UNDERSTANDING AND IMPROVING THE USABILITY, SECURITY, AND PRIVACY OF SMART LOCKS FROM THE PERSPECTIVE OF THE END USER

by

Hussein Hazazi

A dissertation submitted to the faculty of
The University of North Carolina at Charlotte
in partial fulfillment of the requirements
for the degree of Doctor of Philosophy in
Computing and Information Systems

Charlotte

2024

Approved by:

____

Dr. Mohamed Shehab

____

Dr. Heather Richter Lipford

____

Dr. Richard Lambert

____

Dr. Weichao Wang

ABSTRACT

HUSSEIN HAZAZI. Understanding and Improving the Usability, Security, and Privacy of Smart Locks From the Perspective of the End User. (Under the direction of DR. MOHAMED SHEHAB)

Over the past two decades, the Internet of Things (IoT) has seen a significant expansion in both the sophistication and variety of its applications. These applications span several domains, including enhancing and automating services in healthcare, advancing smart manufacturing processes, and elevating home living standards through smart home technologies. These technologies empower individuals with greater control over their home appliances. Smart locks are smart home devices that were introduced as replacements for traditional locks. Smart locks, designed to go beyond the basic functionality of traditional locks by offering additional features, have seen a surge in market growth and competitiveness. According to the Statista Research Department, it is projected that the global market for smart locks will surpass four billion dollars by 2027 [47]. A number of studies have examined end users' concerns, needs, and expectations regarding smart homes in general [35, 99, 80, 97, 33, 98]. However, little research has been conducted to examine these aspects of the smart lock in particular. To address this gap, we conducted a series of user studies that aim to elucidate how smart locks are integrated and interact within smart home environments, focusing on user interactions both with the locks themselves and when they are part of broader automation scenarios. This dissertation contributes to a deeper understanding of smart lock technology from a user-centric viewpoint. It offers insights into user motivations, concerns, and preferences regarding smart lock usage and automation. It also highlights the importance of balancing convenience and security, the pivotal role of trust, and the complexities of integrating smart locks into broader smart home systems.

ACKNOWLEDGMENTS

First and foremost, I would like to thank my father, brothers, and sisters, who have provided encouragement and support in every possible way. Special thanks to my mother, whose memory and spirit have continued to guide me, may god have mercy on her soul. My deepest thanks also go to my wife, whose patience, understanding, and encouragement were nothing short of extraordinary during these past five years. Your strength and love have been the bedrock of my daily life and this achievement. To my daughters, Meral and Mila, who remind me every day of what truly matters. Meral, your joyful spirit has been my inspiration, and Mila, your smiles have brightened my darkest days.

A special word of gratitude goes to my Ph.D. supervisor, Dr. Mohamed Shehab, for his invaluable guidance and mentorship. Dr. Shehab hasn't been only a mentor but a great supporter throughout this academic journey. I also wish to extend my gratitude to the members of my dissertation committee, Dr. Lipford, Dr. Wang, and Dr. Lambert. The feedback and insights you provided were crucial in refining my research and broadening my perspectives.

I am extremely grateful to those who supported and encouraged me throughout this journey. The journey was long and challenging, but the unwavering support I received made it immensely rewarding.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1: INTRODUCTION

Recently, there has been a growing trend in residential architecture and technology for smart homes in an effort to give homeowners more control over various aspects of their home with the touch of a button. In smart homes, traditional home devices and appliances such as door locks, doorbells, and smoke alarms are replaced with their "smart" counterparts. With the help of embedded sensors and communication protocols, these interconnected smart home devices are able to collect and exchange information as well as allow homeowners to control them remotely.

However, implementing smart home technology also raises several privacy and security concerns since they can be more vulnerable to security and privacy issues because of their ability to communicate. An unauthorized manipulation of software or hardware in these devices can lead to the leakage of sensitive user information [46]. Moreover, smart devices with internet connectivity are considerably more vulnerable to remote attacks due to the fact that attackers can download malware to them or directly access their networked control interfaces when connected to the internet [50]. In the last few years, smart locks have emerged as a replacement for traditional locks that offer more features and enhancements. Approximately $0.42 billion was spent on smart locks in 2016, according to a Statista report; however, by 2027, the market is expected to surpass four billion dollars [47]. As consumers gradually replace their traditional locks with smart locks, it is becoming increasingly important to investigate the security and privacy issues associated with smart locks. In fact, smart locks are estimated to have an even larger global market size if not for security and privacy concerns. According to their paper “Smart Locks for Smart Customers?”, Hylta et al described a study conducted in London in 2017 on customers’ adoption of smart locks. 64% of the 54 respondents said they would hesitate to purchase a smart lock, with 50% citing security concerns as the reason [14]. Even though the ability to connect and communicate with the cloud and other smart home devices can be a security concern for some prospective smart lock buyers or current users, other users might find it extremely beneficial as it allows for more control and extra features.

In order to get smart locks that are equipped with an embedded Wi-Fi modem to be connected to the internet, they are usually connected to the user’s home network, which is done as a part of the initial configuration of the device (also called the onboarding process). Due to the fact that smart locks are headless devices, connecting them to the home network is not as straightforward as connecting devices that are equipped with a keyboard or a touch screen [89]. Therefore, smart lock manufacturers implement Wi-Fi provisioning schemes that mostly take advantage of the user’s smartphone to share the home network credentials with the lock. Each provisioning approach has its advantages and disadvantages which smart lock manufacturers take into consideration while choosing the appropriate approach for their smart lock. Even though the end result is the same, which is getting the smart lock connected to the home network, the provisioning process that the user goes through on their smartphone differs depending on the provisioning scheme implemented by the manufacturer. A provisioning process that is not intuitive or unnecessarily complex can lead to failed provisioning or customer dissatisfaction. However, most of the research being done on Wi-Fi provisioning focuses on their scalability and security flaws without putting much focus on the end user experience. Therefore, in Chapter 4 of this dissertation, we provide an empirical comparison of the users' perceptions of provisioning the smart lock using Bluetooth Low Energy (BLE) and Software-enabled Access Point (SoftAP), which are two of the most widely used provisioning approaches in smart locks and headless IoT devices in general.

Home automation serves many purposes within the smart home such as increasing convenience and managing redundant tasks [82]. Some studies have also proven its positive impact on home resource management [32, 76, 55]. However, some smart homeowners have shown security concerns regarding home automation [45]. Smart locks can be incorporated in various automation scenarios within the smart home that can theoretically improve several aspects of the user's smart home experience. In Chapter 5, we explore the end users' willingness to set up automation scenarios that include the smart lock and their motivation behind creating such scenarios. Furthermore, we investigate the overall effect, positive or negative, that creating and executing such scenarios would have on the smart home and its inhabitants. Automation scenarios can include several smart home devices alongside the smart lock. While unlocking the home's front door is done through the smart lock in these scenarios, the authentication process before unlocking the door and what happens once access is granted can be controlled through the other devices included in the automation. Therefore, in Chapter 6, we explore the limitations and end user concerns associated with such automation scenarios. Furthermore, we explore types of configurations and customizations the end user needs to control in order to increase the level of security and trust in such automation scenarios.

1.1 Problem Statement and Contributions

The increasing popularity of smart home devices like smart locks presents a complex balance. While they offer convenience, they also raise concerns about security and privacy. These factors significantly affect how people decide to use and accept these technologies. Despite the potential of smart lock automation to enhance home security and user convenience through remote access and automation, their integration into the smart home ecosystem raises significant concerns [60, 101, 41]. The vulnerabilities associated with their connectivity and the internet, such as the risk of unauthorized access and data leakage, along with the complexity of device provisioning, pose critical challenges. Furthermore, incorporating smart locks into smart home automation scenarios introduces additional layers of complexity regarding user trust, perceived utility, and the management of privacy and security risks [39, 41, 95, 79]. These concerns are compounded by a lack of comprehensive user-centric research that explores the end-user's perception, requirements, and concerns regarding their integration into daily life and the broader smart home environment.

The overarching goal of this dissertation is to address the gap in existing research by focusing on the intersection of usability, security, and privacy associated with smart locks from the end-user's perspective. Therefore, we explore several aspects of smart locks which include their standalone usage (Chapter 3), their initial connection to the internet (Chapter 4), and their integration with other smart home devices within the smart home environment (Chapters 5 and 6). Through a series of user studies, this work seeks to provide a thorough analysis of the current state of smart lock technology, identify key areas for improvement, and explore the implications of smart lock usage within the context of a connected home environment. The goal is to contribute to the development of smart lock technologies and practices that prioritize user experience, security, and privacy. In summary, our work makes the following contributions:

- Provide a thorough analysis of the usability, security, and privacy of smart locks from the perspective of the end user which gives us an understanding of how to improve each of the three aspects.

- Empirically evaluate and compare two smart lock provisioning approaches, BLE and SoftAP, and identify issues and drawbacks within the provisioning processes of the two approaches.

- Explore the motivation, effectiveness, and security concerns associated with creating smart home automation scenarios that include the smart lock.

- Explore the end user's perceptions, requirements, and concerns regarding smart lock automation scenarios involving multiple smart home devices.

- Provide a set of design guidelines to improve the design and functionality of smart locks and their integration with other smart home devices while enhancing the end user's experience.

1.2 Research Outline & Questions

Several studies have examined end users' concerns, needs, and expectations regarding smart homes in general [80, 97, 33, 98, 70, 62]. However, little work has been done to explore these aspects of the smart lock in particular. To address this gap, we have conducted a series of user studies that aimed to explore several aspects of the smart lock from the perspective of the end user. Our work investigates the following overarching research questions:

- RQ1: How do end users perceive the usability, privacy, and security of smart locks and how do they mitigate those concerns?

- RQ2: What are the shortcoming and challenges of using SoftAP and BLE to provision smart locks and how do they compare in terms of usability, learning curve, security, efficiency, reliability, and their impact on other phone functions based on the end user's experience?

- RQ3: What motivates smart lock users to include them in smart home automation scenarios and how does it affect the overall security, awareness, and convenience levels within the smart home?

- RQ4: What are end users' main concerns associated with setting up smart home automation scenarios that include the smart lock in their homes, and what factors affect their decision to set up those automation scenarios?

- RQ5: How do end users perceive the limitations, pitfalls, and concerns associated with smart lock automation scenarios that involve multiple smart home devices, and what configuration options can help mitigate those concerns?

- RQ6: How does incorporating multiple smart home devices and conditions into a smart lock automation scenario affect the level of trust and perceived level of complexity end users have towards such automation scenarios?

