau et al [23]. However, removing this feature does limit the use of these assistants, and so instead, consider changing the 'trigger' word to something unique that won't accidentally trigger recordings and regularly check your voice assistant's logs and clear them.

Users should consider upgrading devices if they are old or incompatible with new updates. Out-of-date devices will no longer receive updates including important security patches, meaning they could be vulnerable to attack. Along with this, newer IoT devices have focused more on security, and therefore may be safer to begin with. They will also likely contain new features, and be more efficient, due to the recent advancements in IoT devices.

Finally, ensure your personal data is kept safe through the use of antivirus software to prevent attacks, and regular backups, such as to the cloud, or on a backup medium. This ensures that in the case of a malware attack, your data can be restored [20].

5. Conclusion

In conclusion, smart home and IoT devices bring many advantages to their users, however at the cost of potential data and network security vulnerabilities.

The security approaches used in a domestic smart home application are very different to those used in industry. The main issue lies with the lack of security knowledge and application by device manufacturers, the installation, configuration and maintenance of these devices by untrained individuals, and the lack of security features found within a home environment.

It is important to make consumers aware of smart home privacy vulnerabilities in order to incentivise manufacturers to properly consider privacy and security issues in the design and maintenance of their products. Improved policies surrounding privacy and access should be implemented for ISPs and other network observers in order to better overcome the challenges posed by IoT devices.

6. References

- [1] R. K. Kodali, V. Jain, S. Bose, and L. Boppana, "IoT based smart security and home automation system," in *Proceeding - IEEE International Conference on Computing, Communication and Automation, ICCCA 2016*, 2017, pp. 1286–1289.
- [2] N. Apthorpe, D. Reisman, and N. Feamster, "A Smart Home is No Castle: Privacy Vulnerabilities of Encrypted IoT Traffic," May 2017.
- [3] Oracle UK, "What Is the Internet of Things (IoT)? | Oracle United Kingdom." [Online]. Available: <https://www.oracle.com/uk/internet-of-things/what-is-iot.html>. [Accessed: 28-Apr-2020].
- [4] Statistica Research Department, "Global smart home spending 2014-2023 Statista," Feb. 2020.
- [5] "Smart Home - United Kingdom | Statista Market Forecast," 19-Feb-2019. [Online]. Available: <https://www.statista.com/outlook/279/156/smart-home/united-kingdom>. [Accessed: 25-Apr-2020].
- [6] E. Fernandes, J. Jung, and A. Prakash, "Security Analysis of Emerging Smart Home Applications," in *Proceedings - 2016 IEEE Symposium on Security and Privacy, SP 2016*, 2016, pp. 636–654.
- [7] "Hacker breaks into smart-home Google Nest devices, terrorizes couple - Business Insider." [Online]. Available: <https://www.businessinsider.com/hacker-breaks-into-smart-home-google-nest-devices-terrorizes-couple-2019-9?r=US&IR=T>. [Accessed: 04-May-2020].
- [8] Anthony Spadafora, "Smart lock security flaw could leave your door wide open | TechRadar." [Online]. Available: <https://www.techradar.com/uk/news/smart-lock-security-issues-leave-the-door-open-for-hackers>. [Accessed: 05-May-2020].
- [9] M. F. Elrawy, A. I. Awad, and H. F. A. Hamed, "Intrusion detection systems for IoT-based smart environments," *Journal of Cloud Computing*, vol. 7, no. 1. Springer Verlag, 01-Dec-2018.
- [10] B. Ali and A. I. Awad, "Cyber and physical security vulnerability assessment for IoT-based smart homes," *Sensors (Switzerland)*, vol. 18, no. 3, pp. 1–17, 2018.
- [11] M. Shobana and S. Rathi, "IOT Malware : An Analysis of IOT Device Hijacking," 2018.
- [12] T. Denning, T. Kohno, and H. M. Levy, "Computer security and the modern home," *Communications of the ACM*, vol. 56, no. 1. pp. 94–103, Jan-2013.
- [13] N. Apthorpe, D. Reisman, and N. Feamster, "A Smart Home is No Castle: Privacy Vulnerabilities of Encrypted IoT Traffic," May 2017.
- [14] NortonLifeLock, "12 tips to secure your smart home and IoT devices." [Online]. Available: <https://us.norton.com/internetsecurity-iot-smart-home-security-core.html>. [Accessed: 07-Jun-2020].
- [15] "Internet Security Threat Report ISTR," 2017.
- [16] R. E. Navas et al., "Demo: Do not trust your neighbors! A small IoT platform illustrating

a man-in-the-middle attack," p. 10, 2018.

- [17] Stilianos Vidalis and Olga Angelopoulou, "Assessing Identity Theft in the Internet of Things," Mar. 2014.
- [18] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS in the IoT: Mirai and other botnets," *Computer (Long. Beach. Calif.)*, vol. 50, no. 7, pp. 80–84, 2017.
- [19] "Smart Home: Threats and Countermeasures - Rambus." [Online]. Available: <https://www.rambus.com/iot/smart-home/>. [Accessed: 10-May-2020].
- [20] N. Nthala and I. Flechais, "Rethinking Home Network Security," 2018.
- [21] M. Balliu, I. Bastys, and A. Sabelfeld, "Securing IoT Apps," *IEEE Secur. Priv.*, vol. 17, no. 5, pp. 22–29, Sep. 2019.
- [22] H. Lin and N. Bergmann, "IoT Privacy and Security Challenges for Smart Home Environments," *Information*, vol. 7, no. 3, p. 44, Jul. 2016.
- [23] J. Lau, B. Zimmerman, and F. Schaub, "Alexa, are you listening? Privacy perceptions, concerns and privacy-seeking behaviors with smart speakers," *Proc. ACM Human-Computer Interact.*, vol. 2, no. CSCW, pp. 1–31, Nov. 2018.