To address the first research question, we conducted a semi-structured interview study with 29 participants (Chapter 3) who had been using smart locks for at least two months and have shared access to the smart lock with others in their household. The aim of this study was to get an insight into any usability, security, or privacy concerns they may have in relation to the smart lock. Among other findings, our results show even though the participants had security concerns such as the possibility of shoulder surfing attacks and the risk of losing smartphones, they largely believed that the convenience of using smart locks outweighed the potential security risks. The study also reveals that trust in the manufacturer and other smart lock users also plays a big part in users' attitudes towards smart lock security. One of the most frequently used features of smart locks is their ability to connect to the internet giving their users the option to remotely control them. Therefore, we conducted a comparative within-subjects user study with 60 participants (Chapter 4) which addresses the second research question related to evaluating two widely used approaches to connect the smart lock to the internet, SoftAP and BLE. The comparison was structured based on six different categories: usability, security, learning curve, efficiency, reliability, and effect on other smartphone functions. Each participant was asked to provision two ESP32 devices using both provisioning approaches. The ESP32 devices were connected to a smart lock to allow the user to lock and unlock the door if the device was successfully provisioned. Finally, each participant was asked to fill out an online survey to evaluate their experience with each provisioning approach. The results of the second study show a statistically significant difference in the users' evaluation of the two approaches in four out of the six categories (usability, learning curve, efficiency, and reliability) in favor of BLE. The study also reveals limitations associated with each of the two approaches such as the need to connect to two different networks while using SoftAP and the inconsistent Bluetooth pairing process in BLE. In our third study (Chapter 5), we utilized a mixed-methods approach to address research questions 3 and 4. A total of 21 smart lock owners participated in the study. Each participant engaged in a hands-on activity, using pen and paper to conceptualize and articulate at least four smart home automation scenarios involving the smart lock. Following this creative task, participants completed an online survey to provide structured feedback on their own scenarios. Through the analysis of 87 automation scenarios created by the participants, the results of the study emphasize the effectiveness of creating smart home automation scenarios that include the smart lock in enhancing several aspects of the smart home experience such as security, convenience, and awareness. Additionally, our findings provide a general categorization of such automation scenarios based on the purposes they serve within the smart home as well as shed light on end users' usability, security, and privacy concerns associated with such automation scenarios. Around 84% of the automation scenarios created by the participants contained at least 2 smart home devices. In such automation scenarios, both the authentication process before unlocking the door, and the security measures taken once the door is unlocked can be controlled through the other smart home devices involved in the scenario. Therefore, in our fourth and final study (Chapter 6), we conducted semi-structured interviews with 30 participants to answer research questions 5 and 6. During the interviews, we showed the participants a sequence of videos, where each video incrementally introduced additional conditions or smart home devices into an automation scenario designed for automating the unlocking of the user's home to provide a service (in-home package delivery). Our objective was to explore the users' perceptions of the limitations and pitfalls associated with the smart home devices included in each video. Furthermore, we aimed to gain a better understanding of the type of settings and configurations the end user needs to have control over to help mitigate those limitations and concerns. Our findings showed that a major limitation of the other smart home devices involved in the automation scenario is their lack of accuracy which can lead to unauthorized access or false security breach alarms. Other limitations also included the possibility of failing to trigger a critical chained automation, the lack of communication with the humans involved in the automation, and the lack of re-locking assurances once the automation is complete. However, the results also show that many of those limitations can be mitigated through giving the end user more control over various settings or configurations the other smart home devices involved in the automation scenario. These configurations include manual override, more authentication options, and the ability to set more constraints and restrictions over when and how the automation should be executed. Our findings also show that while including more smart home devices and configurations into a smart lock automation scenario increases the level of security and trust in that scenario, it also increases the perceived level of complexity. Therefore, there is a need to simplify the creation of such automation scenarios to make them more user-friendly and less complicated. In Chapter 7, we discuss the main findings and contributions of this dissertation as well as provide a set of design guidelines that aim to improve the usability, security, and privacy of smart locks.

CHAPTER 2: BACKGROUND

2.1 Smart Locks

2.1.1 Smart Locks Architecture

Smart locks consist of three main components which are an electronically augmented deadbolt installed on the door, a companion mobile application installed on the user's smartphone, and a remote web server [90]. In order to control the smart lock, users must have an active account on the companion mobile application. As far as architecture is concerned, smart locks can use one of two types of network designs. Those two network designs are the Device-Gateway Cloud (DGC) and Direct Internet Connection [40].

Device-Gateway-Cloud (DGC). Since most smart locks store their data in the cloud, smart locks require internet connectivity in order to connect to their remote servers to receive updates on access control instructions. A smart lock utilizing this architecture is not directly connected to the Internet. It is, however, possible for such locks to retrieve the necessary information from the cloud in two different ways. One approach involves connecting the lock to the user's smartphone via a local wireless channel, such as Bluetooth Low Energy (BLE) [90], and then using the smartphone's internet connection as a gateway for connecting to the lock's remote servers and retrieving the necessary information and updates. The downside of this approach is

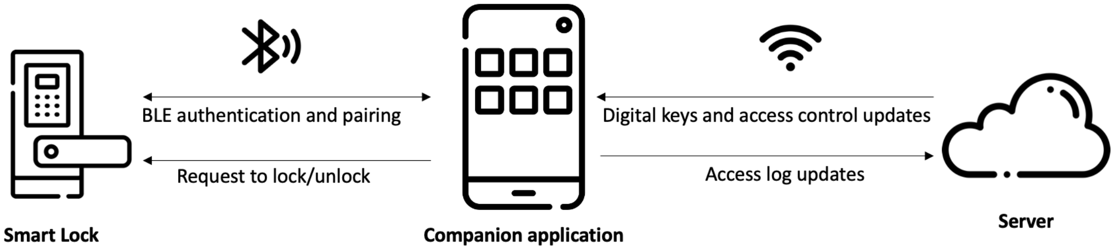


Figure 1: Device-Gateway-Cloud (DGC) architecture

that in order to control and use the features of the smart lock, the user must be within Bluetooth range of the lock. To overcome this issue, smart lock manufacturers that construct their locks using the DGC architecture (figure 1) typically provide users with the option to purchase a Wi-Fi bridge (usually sold separately) as an alternative method of connecting the smart lock to the server without relying on the smartphone's internet connection. The Wi-Fi bridge communicates with the smart lock via Bluetooth or another short-range wireless technology, such as Z-Wave. Using this setup, smart locks can connect to the cloud as long as the Wi-Fi bridge is working correctly, allowing users to control their locks remotely using their smartphones without being within Bluetooth range.

Direct Internet Connection (DIC). Smart locks utilizing this design architecture (figure 2) an integrated Wi-Fi modem which enables them to connect to the home's Wi-Fi network [90]. This connection allows the locks to directly access remote servers for essential information and updates. Users can manage the lock remotely via a companion app on their smartphone. However, because these smart locks rely solely on a direct internet connection for all cloud communications through their Wi-Fi, there's a risk that users might find themselves unable to access the lock if they

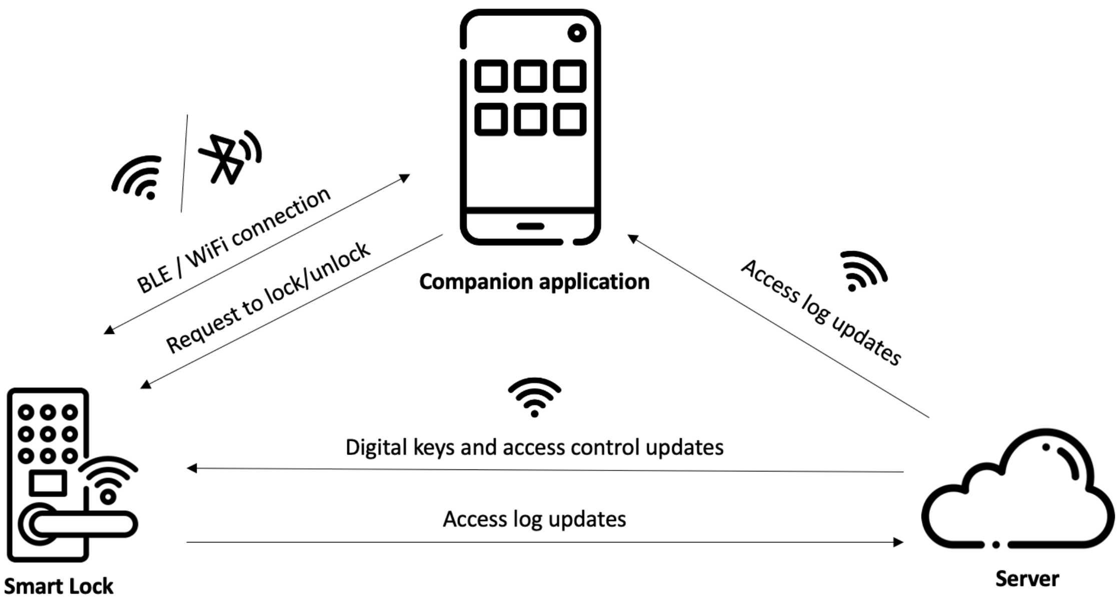


Figure 2: Direct Internet Connection (DIC) architecture

are disconnected from the internet.

2.1.2 Access Control

Most smart locks employ role-based access control systems, which come with predefined access tiers and allow the lock's owner to specify the dates and times users are permitted to use the lock [90]. Typically, commercial smart locks feature four primary levels of access: owner, resident, recurring guest, and temporary guest [40]. An owner-level user has the authority to issue and revoke electronic keys, access the log of entries, and lock or unlock the door anytime. In contrast, resident-level users are restricted from granting or revoking access to others and cannot view the entry log, although they retain the ability to use the lock whenever they choose. Recurring guests are granted access only at specific times designated by the owner (such as every Thursday from 8am to 10am), whereas temporary guests can use the lock for a set duration, like 24 hours.

2.1.3 Authentication and Authorization

To operate a smart lock via their smartphones, users are required to register for an account through the lock's website or its companion application. Their account credentials are then used to authenticate their identity, ensuring that the lock can only be operated by individuals with the correct credentials. This allows users to control the lock from any device equipped with the lock's app [87]. The permissions to access the lock are dictated by the user's digital key access level, with the smart lock's access permissions stored on the cloud. Consequently, verification against the access list occurs every time a user attempts to use the lock. Smart locks equipped with Wi-Fi can directly connect to the cloud to verify a user's authorization based on their access level for specific times and dates. In contrast, smart locks using a Direct to Cloud (DGC) architecture depend on a smartphone or Wi-Fi bridge to access the cloud for authorization information, determining if a user is allowed to use the lock at a given time and date [40].

2.1.4 Smart Locks Security and Privacy

Smart locks have not been extensively studied from the point of view of the end user with regards to usability, privacy, or security. However, several papers have examined privacy and security from the perspective of researchers and based on their own testing of various smart lock models. Ye et al. [96], for example, analyzes the security of the August smart lock to illustrate any possible threat models. They identified possible security concerns related to the analyzed August smart lock model which might be a threat to the security and privacy of the end user. Those concerns include the fact that the lock was susceptible to several attacks such as Denial of Service (DoS) and that allows an attacker to obtain the lock owner's personal information which puts their privacy at risk. Ho et al. [40] also analyzed 5 commercially available smart locks in terms of their privacy and security to identify possible vulnerabilities as well as propose viable defenses against such vulnerabilities. According to the paper, some of the analyzed smart locks were found to be susceptible to two types of state consistency attacks as well as relay attacks, unwanted unlocking among other issues. The paper also proposes frameworks to defend against such attacks. Other research papers [26, 68, 44, 13, 90, 69] aim to propose frameworks that can improve the security and privacy of smart locks either through using the blockchain technology [26], face recognition [68, 44], or steganography and cryptography [13]. The lack of granularity within access control management systems used in commercially available smart locks has also been recognized by several papers as an issue that might compromise the security and privacy of smart locks. Xin et al. [90] propose an attribute-based access control system instead of the role-based system that is currently used in most smart locks that increases the granularity of access control within smart locks. Moreover, it aims to solve other security attacks such as state consistency attacks, unauthorized unlock, and the cascading deletion of permissions.

2.1.5 Smart Home User Studies

As a member of the smart home device family, smart locks share several common attributes and functions with their counterparts. Most notably, these devices are typically managed through a dedicated companion app and maintain access logs. Previous studies have investigated various facets of smart home device usability, exploring topics like the motivation behind investing in such devices and the impact they have on enhancing domestic life quality. In a user study conducted by Oliveira et al. [65], a significant number of participants expressed that the adoption of smart home devices elevated their sense of security and control within their homes. Participants also identified additional incentives for adopting these devices, such as the convenience they offer and the sense of staying abreast of technological advancements. Furthermore, Coskun et al. [25] stated that smart home devices are generally expected to outperform their traditional counterparts in terms of functionality. However, the reliance solely on smartphone control and the absence of manual control options for some of the simplest yet most frequently used features was found to heighten user frustration [28]. This reflects the necessity for a balance between technological advancement and user-friendly design in the development of smart home devices.

Prior studies have also explored the security and privacy concerns of end-users regarding smart home devices. For instance, Haney et al. [35], in their study involving interviews with 40 smart home device users, sought to understand any security or privacy worries these users may harbor and the strategies they adopt to alleviate these concerns. Their findings pointed out that the principal worry for users centered around devices equipped with audio and video features potentially being breached, a sentiment echoed by Zheng et al. [99] in their study. This suggests that users may express less concern over the security implications associated with other smart home devices lacking audio or video capabilities, such as smart locks. A number of studies, such as Haney et al. [33] and Tabassum et al. [80], report a seeming lack of concern among certain users regarding the security and privacy aspects of smart home devices. However, this apparent lack of concern doesn't necessarily denote lack of awareness. In fact, the studies indicate that this lack of concern often stems from a trust in the device manufacturer's ability to rectify any security issues, or a belief among users that they are unlikely to be targets for potential attackers [97]. Some users expressed that their concern was confined only to smart home devices located in sensitive areas within their homes, suggesting a nuanced understanding of privacy and security concerns in different contexts [98]. Zlatolas et al. [63] also conducted a survey study with 306 participants in order to get an insight into their security perceptions of IoT devices within the smart home. The findings of the study revealed a positive impact of device vulnerability awareness on the perception of security importance. Meaning that users who were more aware of the security vulnerabilities of smart home devices also believed in the importance of implementing mitigation strategies in order to protect their smart home devices against possible security threats and vulnerabilities.

While those studies explore smart home devices in general, it is equally important to conduct studies with a narrower focus on smart locks. Smart locks have unique operational purposes within the smart home which may introduce distinct security and privacy challenges. Similarly, they may have specific mitigation strategies tailored to these unique challenges. For instance, our first study reveals that video doorbells and chain guards are frequently used to mitigate the privacy and security issues of smart locks. Such mitigation strategies may not be relevant for other smart home devices. In fact, several user studies were dedicated to exploring particular devices within the smart home, like smart speakers, in order to gain a better understanding of the limitations and mitigation strategies unique to those devices [19, 22, 42, 48, 56]. Tabassum et al. [81] conducted a user study with 39 participants (18 owners of smart locks and video doorbells and 21 non-owners) to explore the users' perceptions of the configurations and controls available in smart locks and video doorbells. Some participants reported concerns regarding unauthorized attempts to unlock the smart lock, but they mostly turn the notifications on in order to be alerted to such attempts. Other participants were also concerned about hacking attempts which might allow adversaries to remotely unlock the door and provide physical access to the home. For most of the security concerns, some participants stated that their only way to cope with those concerns was to put trust in the manufacturers' security measures. However, unlike Tabassum et al., our study puts more focus on examining smart locks users' level of concern regarding specific aspects of the security and privacy of the smart locks as well as investigating the usage behaviors of smart lock users.

The results of our first study mostly align with previous work while identifying additional privacy and security concerns and mitigation strategies specific to smart locks. Furthermore, our work investigates the usage behaviors of the smart lock's end users.

2.1.6 Wi-Fi Provisioning

Smart locks need to be connected to the home network in order for the user to unlock their full potential and functionality, such as the ability to remotely control access to the lock or set up specific automation scenarios [8]. This step is called

Wi-Fi provisioning, and it requires the end user to provide the smart lock with the Service Set Identifier (SSID) and password for the home network to get the smart lock connected to the internet [100]. However, smart locks are headless devices that lack a user interface or a keyboard through which the user can provide the SSID and the password to the lock. Therefore, several Wi-Fi provisioning schemes take advantage of the user's smartphone as an interface to collect the home network credentials from the user and communicate them with the smart lock. Two of the most commonly used approaches to provision smart locks are SoftAP and BLE.

Software-enabled Access Point (SoftAP). SoftAP is a provisioning scheme that allows the users of headless IoT devices, such as smart locks, to configure their Wi-Fi network's SSID and password [61]. The smart lock in this case uses the embedded Wi-Fi radio to create a temporary access point that the user's smartphone can connect to. The user is required to install the lock's companion application on their smartphone, which will guide them through the process of connecting to the temporary access point and sharing their home network credentials with the lock. The temporary access point is then terminated by the lock and a connection to the home network is established using the credentials provided by the user.

Bluetooth Low Energy (BLE) BLE is an out-of-band (does not require Wi-Fi radio) Wi-Fi provisioning method that can be used to provision smart locks [49]. In order to utilize this approach, the smart lock must be equipped with a BLE chipset. The un-provisioned smart lock broadcasts advertising packets which allows the user's smartphone to discover it and then connect to it. Once a secure Bluetooth connection is established, the lock's companion application collects the user's home network credentials and communicates them with the IoT device through Bluetooth. These credentials are then used by the device to connect to the home network and to access the Internet.

While limited research has explored the user experience aspects of Wi-Fi provisioning for smart home devices, various studies have explored different facets of the provisioning process. Reiter et al. [73] stressed the significance of security, reliability, and ease of use when selecting a Wi-Fi provisioning approach for smart home IoT products. These factors are crucial as these devices target smart homeowners who may not have a deep understanding of the provisioning process. The provisioning process entails sharing home network credentials with the smart home device being configured, making it susceptible to man-in-the-middle attacks [52]. Granata et al. [31] discovered that during the Wi-Fi provisioning process, the SoftAP network broadcasted by a smart home device could enable an attacker to retrieve the device's private key, subsequently allowing the attacker to decrypt the user's home network credentials. Additionally, in their security analysis of SmartCfg, a Wi-Fi provisioning approach for smart home devices, Li et al. [49] found that while SmartCfg was effective in configuring Wi-Fi, several design-related issues in SmartCfg solutions compromised smart home security and privacy. Notably, six out of eight manufacturers analyzed in the study provided SmartCfg implementations with security flaws that could grant attackers access to the end user's home network. Similarly, Valente et al. [86] discussed another security concern related to provisioning IoT devices, namely the lack of encryption for the Access Point (AP), resulting in home network credentials being transmitted in plain text, susceptible to interception by eavesdroppers. Liu et al. [51] identified an issue within the provisioning process employed by JoyLink, a smart home solution supporting over 6100 devices in China with Wi-Fi or BLE modules. This issue could lead users to connect their smart home devices to a counterfeit network set up by an attacker, rather than connecting to their actual home network. However, while prior work explores the technical aspects of provisioning approaches for IoT headless devices, our second study focuses specifically on exploring end users' perceptions and concerns associated with using two widely used provisioning approaches, SoftAP and BLE, to provision the smart lock.

2.1.7 Smart Home Automation Scenarios

Home automation is typically set up and controlled through hubs or platforms (e.g., Samsung SmartThings, Amazon Echo, Google Home, and Apple HomeKit). These systems act as intermediaries to facilitate communication among various smart devices from different manufacturers [20]. Their primary goal is to offer homeowners centralized control over their devices. Additionally, these platforms allow for the creation of ”trigger-action” automation scenarios involving multiple smart devices. For instance, with SmartThings, a user can configure an automation (referred to as a ”scene”) that triggers the hallway's smart lights to turn on for 60 seconds when the smart lock is unlocked from the outside [88]. Online workflow automation platforms like IFTTT (If This Then That) and Zapier are also utilized by some homeowners for similar purposes [2, 3]. Research indicates that most users can easily create such automation scenarios with these systems, even without any programming knowledge [85]. While different systems may require varying syntax for scenario creation, studies have found a preference among users for if-then (or when-then) statement formats, akin to those used by platforms like IFTTT [27, 78].

Several user studies have explored users' limitations and requirements associated with creating and setting up smart home devices. Soares et al. [78] conducted a survey with 20 participants to understand the types of automation rules users wish to implement in their homes. The paper systematically categorized 177 home automation scenarios created by the participants into seven interaction categories to uncover common patterns in user expectations for smart home interactions. Unlike our work in chapter 5, this study categorized the participants' created automation scenarios based on their format similarity, not the motivation behind creating those scenarios. Furthermore, our study necessitates the inclusion of the smart lock in each automation scenario. Mattioli et al. [59] conducted a user study with 34 participants lacking IoT programming experience who were asked to create smart home automation scenarios. The study aimed to identify whether current trigger-action programming (TAP) languages are equipped with the necessary constructs and operators to realize the envisaged automations. The participants created 204 smart home automation scenarios. Through the analysis of 204 desired home automations, the study uncovered a critical need for enhancing TAP languages to accommodate more complex, user-defined scenarios. Smart home automation takes advantage of the interconnected nature of smart home devices in order to improve various aspects of the home inhabitants' lives. Prior research [16, 18, 93, 21] explored the factors influencing the user's decision to create smart home automation scenarios. Their findings suggest that convenience, enhanced security awareness, and improved energy consumption are key drivers behind the adoption of smart home technologies. Our third study in Chapter 5 narrows the lens to specifically examine the motivations driving the integration of smart locks into home automation scenarios.

Understanding user concerns and the factors that influence the decision to integrate smart locks into home automation setups is crucial. Brush et al. [18] highlight real-world challenges and opportunities in home automation, pointing to usability and interaction as significant considerations for users. Moreover, Touqeer et al. [83] provide a systematic review of security and privacy-preserving challenges in smart home environments, emphasizing the importance of addressing these concerns especially when more devices have to communicate with each other. Furthermore, research into smart home security has highlighted several vulnerabilities inherent to complex automation scenarios that involve multiple smart home devices. Several studies have pointed out that scenarios involving multiple smart devices could suffer from various vulnerabilities such as integrity violations and feature interactions [95, 79]. These vulnerabilities arise when devices act on information from less trusted sources or when conflicting rules create logical inconsistencies, undermining the reliability of the system.

Our work in chapters 5 and 6 builds upon the existing body of smart home automation research by offering a detailed exploration of the end user's perception regarding incorporating smart locks into smart home automation scenarios. It seeks to fill the literature gaps regarding user motivations, specific impacts, concerns, and configurations specifically associated with smart automation scenarios that include the smart lock.

CHAPTER 3: EXPLORING THE USABILITY, SECURITY, AND PRIVACY OF SMART LOCKS FROM THE PERSPECTIVE OF THE END USER

This study has been published in the Symposium on Usable Privacy and Security (SOUPS), 2023 in California, USA [36].

3.1 Research Purpose

Smart home devices have recently become a sought-after commodity among homeowners worldwide. Among these, smart locks have experienced a marked surge in market share, largely due to their role as a primary safeguard for homes and personal possessions. Several studies [35, 99, 97, 98] have explored concerns related to the usability, security, and privacy of smart homes from the user's perspective, while other researchers [96, 40, 69] have examined the issues and possible mitigation strategies related to the privacy and security of smart locks from a technical perspective. However, little research has been done on smart locks' usability, privacy, and security from the end user's perspective, creating a gap in the research. To address this, we conducted semi-structured interviews with 29 smart lock users who had used their locks for at least 2 months before the interview and had used their smart locks to share access with other users. As part of this study, we investigated the following research questions:

- RQ1: What aspects of the smart lock's design and functionalities make it appealing to users from a usability standpoint?

- RQ2: What privacy and security concerns do end users have regarding smart locks?
- RQ3: How do end users deal with their privacy and security concerns?
- RQ4: What are the end user's perceptions regarding how the security and privacy of smart locks can be improved?

3.2 Methodology

We conducted a semi-structured interview study with smart lock users in order to gain a deeper understanding of smart lock users' opinions on different aspects of the lock based on their experience using the lock. The methodology choice allowed for a comprehensive and nuanced exploration of users' experiences, concerns, and suggestions for improvements in smart lock technology.

3.2.1 Participants

We sought participants who had used their smart locks for at least two months and shared electronic keys (digital keys) with others (family members, neighbors, parcel delivery, etc.). The participants were recruited through an advertisement post on the SmartHomes sub-reddit on the Reddit forums as well as a mass email sent to the students and employees at the university. Potential participants were asked to fill out a screening survey which contained questions such as what type of smart locks they have, for how much time have they been using them, and how many people do they share the locks with. Such questions allowed us to verify the participants' eligibility to take part in the study. A total of 29 participants were recruited. Among the participants, 10 were males and 19 were females, and all of them live in the United States. Most of them (n=16) were in the age group of 26-35 while 10 participants were in the age group of 18-25 and 3 participants were in the age group of 36-50. The majority of participants (n=24) stated that they had been using at least one smart lock for more than 4 months while 5 other participants had used their locks for 2-4 months.

3.2.2 Procedure

A researcher contacted participants who were selected for the study based on the screening survey to arrange a date and time for the interview. According to each participant's preference, all interviews were conducted virtually over Zoom, Google Meet, or Webex. Interviews lasted about 40 minutes on average and each participant was given a $10 Amazon gift card for participating in the study. The study was approved by the university's Institutional Review Board (Protocol #21-0295). Each interview was divided into two sections. The first part focuses on exploring the usability aspect of the smart lock while the second part focuses more on the privacy and security aspect of smart locks. Each part contained open ended questions as well as Likert scale questions. Participants were asked to explain their reasons for choosing a particular answer in order to better understand their perspective. Towards the end of the privacy and security section of the interview, we ask the participants to watch a YouTube video that was prepared and uploaded by one of the researchers which contains a demonstration of 2 types of state consistency attacks that some smart locks are susceptible to. Once the participant finishes watching the video, the

Table 1: Participants' demographic information - first study

Participant	Gender	Age group	Education	Occupation
P1	Female	18-25	Bachelor's	Educator
P2	Male	26-35	Graduate student	Research scientist
P3	Female	26-35	Bachelor's	Athletic trainer
P4	Male	26-35	Masters	Student
P5	Male	26-35	Bachelor's	Unemployed
P6	Female	18-25	-	Student
P7	Male	26-35	Bachelor's	High school teacher
P8	Male	26-35	Bachelor's	Student
P9	Female	26-35	Masters	Student
P10	Female	26-35	Some college	Student
P11	Female	36-50	Graduate degree	Student
P12	Male	26-35	Master's degree	IT Professional
P13	Female	26-35	Some college	stay at home mom
P14	Female	26-35	Some college	Student
P15	Female	18-25	Some college	Nanny
P16	Female	26-35	Some college	Student
P17	Female	18-25	Some college	Pharmacy technician
P18	Female	18-25	Grad student	Student
P19	Female	26-35	Grad student	Student
P20	Male	36-50	Masters	Data analyst
P21	Female	18-25	Some college	Student
P22	Male	26-35	Some college	Student
P23	Male	36-50	PhD	Professor
P24	Female	26-35	Master's	Health educator
P25	Female	18-25	Some college	Student
P26	Female	18-25	Some college	Student
P27	Female	26-35	Associate degree	Customer Service Rep
P28	Female	26-35	Grad student	Teacher
P29	Male	18-25	Some college	Student

researcher asks them some questions regarding the two issues illustrated in the video in order to evaluate their level of familiarity and concern regarding those smart lock vulnerabilities.

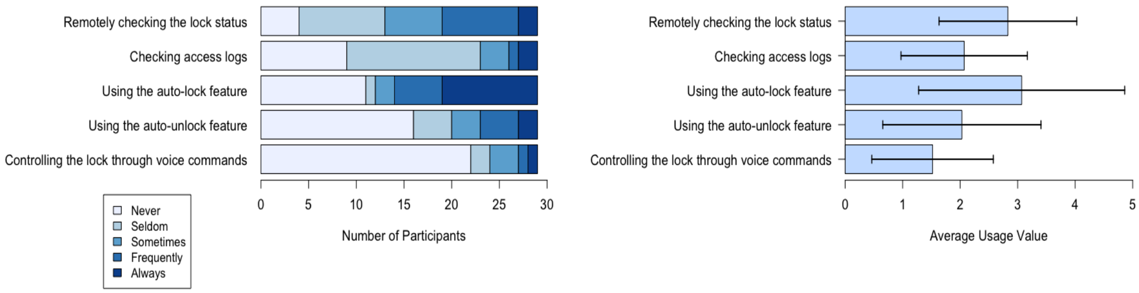
3.2.3 Data Analysis

Each interview conducted was audio-recorded and subsequently transcribed for analysis. Our data collection was bifurcated into qualitative and quantitative components. The qualitative data was processed using an inductive coding approach. This procedure was carried out independently by two researchers who then engaged in discussions to finalize the coded data, thereby resolving any potential disagreements. The final codebook consisted of 13 main codes and 53 subcodes. As for the quantitative data, our main approach involved the use of descriptive statistics, given that the bulk of our interview questions were not formulated to test for statistical significance among variables. Nevertheless, for the few questions that did require a test of statistical significance, we employed the non-parametric Wilcoxon Signed Ranks Test, considering the data didn't adhere to a normal distribution pattern.

3.3 Results

3.3.1 Usage Behaviors

The purpose of this section of the paper is to identify the popularly used smart lock features as well as understand end users' usage behaviors. Investigating these aspects of smart locks leads to a broader understanding of what aspects of the smart lock's design and functionalities make it appealing to end users from a usability standpoint (RQ1).



(a) Usage frequency

(b) Average usage frequency

Figure 3: Smart lock's features usage frequency

Adopting a Smart Lock. As an emerging technology, smart locks have their strengths and weaknesses in terms of privacy, security and usability, especially when compared to traditional locks that homeowners are already familiar with. In response to a question about whether participants hesitated before switching to a smart lock from a traditional lock, 12 participants said that they had some concerns initially and that it took them some time to become convinced that adopting a smart lock was the right choice. The two main reasons behind the hesitation were price and security. A smart lock can cost up to ten times as much as a traditional lock, which can be a big financial commitment. The security of smart locks was also a big concern among some participants who hesitated before adopting a smart lock.

Asked why they chose to switch from a traditional lock to a smart lock, the majority of participants (n=20) said it was because of how convenient using a smart lock is compared to using a traditional lock, whereas only 8 participants cited security as a reason for using one.

Automation. By using communication protocols such as Zigbee and Z-Wave, smart home devices can communicate with each other to automate tasks. In spite of this, only 4 out of 29 participants created automation scenarios that utilized smart locks. P2, for example, has an automation scenario set up so that when an authorized user unlocks the smart lock, the home security alarm is automatically disabled without having to manually disable it every time a resident enters the house. Many automation scenarios can be set up using the smart lock to increase the level of convenience and security of a house, but most participants were not aware of the possibility of creating automation scenarios that include the smart lock.

Features and Capabilities. Compared to traditional locks, smart locks offer more features besides the basic function of locking and unlocking doors. The three most popular features that participants mentioned, unprompted, when asked to describe the features of their smart locks that they liked most were the ability to remotely control the lock (n=14), keyless entry (n=10), and the ease of giving others access (n=5). The ability to remotely check if the door is locked (n=3), the ability to unlock the door in multiple ways (n=3), and the auto lock feature (n=2) were not as popular among participants.

We also engaged the participants to evaluate their usage frequency of distinct smart lock features. To do this, we used a Likert scale that used the following designations: ‘never’, ‘seldom’, ‘sometimes’, ‘frequently’, and ‘always’, where ‘never’ corresponded to 1 and ‘always’ to 5. The ”auto-lock” and the ”remote lock status checking” features emerged as the most utilized among the smart lock features, as illustrated in Figure 3. The popular preference for these features stems from the heightened sense of security they afford to participants, particularly when they’re away from home, by

Table 2: Reasons for enabling smart lock notifications

Reason for turning on notifications	**Count**
Get alerts when the deadbolt is jammed	10
Get alerts about who is accessing the house	8
Get security alerts	4
Get battery alerts	1

guaranteeing the door is securely locked.

In terms of notifications, the majority of participants (n=21) stated that they keep smart lock notifications on. According to participants, the most common reason for enabling notifications is to be notified when the deadbolt jams on the door frame and does not lock properly, which is a common problem with smart locks. Notifications were also enabled to keep track of who was accessing the house in real-time, get alerts when the smart lock's battery was low, and see who was entering the apartment in real-time. in contrast, some participants (n=8) stated that they prefer to turn notifications off either because they don't prefer to use the app at all or because they find notifications annoying. Another participant was concerned that turning notifications on could violate other household members' privacy.

Managing Electronic Keys. Electronic keys are usually shared and revoked through the companion application. They can be in the form of a token on the user's smartphone or an access code that the user needs to enter every time they unlock the door. Participants were asked to evaluate two factors - ease of use and reliability - when it came to sharing their smart locks with others. Twenty-two participants found sharing access to the smart lock quite easy, but seven found it quite challenging, especially for older or less tech-savvy individuals. Among the participants, only two found it difficult to revoke someone's access to the smart lock. It is also worth mentioning that 13 participants reported that they never felt the need to revoke another person's access. Participants did not report any issues with the reliability of the access sharing process. When they share access with others, the other person is always able to operate the lock based on their access rights with no issues.

Access Sharing Patterns. Access to the smart lock is usually shared through sending an invitation either by phone or email. When the other person accepts the invitation, they would be able to control the lock to the extent of their access level. Another way to share access to the smart lock is through an access code, usually 4 to 6 digits long, that allows the other person to unlock the door. Out of 29 participants, 13 reported that they only share access to their locks with people who live with them, such as roommates or family members. They feel more secure knowing that only the residents can unlock the door. The rest of the participants (n=16) stated that they give access to those who live inside the house, as well as others who don't live in the house such as guests, babysitters, contractors, dog walkers, etc. However, it is common for them to give "temporary access" to some of those who do not live in the house. For example, a dog walker who walks the dog from 10am to 11am can only unlock the door during these hours. Others, such as visiting family members or friends, can access the house at any time, but do not have full access to the lock in terms of checking access logs, giving access to others, or any other features besides locking/unlocking the door.

Usability Improvements Although some participants were fairly satisfied with the smart lock's current features, others believed that it could be significantly improved by making some modifications and adding some new features. Some of these modifications include:

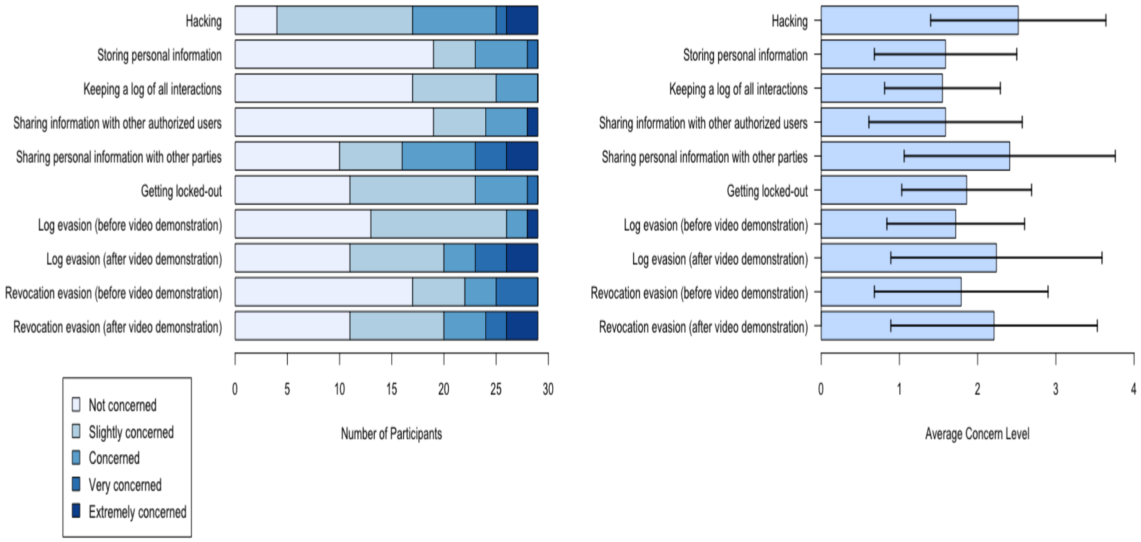
Improving the Battery. In the case of smart locks, a dead battery can leave someone locked out of their home, especially if the lock doesn't offer any other means of unlocking it. Some participants (n=3) suggested different ways to improve the battery.

> **P27:** *"It would be nice if there was such thing as like a mini key fob that I could put on the bottom of the lock, just give it a charge so I can unlock it real quick to get into the house. That way, I could have that on my keys, and if I'm locked out when the battery's dead, I could just kind of like jump start it."*

Smart Watch Integration. One of the participants suggested allowing smart locks to be operated by smart watches. This would be a very convenient feature especially for runners who prefer to leave their smartphones at home and only wear their smart watch. However, this feature already exists in some smart locks and watches such as the August smart locks that are compatible with Apple watches. Not all commercially available smart locks and smart watches support this feature though.

3.3.2 Security and Privacy Concerns

The purpose of this section is to explore and analyze the participants' insights regarding their privacy and security concerns (or lack thereof) with their smart locks (RQ2). In order to ensure that they have had enough time to develop an opinion



(a) Level of concern

(b) Average level of concern

Figure 4: The participants' level of concern associated with different smart locks privacy and security threats

regarding the security and privacy controls of their smart locks, all participants have owned/used their smart locks for at least two months prior to the interview date and have used shared access to the lock with other users.

To gain an overall comprehension of the primary security and privacy concerns that smart lock users possess, we initially asked the participants about any general security or privacy concerns they have associated with smart locks (Table 3). This

Table 3: The participants' security and privacy concerns related to smart locks (unprompted)

Security or privacy concern	**Count**
Hacking	9
Using and sharing access codes	7
Physical tampering with the lock	3
Losing the smartphone	2
Getting locked out	2
Revocation evasion	1

was followed by questions regarding their degree of concern about specific security and privacy issues related to smart locks (Figure 4). The specific threats presented to the participants were formulated based on findings from previous research in the fields of smart locks and smart home security. These threats included concerns of log evasion, log revocation, and the possibility of being locked out, as discussed in previous studies such as [53, 40, 67, 87], which explored the security vulnerabilities prevalent in some smart lock systems. Furthermore, we asked the participants about concerns regarding hacking threats, storage of personal information, maintaining a log of all interactions, sharing personal details with other authorized users, and the possibility of information being disseminated to other parties. These additional concerns were also derived from previous research [35, 99, 84, 97], which explored security concerns of smart home users associated with smart home devices. The participants' responses were recorded using a Likert scale, with designations ranging from 'not concerned' (assigned a score of 1) to 'extremely concerned' (score of 5).

Profiling and Information Collection. The majority of participants (n=19) expressed no concern about the smart lock collecting personal information about them and the residents of their home, which is consistent with previous research such as [35]. In fact, some participants appreciated that this sort of information is collected which can help improve the quality of the access logs. Some of those "not concerned" participants also believe that the information the lock collects is not significant and cannot harm them in any way, although when asked about the type of information they think the lock collects, some of them thought the lock only collects their name and email which is not accurate [1]. However, some other participants were more concerned about selling or sharing this information with other parties. P18, who was extremely concerned about sharing their information with third parties, says:

> **P18:** *"Sharing my privacy information with some other third parties is what I think is illegal and I don't feel it will be safe, because I trust that particular company and I don't trust the other."*

Based on the type of information the smart lock collects about its users and the fact that the smart lock also has the capability of sending and receiving information to and from other smart home devices, this creates the possibility of a profiling issue which is a huge privacy risk that most smart home users have to deal with. None of the participants explicitly mentioned "profiling" which could be because they are not familiar with that term or not even familiar with the type of information the smart lock collects and that it can lead to profiling. However, some participants were worried about others knowing the schedule of exactly when they are home and when they are not.

Hacking. When asked, unprompted, about which privacy and security issue participants were concerned about the most when it comes to their smart locks, hacking was by far the most mentioned concern (N=9), which is in line with prior studies such as [35]. However, although 3 participants expressed extreme concern about hacking, a large portion of the participants were only slightly concerned (N=13) mostly because they don't believe themselves or their houses to be a potential or a high priority target for hackers, which seems to be a common thought process for a lot of homeowners [80, 34].

> **P22:** *"slightly concerned. I recognize that it can happen. But I don't see that our house is being a high priority target. It's not like we're particularly I don't feel like that we would be. I don't foresee us. Basically, security through obscurity is what I'm banking on. I don't see why anyone would want to get into our house specifically."*

Using and Sharing Access Codes. Seven participants (n=7) expressed concern about the security implications of using or sharing their access codes. For example, two participants were concerned about an adversary observing them or other residents while using their access code to unlock their smart lock, which could allow the adversary to unlock their door later. Other participants (n=3) were more worried about the wear and tear of the keypads or touchpads that come with their smart locks (the most frequently used buttons wear faster than the others). Touchpads can show fingerprints, which can help an adversary figure out the access code based on observing how the keypad or touchpad looks based on which 4 buttons are used the most. Additionally, one participant was concerned about sharing access to the lock with others since they might not take security very seriously and make it easier for someone else to gain unauthorized access.

Physical Tampering with the Lock. The physical security of the smart lock was a concern for some participants (n=3). P5 is concerned about the lock itself being stolen for how expensive it is. Two other participants, on the other hand, were worried about the possibility of a burglar tampering with the lock and being able to gain access to the home. Especially in smart locks that have a physical keyhole as an extra option to unlock the door which can make it susceptible to picking just like traditional locks.

Losing the Smartphone. For a smart lock user, losing their smartphone is equivalent to losing their home key, especially if they do not secure their smartphone with a strong passcode or if they have the auto-unlock feature ON, which allows the lock to unlock itself when the smartphone is within a certain range of the lock without having to unlock the smartphone's passcode. Two participants were concerned that this could happen and an adversary could gain access to their homes. However, most smart locks already give their users the option to log in to their accounts through a website and disable the lost phone to avoid such an issue.

Getting Locked Out. Getting locked out of the home can be a huge security issue especially when it happens late at night or in a dangerous neighborhood. Although only about 28% of the participants (n=8) reported that they were locked out of their homes at least once because of the smart lock, the majority of participants (n=18) showed at least a slight concern that they might get locked out due to a smart lock related issue such as losing connectivity to the internet or a dead battery. Most of those who had already been locked out in the past also mentioned that it was indeed either an internet connectivity problem or a battery related issue.

Log Evasion and Revocation Evasion. Log evasion and revocation evasion affect smart locks that follow a Device-Gateway-Cloud architecture since they mostly rely on Wi-Fi bridges or the user's smartphone to access the internet [40]. Through a companion app on the user's smartphone, these smart locks retrieve the access control list from a remote server and verify it with the lock through Bluetooth to determine if a particular user is authorized to operate the lock. Unless the user's phone is connected to the internet or a Wi-Fi bridge is available, the lock cannot retrieve the most recent access control list. As a result, even if user X's access to the smart lock was recently revoked, they can still operate the lock until the lock can connect to the internet and update the access control list. This is called revocation evasion which is the first type of state consistency attacks. Likewise, a legitimate user, who has authorization to operate the lock, can also avoid appearing in the access logs simply by turning off their smartphone's internet connection. This is the second type of state consistency attack (evasion of access logs).

Although state consistency attacks have been heavily discussed in the literature [53, 40, 67, 87], only 3 participants stated that they were aware of the revocation evasion issue within smart locks while only 2 participants were aware of the log evasion issue. Users tend to be less concerned about security issues they are not familiar with. To give participants an overall understanding of the issues and how they can occur, we prepared a video demonstrating two types of state consistency attacks on one of the most popular smart locks on the market. We first asked the participants, on a scale of 1 to 5, how concerned they were regarding each of the two issues before watching the video and then again after watching the video towards the end of the interview. Our aim was to examine how raising the level of awareness of security threats affects users' level of concern about those threats.

The results showed an increase in the level of user concern regarding both of the security issues after watching the video as illustrated in Figure 3a and table 4. In order to determine whether statistically significant differences exist between the par-

Table 4: The mean and standard deviation for the participants' level of concern regarding state consistency attacks in smart locks before and after watching the demonstration video

Pre-Video ($\bar{x}$, s)	**Post-Video ($\bar{x}$, s)**	**Z-value**	**P-value**
Log Evasion Threat			
(1.72, 0.882)	(2.24, 1.354)	-2.334	**0.020**
Revocation Evasion			
(1.79, 1.114)	(2.21, 1.320)	-1.530	0.126

ticipants' level of concern before and after watching the video of the two security issues, a Wilcoxon Signed Ranks Test was performed. The tests revealed a statistically significant difference in the participants' level of concern in regards to log evasion (Z= -2.334, p=0.020, α= 0.05). However, the tests did not reveal a statistically significant difference in the participants' level of concern in regard to revocation evasion (Z= -1.530, p=0.126, α= 0.05). The reason behind this is that the participants were already more concerned about the possibility of revocation evasion compared to the possibility of log evasion even before knowing that the issues do exist. Therefore, although the participants' level of concern has mostly increased towards both issues after watching the video, it was more noticeable for log evasion.

After watching the video demonstration, most of the participants believed both issues to be very serious. However, they considered revocation evasion to be more serious compared to log evasion ($\overline{x} = 3.90$ and $\overline{x} = 3.49$, respectively). Referring to the revocation evasion problem, P13 says:

> **P13:** *"Extremely serious. That can really make or break someone's life extremely, especially with stalkers and domestic violence issues. I'm just trying to think about all the issues that someone has changed their locks*

> *because of some type of danger or harm that they felt that they might have been in to revoke someone's access into their home. So that person can still access their home, when they are not on Wi-Fi. That's scary."*

Furthermore, we asked the participants if they would switch back to traditional locks if they found that their smart locks had either of those problems. For both the revocation evasion and the log evasion issues, most participants (n=19 and n=23 respectively), stated that they would NOT go back to using a traditional lock. Some participants explained how they would buy a different smart lock instead of going back to a traditional lock because they appreciate the features that a smart lock offers. However, most of them stated that now that they know about those issues, they will make sure to test their smart locks and be more careful about which smart lock they buy in the future and who they share access to their locks with.

3.3.3 Reasons for the Lack of Concern

Using Mitigation Strategies. Some participants mentioned that having added layers of security such as using a video doorbell or installing an alarm system on their smart locks was a factor that increased their trust in their smart locks and made them less concerned about possible security and privacy issues related to the smart locks.

Trusting Other Users. Most of the participants who did not seem very concerned about most security issues related to smart locks stated that they only share access to their smart locks with people they absolutely trust and are not expecting any of these individuals to actively invade their privacy or compromise their security.

Trusting the Manufacturer. The manufacturer's security and privacy policies play a crucial role in protecting the integrity and confidentiality of the data that is transferred from the end user to the manufacturer. Similar to previous research [80], some participants stated that they trust the manufacturer to not sell or share their data with other third parties as well as keep their data secure on the cloud against any hacking attempts.

Everything about me is Already Out There! Some participants stated that their lack of concern with some privacy and security issues related to smart locks is due to the fact that their personal information is already on the internet one way or another and has already been sold to advertising agencies by other applications and services that they used in the past. Therefore, they were not greatly concerned about their smart locks sharing personal information with other parties.

My House is not a Target! The participants were mostly aware of the fact that smart locks are susceptible to hacking. However, some of them did not show any concern regarding the possibility of hacking mainly because they were under the impression that hackers would have no interest in compromising their smart locks and gaining access to their homes.

3.3.4 Mitigation Strategies

Even though some participants showed concerns related to the security and privacy of smart locks, they also made it clear how convenient it is to use the smart lock and enjoy the added features compared to its counterpart the traditional lock especially when its counterpart also has its own security and privacy issues. However, the participants reported that they tend to use specific protective measures and mitigation strategies to cope with those concerns and improve the security of their smart locks without losing the convenience factor of using a smart lock (RQ3).

Adding Another Layer of Security. When asked if they use any other devices or gadgets to increase the security and privacy of their smart locks, most participants (n=25) stated that they do. The majority of those (n=24) have a video doorbell installed, which records everything that happens around the area where the smart lock is installed. In addition, it allows users to see who is actually at the door before unlocking it. The second most commonly used device to improve the security of smart locks was a chain guard or a swing guard (n=4), which is a small device that, when engaged, can be installed on the door and door frame to make it harder for an intruder to access the home even if they managed to get the smart lock to unlock. Two participants (n=2) also installed a secondary lock on the door, so that even if the smart lock was unlocked, the intruder would still have trouble getting in. Several participants (n=2) reported that their home had a security system that could alert them in case of a break-in. Those systems usually require the user to input a passcode every time they get through the front/back to stop the alarm from going off.

However, we asked the participants if they would still feel safe with the smart lock if those other security layers were not installed. To our surprise, 21 participants said they would, indicating either that they are confident in the security features of smart locks or that they do not consider their homes a target for intruders.

Configuring the Network. Some participants (n=3) suggested improving the security of the network that the smart lock connects to as a solution to concerns related to hacking and remote manipulation of the lock.

> **P12:** *"My biggest concern was the connectivity to the internet and, obviously, the ability that someone else may have to access the lock remotely, or gain access to the code or anything of that nature. I've kind of mitigated that by using Bluetooth instead of connecting it directly to wireless. And then when it's connected on my phone through Bluetooth, I actually have a separate wireless network that I'm connected to the separate VLAN so that anytime I'm connected to that device, it's not on the center VLAN that I use to surf the web and stuff like that."*

We hypothesized that improving authentication through using Multi-factor Authentication (MFA) would be something that at least some participants might mention as a possible mitigation strategy but when asked unprompted, none of the participants mentioned it. For this reason, we asked the participants if the applications they use to control their smart locks support MFA. About half of the participants (n=14) stated that their application does offer it, while 10 participants stated that they don't have this feature and 3 other participants did not know if they had it or not.

For the 14 participants who had access to MFA, 10 of them had it in the form of a One-Time-Password (OTP) that is sent to their phone or email when they log in from a new device, 5 participants have it in the form of a PIN, fingerprint, or face ID, that is required every time they use the companion application, and 1 participant had it in the form of a confirmation from an already logged in person. However, only one person out of the 14 participants who have the MFA feature stated that they use it frequently (in the form of a PIN, fingerprint, or face ID) while the others either don't use it or are required to use it every time they log in from a new device.

Managing Access Codes Carefully. Some participants (n=3) stated that they choose to manage access codes more carefully and put some regulations in place when it comes to creating and sharing access codes. This includes things like changing the access codes frequently and giving access only to a limited number of people who absolutely need it. Moreover, the companion applications used to control smart locks are usually reliable when it comes to sending out notifications of every interaction with the lock in real time to the homeowner as well as keeping an access log that records every interaction with the lock along with other information such as who interacted with the lock, when, and how. Some participants (n=2) said that this has been very effective for them when it comes to dealing with their security concerns since they can always be notified of who is using the lock so they can confirm whether it was a person they recognize or not and can react to the situation accordingly.

Maintaining the Keypad/touchpad. As mentioned in the previous section, smart locks that are equipped with a touchpad/keypad have their own security issues especially when it comes to the wear and tear of the buttons and the touch screen itself. Participants (n=2) who have this sort of smart locks take some protective measures to deal with those possible security risks such as covering the touchpad/keypad with a plastic wrap so that it does not wear down as quickly as well as wiping off any fingerprints that it might catch after each use.

3.3.5 The Security of Smart Locks Compared to Traditional Locks

When asked whether it made them feel safer having a smart lock installed in their home compared to having a traditional lock, the majority of participants (n=19) said that it did. According to the participants, having features such as the ability to remotely lock the door, get security notifications, restrict others access time, and the ability to use the auto-lock feature made them feel that their home is secure even when they are away from home. However, other participants (n=10) did not necessarily feel more secure with the smart lock, but they appreciate its convenience. Some of them even felt less secure for various reasons such as the possibility of getting hacked, and the fact that others can see them as they type in their access codes and might be able to use that access code in the future.

3.3.6 Security and Privacy Improvements

In this section we report and discuss the participants' insights regarding how the smart lock's design and functionality can be altered in a way that enhances its overall security and privacy (RQ4).

Built-in Camera. Most commercially available smart locks don't have a built-in camera, but some of them can be easily integrated with other commercially available video doorbells. However, some participants (n=6) believe that having the doorbell camera already built-in can save the user money and time spent to integrate the two which sometimes might not even allow the user to use the full capabilities of both devices. Moreover, some participants lack the technological background to connect the two devices together. In fact, some participants (n=8) have both devices but do not have them connected due to different reasons such as not knowing how to connect them or the fact that they are not compatible in the first place. In terms of security, a built-in camera allows the users to see a video of who is interacting with the lock in real time as well as knowing exactly who is at the door before letting them in.

Improve Authentication. Some participants (n=6) believe that the authentication process within smart locks can be improved to increase the overall security of smart locks. According to the participants, they would feel more secure if instead of using an access code or a button on the companion application to authenticate, they would be able to use a more secure method such as face recognition or fingerprint (which is already available on some smart locks but not the most popular ones). However, some of participants also liked the idea of using Multi-factor Authentication (MFA) to improve the authentication process for logging into the companion application which was discussed at some point during the interview. Most of them were not familiar with the concept of MFA before the interview.

More Data Transparency. In line with previous work [94], several participants (n=5) believe that the manufacturer needs to be more transparent when it comes to explaining how the customer data is being used, who it's shared with, and how much of the user's information is shared.

> **P12:** *"I would say that it would be easier to have a little bit of better visibility into how your data is being used. It's not so transparent as to how your data is being used from third parties or from the company itself."*

Improving the Physical Security of the Lock. Two participants stated that the smart lock is not physically secure and could use some improvements in that aspect. This can be accomplished by implementing an intrusion detection system or a tamper detection system with specific sensors that can detect any tampering with the lock, attempts to break it, or hitting it with a strong force.

3.4 Discussion

Smart Lock Adoption. Our study revealed that most participants chose to adopt a smart lock mainly because the features that the smart lock offers make it more convenient compared to a traditional lock. This, however, contradicts with a prior study by Mamonov et al. [57] that aimed to explore the key factors affecting smart lock adoption in which improving the security and safety of the home was the most important factor that influenced the participants intention to adopt a smart lock. This contradiction can be due to the different backgrounds or demographics of the participants in the two studies. Another reason could be the fact the participants in our study have had at least 2 months of experience using the smart lock before the interview, while the participants in the study conducted by Mamonov et al. hadn't adopted the smart lock at that point in time.

Convenience Over Security. Although several participants expressed their concerns about privacy and security issues related to smart locks, most of them believed that the convenience of using the smart lock outweighs its security flaws. After all, its counterpart, the traditional lock, is not necessarily flawless in terms of security since it's susceptible to picking and tampering. However, several participants did not seem to be extremely concerned about the security drawbacks of the smart lock. Some of these participants were not aware of the possible security threats while others trust the mitigation strategies they put in place to increase the privacy and security of the lock and the smart home in general.

Unique Security Concerns and Mitigation Strategies. Our findings revealed security concerns and mitigation strategies unique to smart locks which have not been discussed in prior studies that aimed to investigate the security and privacy concerns and mitigation strategies related to smart home devices in general. For example, some participants in our study expressed concerns regarding shoulder surfing attacks or the fact that attackers might be able to figure out the smart lock's correct access code based on which keys on the keypad are more worn due to being pressed more frequently. These sorts of concerns also introduced mitigation strategies that are more unique to smart locks such as maintaining the keypad/touchpad more regularly and managing access codes more carefully. Furthermore, some participants were also concerned about the possibility of losing their smartphone which would be equivalent to losing their key to the house, while other participants showed concerns regarding the possibility of getting locked out of their homes due to internet connection or battery related issues with the smart lock. While it's possible to mitigate some of the security concerns regarding most smart home devices by installing the device in a different location within the house, or turning the device off for a specific amount of time [97, 80], this is not applicable in the case of smart locks due to obvious reasons. However, our findings show that using an extra layer of security is the main mitigation strategy used by smart lock users to deal with their privacy and security concerns. For most participants, this extra layer of security was a video doorbell due to the fact that video doorbells are usually installed near the smart lock which provides the user with a clear view of what is happening around the lock and who is trying to interact with it.

The Trust Factor. The lack of concern that some participants showed when answering questions related to security and privacy concerns was sometimes due to them having trust either in the other users, the manufacturer, or the security company that installed the smart lock [97, 34]. Having complete trust to the point of neglecting security vulnerabilities could be detrimental to the security of the entire home. For example, one participant mentioned that they do not check access logs because they trust all the other lock users. However, checking the access logs does not necessarily mean a lack of trust, but simply allows the lock owner to verify that only those who should have access to the lock actually do.

Sharing Electronic Keys. The security of the smart lock and therefore that of the entire household, since compromising the smart lock can lead to unauthorized access to the home, is largely dependent on how safely the access codes and electronic keys are being managed. Carefully assigning access codes and electronic keys along with choosing the right access type for each person that uses the lock is extremely critical. For that reason, almost half of the participants chose to only give access to those who live in the house while the other participants, who gave access to non-residents, try to carefully choose the access level based on who needs access to the home, when, and why.

Automation Potential. Smart locks, and smart home devices in general, are equipped with communication protocols specifically designed so that these devices can efficiently communicate with each other to exchange information and provide services. Some smart locks already give their users the option to set up automation scenarios that allow the lock to communicate with other smart home devices and take actions based on data sent to or received from other devices. Those automation scenarios can be used to enhance the usability and the security of the home [72]. However, only 4 participants stated that they have built automation scenes around the smart lock. The participants stated that they did not create automation scenarios mostly due to them not being familiar with the concept of automation. These findings suggest that the process of learning how to create the automation scenes can be a big barrier for those who are not very tech savvy. Improving that process and making it more intuitive will allow more users to use it and familiarize themselves with it.

Data Collection. Although most of the participants were aware that the data the lock collects might be sold or shared with other parties either for advertisement or other purposes, some participants showed a lack of awareness when it comes to understanding what type of personal data the smart lock can store about them and their guests or who their data will be shared with or sold to.

3.4.1 Implications and Recommendations

Access Control Management. Currently, the majority of smart locks implement a Role-based Access Control (RBAC) management system with 4 access levels: owner, resident, recurring guest, and temporary guest [40]. Each of the four access levels has specific access rights associated with it and the only two factors that the homeowner can manipulate when giving access to another user are the date and time (for the recurring guest and temporary guest access levels). However, more than half of the participants (n=16) stated that they share access to their smart locks with other users who don't live inside the house such as a babysitter, a pet walker, or a contractor. To improve the privacy and security of those who live inside the house, it's imperative to enable the homeowner to create more granular access control policies taking into account other environmental and contextual factors. For example, a homeowner might want the contractor to be able to use their access code only if no one is home to ensure the privacy of the home residents. Moreover, even when considering giving access to residents, prior studies, such as the study conducted by He et al. [37], have proved that smart home users prefer to give access based on capability rather than device which also supports the need for more granular access control policies.

Video Doorbell Integration. The fact that over 82% of the participants have a video doorbell installed next to their smart lock gives us an indication of how well these two devices complete each other and using them together can greatly improve the security and privacy of the household. However, many participants stated that although they have both devices, they don't necessarily have them connected either because they are not compatible, or because the user lacks the knowledge of how to connect them to get the most out of the two devices. We recommend, as well as many participants, that smart locks either have cameras already built-in or at least support seamless integration with other video doorbells in the market. The integration process needs to be simple with a clear and concise video tutorial to make it easier for those who are technically challenged to connect the two devices and get the added security and usability features.

Battery. Many participants showed some concern regarding the battery life of the smart lock. Once the battery starts depleting, the lock becomes slower in responsiveness and sometimes does not even lock properly since it lacks the needed torque to properly lock the door. Prior work has indicated that smart locks suffer from sitting idle during extended periods of the day as well as having additional high peak current demands compared to other smart home devices [30]. Therefore, they require better power management in order to improve their battery life. Improving the battery life should be a priority along with increasing the frequency of battery level warnings that show on the user's smartphone before the lock gets to the stage where it struggles to unlock properly and not only when the battery is about to die completely.

Increasing Awareness. Our study shows that there is a general lack of awareness when it comes to security and privacy issues that the smart lock might be susceptible to. The lack of awareness often leads to lack of concern which can stop the smart lock user from implementing the correct protective measures and following the proper security practices to keep the lock secure. Therefore, more work needs to be done to educate the smart lock's user base about the possible security flaws and vulnerabilities. Our results show that the big majority of participants were not aware of state consistency attacks that some smart locks are susceptible to. Making them aware of those issues, however, has proved to increase the level of concern for some participants.

Transparency in Data Collection and Sharing. Our results revealed that the participants' level of concern regarding sharing their personal information with other parties is almost as high as the level of concern regarding hacking (Figure 4b).

Therefore, it's imperative to give the users more control over what data is collected through the smart lock as well as more transparency about who gets access to such data. One way to improve the transparency in data collection and sharing is through adding more privacy controls and improving how privacy policies are displayed to the end user in a way that accommodates for users of different education levels, languages, and ages.

3.5 Limitations

Like many interview-based studies, our convenience sample size was limited and might not wholly reflect the broader population. Our recruitment efforts were predominantly focused on university students and employees, which confined us in terms of geographical diversity and the educational level of our participants. Therefore, nearly all our participants were from the United States with a generally high educational background. We attempted to address this lack of diversity by promoting the study on Reddit forums. However, our attempt was hindered by the fact that most of the responses to the screening survey posted on Reddit came from bot accounts or were instances of a single person submitting multiple surveys. We identified this anomaly thanks to the data analysis and insights provided by the survey platform we utilized, Qualtrics.

3.6 Conclusion

Given the continuous increase in the market size of smart locks year after year all over the world and the role smart locks play in maintaining the security and privacy of the household, more and more research needs to be done in order to improve the design and functionalities of smart locks. There have been numerous research papers published in the past discussing the security and privacy of smart locks from the perspective of the researchers, but little work has been done on the security and privacy of smart locks from the perspective of the end users. In this study, we focus on the end user's perspective of different aspects of the smart lock. We start our interviews by investigating the usage behaviors of smart locks' end users. We learned that big portion of smart lock users tend to share access to the lock with others who don't live in the house which justifies the need for improved access control policies. Our study also revealed that the convenience of smart locks was the number one factor in adopting a smart lock. The study also shows a lack of concern, as well as a lack of awareness, regarding some smart lock security and privacy threats.

CHAPTER 4: A COMPARATIVE STUDY OF USING BLE AND SOFTAP WI-FI PROVISIONING APPROACHES FOR THE SMART LOCK

4.1 Research Purpose

Rapid progress in the development and implementation of Internet of Things (IoT) based applications has led to a new era where they have become an integral part of several social and business sectors such as smart homes, healthcare, and transportation. One of the main reasons these devices have such an impact in each of these sectors is their ability to collect an enormous amount of information and exchange it with the cloud for analysis which can then be used to make critical decisions. However, these smart devices, including smart locks, require internet connection in order to be able to communicate with the cloud and function as intended. The Wi-Fi provisioning of these headless smart devices is not as straightforward as provisioning devices that are equipped with a touchscreen or a keyboard [89]. Alternatively, there are several schemes that are commonly used to provision smart devices such as Software-enabled Access Point (SoftAP), and Bluetooth Low Energy (BLE) [61, 23, 92].

Both of the aforementioned provisioning approaches require human interaction as well as the use of a smartphone that connects to the smart device being provisioned either through Wi-Fi or Bluetooth in order to provide the network information (SSID and password). Figure 8 illustrates the provisioning process for both approaches. While the users of commercially available smart locks have to follow the same provisioning process depicted in figure 8a or figure 8b, depending on the implemented approach, the user interface within the companion application during the process differs from one manufacturer to the other. In this study, we are interested in the Wi-Fi provisioning of smart locks. Unlike the smart devices being configured in a business environment, installing and configuring smart devices in the smart home is usually done by untrained and inexperienced individuals [91]. This might lead to several usability and security issues especially if the average user does not find the provisioning method as simple or intuitive as it needs to be. However, the literature lacks studies that compare and evaluate those provisioning methods from the perspective of the end user in order to understand the strengths and weaknesses of each of them. Moreover, exploring those approaches from a user's perspective provides a basis for improving those methods and re-designing them with the consumer's perceptions and needs in mind and improve smart lock provisioning in smart home settings. Prior research has primarily focused on pinpointing issues within Wi-Fi provisioning schemes, such as security vulnerabilities [31, 49, 86]. In contrast, our work focuses exclusively on user experience. We aim to investigate how users interact with the companion application used during the provisioning of the smart lock via SoftAP and BLE provisioning methods. The objective is to empirically compare these two approaches and identify their strengths and weaknesses exclusively from the end user's perspective.

In this study, we invited 60 participants to provision a smart lock using two different provisioning schemes (SoftAP and BLE). Each of the participants was asked to provision the smart lock twice using a different provisioning method each time and then fill out 2 online surveys to describe their experience with each method. Our work aims to answer the following research questions (RQs):

- RQ1: How do the provisioning approaches, BLE and SoftAP, empirically compare in terms of their usability, learning curve, security, efficiency, reliability, and their impact on other phone functions based on the end user's experience?

- RQ2: What are the shortcomings and challenges present in the provisioning procedures of both approaches that have an adverse impact on the end user's experience when configuring smart locks?

4.2 Study Design and Procedure

We designed our study as a "within-subjects" experiment where the independent variable was the provisioning approach: BLE or SoftAP. We had a total of 60 participants. Each participant used both provisioning approaches to provision the smart lock and then answer an online survey immediately after completing the provisioning process using each of the two methods in order to evaluate their experience with using that approach. In order to ensure that the carryover effect usually associated with within-subjects studies does not affect the results of the study, the order of using the two provisioning approaches was counterbalanced. Therefore, 50% (n=30) of the participants used SoftAP first and the rest of the participants (n=30) used BLE first.

To conduct this study, we utilized the university's usability lab, where eligible participants were invited for in-person sessions with the researcher. These sessions lasted approximately 20 minutes, and each participant received a $5 Amazon gift card as a token of appreciation for their participation in the study. The study received approval from the university's Institutional Review Board (Protocol #22-1074). The research process began with a brief presentation by the researcher, introducing participants to the concept of IoT provisioning. Essential information required to complete the provisioning process, such as network credentials and the Proof of Possession (PoP) for the smart lock, was provided to the participants. They were then tasked with the following steps:

1. Provision the smart lock using one of the two provisioning approaches (the researcher let them know which approach they can use first) through the smart lock's companion application installed on the researcher's smartphone.

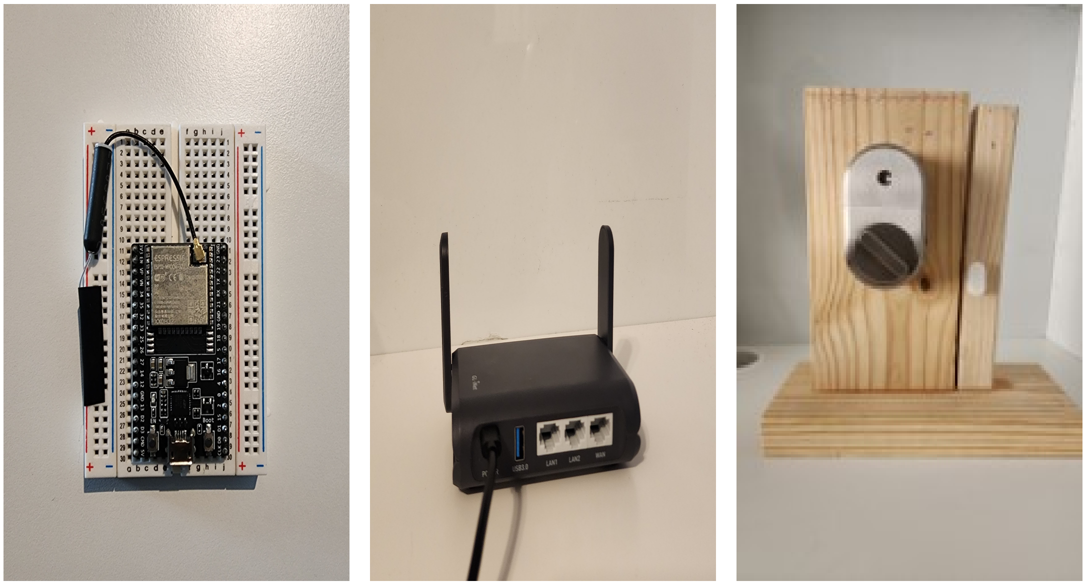
2. Lock or unlock the smart lock through the companion application to ensure that the lock was correctly provisioned.

3. Complete an online survey to evaluate their experience with the provisioning approach they used.

4. Repeat tasks 1,2, and 3 using the other provisioning approach.

4.2.1 Study Setup

The aim of our study was to explore user perceptions concerning the provisioning of the smart lock using BLE and SoftAP methods. However, as far as we know, there are no smart locks on the market that give users the option of using either of the two approaches to provision the lock. Therefore, to facilitate the implementation of both BLE and SoftAP provisioning approaches, we used the ESP32 micro-controller which supports both Wi-Fi and BLE functionalities. The ESP32 device was programmed using the Espressif IoT Development Framework (ESP-IDF) which supports uni-

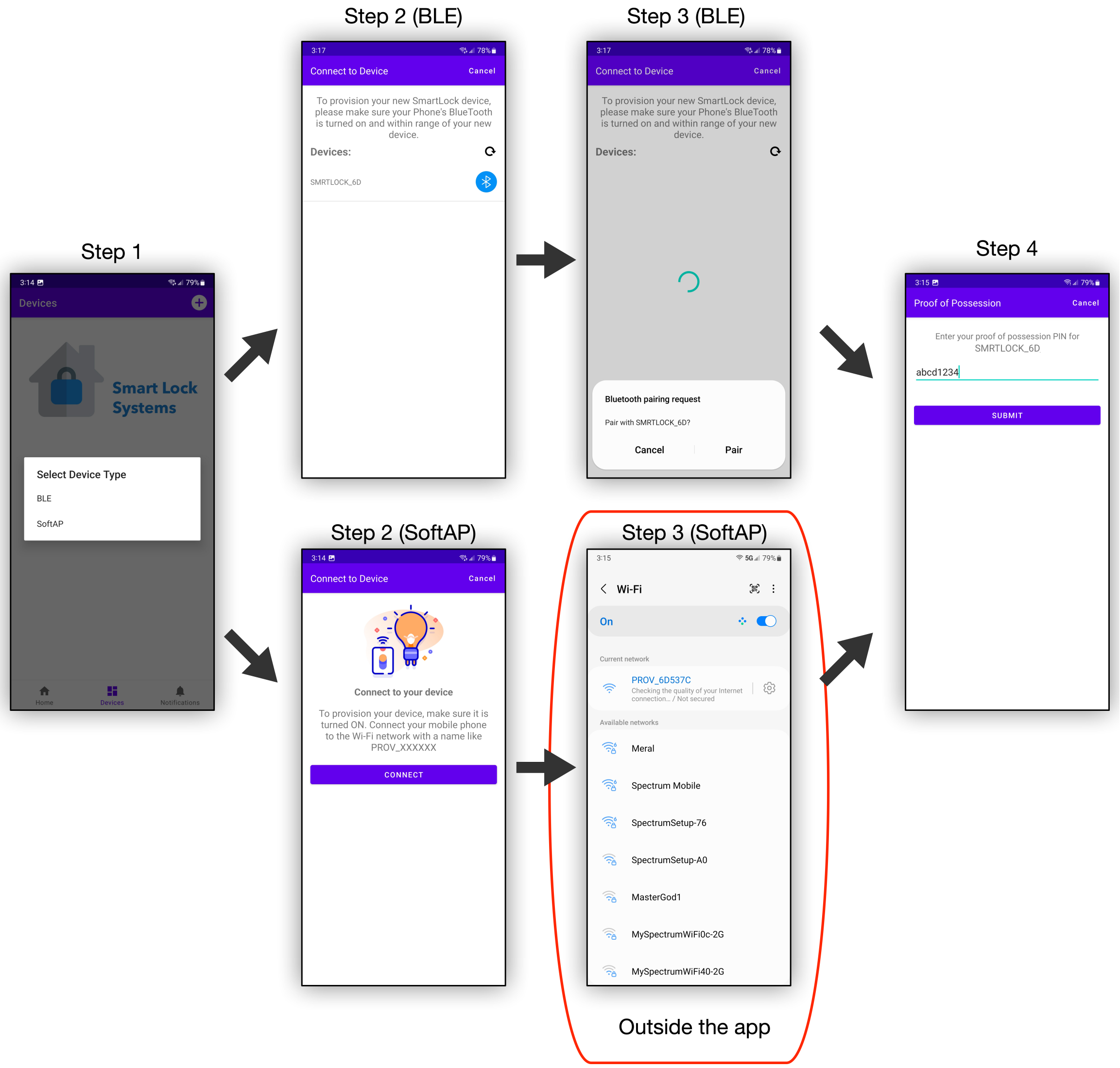


(a) ESP32 (b) Router (c) Smart lock

Figure 5: Study setup

fied provisioning to enable developers to configure these devices with Wi-Fi either through BLE or SoftAP [6], we programmed two ESP32 devices, one to provide BLE provisioning and the other providing SoftAP. Participants were uninformed about the ESP32 devices being part of the study setup; they were led to believe that their task was to provision the visible smart lock device, as depicted in Figure 5c, during the study. To maintain control over the Wi-Fi settings, we utilized our own router and pre-configured Wi-Fi pin code. We used the August 3rd generation smart lock, which provides integration compatibility with the If This Then That (IFTTT) platform [5, 2]. By leveraging IFTTT, we configured triggers enabling users to connect to the August smart lock and send lock or unlock commands through our mobile app, but only after they had successfully completed the provisioning process. From the participants' perspective, the end goal of this provisioning exercise was to acquire the capability to control the smart lock and issue lock and unlock commands. Once the participants had successfully locked and unlocked the smart lock, we informed them that we would be resetting the smart lock device. We then asked them to undertake the provisioning process once again, this time using the alternative provisioning approach following the same steps.

The Companion Application. We developed an Android companion application that enabled the participants to provision the ESP32 devices using either BLE or SoftAP provisioning approaches through the same application, and then to control



To provision your new SmartLock device, please make sure your Phone's BlueTooth is turned on and within range of your new device.

Pair with SMRTLOCK_6D?

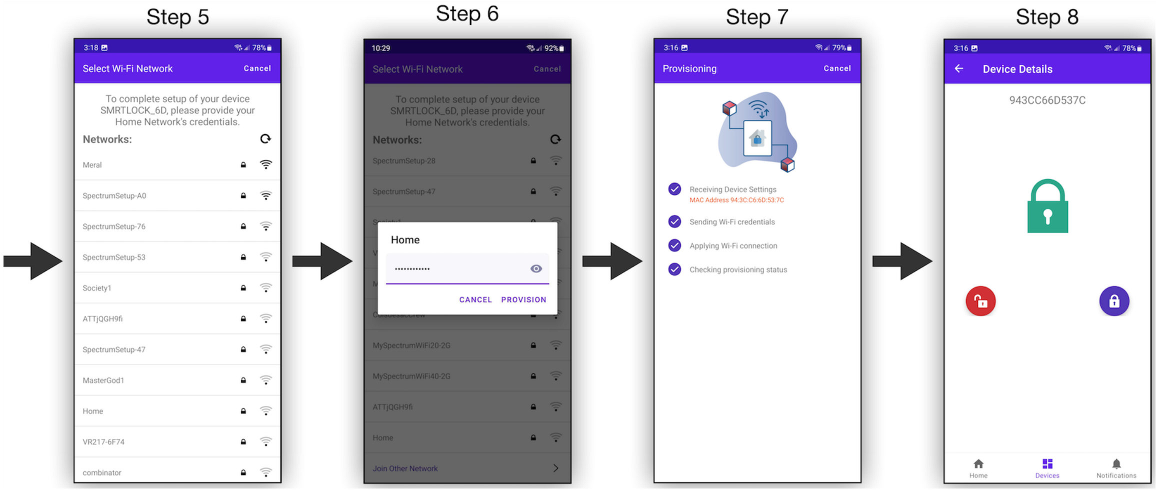
To provision your device, make sure it is turned ON. Connect your mobile phone to the Wi-Fi network with a name like PROV_XXXXXX

Checking the quality of your Internet connection... / Not secured

Enter your proof of possession PIN for SMRTLOCK_6D

abcd1234

Figure 6: The provisioning flow on the companion application



To complete setup of your device SMRTLOCK_6D, please provide your Home Network's credentials.

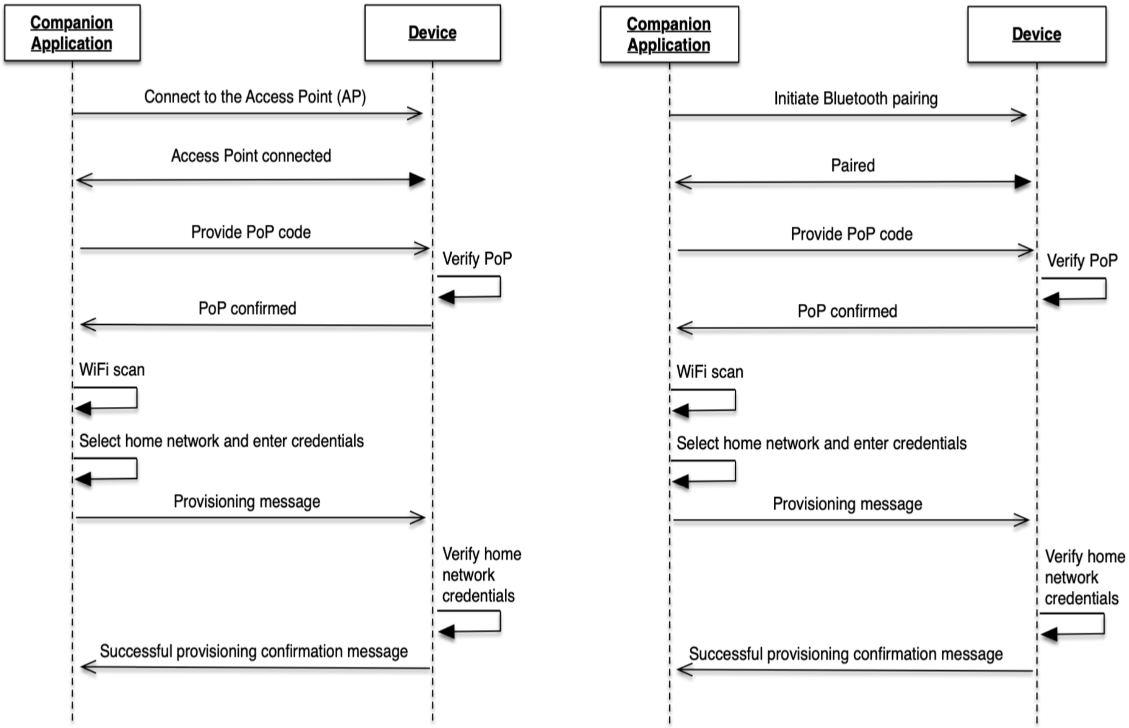
Home: ············

✓ Receiving Device Settings
MAC Address 94:3C:C6:6D:53:7C
✓ Sending Wi-Fi credentials
✓ Applying Wi-Fi connection
✓ Checking provisioning status

943CC66D537C

Figure 7: The provisioning flow on the companion application (continued)

the smart lock device once the provisioning steps are completed. The provisioning implementation was based on the Espressif IoT Development Framework provisioning Android SDK, and was updated to include the required instructions to guide the user through the provisioning process. Figures 6 and 7 show screenshots of the different app screens for both the BLE and SoftAP approaches. Upon launching the application, participants were prompted to select their preferred provisioning approach, as illustrated in Step 1 in Figure 6. Half of the participants were instructed to begin with BLE and then proceed with SoftAP, while the other 50% followed the reverse order, starting with SoftAP and subsequently using BLE. For BLE provisioning, Steps 2 and 3 entailed BLE scanning and connecting to the chosen BLE device. Conversely, in the case of SoftAP, Step 2 and 3 required participants to temporarily exit the companion application and access the device's settings app to connect their smartphone to the temporary access point generated by the device, as displayed in Figure 6. It's important to note that provisioning Steps 4 to 7 remained consistent for both provisioning methods. However, the SoftAP provisioning approach necessitated users to momentarily leave the companion application and return to the settings app to connect their smartphone to their Wi-Fi network. Upon successful completion of provisioning, participants gained the ability to lock and unlock the smart lock, as depicted in Step 8 in Figure 6.


Companion Application
Device
Connect to the Access Point (AP)
Access Point connected
Provide PoP code
Verify PoP
PoP confirmed
WiFi scan
Select home network and enter credentials
Provisioning message
Verify home network credentials
Successful provisioning confirmation message
Companion Application
Device
Initiate Bluetooth pairing
Paired
Provide PoP code
Verify PoP
PoP confirmed
WiFi scan
Select home network and enter credentials
Provisioning message
Verify home network credentials
Successful provisioning confirmation message

(a) SoftAP

(b) BLE

Figure 8: Sequence diagrams for the flow of the SoftAP and BLE provisioning processes

4.2.2 Participants

We recruited participants through a user study announcement email which is sent to the university's students, faculty members, and staff. Our sole eligibility criterion was that participants had to be at least 18 years old. In total, we recruited 60 participants, comprising 33 females, 25 males, and 2 individuals who opted not to disclose their gender. The largest group of participants (n=44) fell within the 18-24 age group, while 9 participants were aged 25-34, 4 participants fell into the 35-44 age bracket, 2 participants belonged to the 45-54 age group, and one participant was in the 55-64 age range. Regarding their experience with setting up smart home devices, approximately a third of the participants (n=21) self-reported having an average level of experience, while 18 participants considered themselves somewhat above average. Additionally, 9 participants claimed to have a significantly above-average level of experience. Conversely, 4 participants indicated a somewhat below-average level of experience, and 8 participants reported having a significantly below-average level of experience.

4.2.3 Data Analysis

We utilized an inductive approach to code the qualitative. Two researchers coded the open-ended questions independently then discussed and finalized the coded data to resolve any disagreements. Any discrepancies between the coders were discussed until consensus was reached. Therefore, we did not administer Cohen's Kappa. As for the quantitative data, we used non-parametric tests, Wilcoxon Signed Ranks Test and Spearman correlation, to test for statistical significance since the data was not normally distributed.

4.3 Results

In this section, we present the results of our quantitative and qualitative analysis of participants' perceptions and insights regarding the two provisioning approaches.

Table 5: Wilcoxon Signed Ranks Test

	SoftAP ($\bar{x}$, s)	**BLE ($\bar{x}$, s)**	**Z-value**	**P-value**
Security	(4.06, 0.86)	(4.07, 0.86)	-0.027	0.979
Effect on other phone functions	(2.30, 1.14)	(2.03, 1.07)	-1.534	0.125
Reliability	(4.22, 0.74)	(4.47, 0.58)	-2.885	**0.004***
Usability				
System Usability Scale (SUS)	(70.62, 21.99)	(85.54, 12.08)	-4.325	**0.001***
Single Ease Question (SEQ)	(5.55, 1.24)	(6.42, 0.74)	-4.838	**0.001***
Learning curve				
Number of tries	(1.88, 0.86)	(1.08, 0.28)	-4.993	**0.001***
Number of times the participant asked for help	(0.92, 0.79)	(0.07, 0.25)	-5.433	**0.001***
Efficiency				
Provisioning time in seconds (measured by the researcher)	(127.63, 34.78)	(90.17, 32.70)	-5.205	**0.001***
The time required to complete the process was acceptable (scale of 1-5)	(4.20, 1.10)	(4.65, 0.88)	-2.493	**0.013***
There were too many steps required to use this provisioning approach (scale of 1-5)	(2.57, 1.40)	(1.70, 0.96)	-4.337	**0.001***

* statistically significant

4.3.1 Quantitative Results

Our quantitative evaluation encompasses six categories: usability, learning curve, security, efficiency, reliability, and the effect on other phone functions (RQ1). Previous research papers, such as [64, 66, 36, 58, 38, 9], mentioned the first five categories as important elements in gauging end-user satisfaction with smart home devices or related services. While using SoftAP, the participants need to connect to disconnect from the internet during parts of the process. Therefore, we also included the last category, assessing their effect on other phone functions, to get a better understanding of how it effects users.

Security. Generally, there was no statistically significant difference in the participants' perceptions regarding the overall security of the two provisioning approaches or the privacy of the information being transmitted between the smartphone and smart lock during the provisioning process (Z= -0.027, p=0.979, α= 0.05). In fact, the majority of participants regarded both BLE and SoftAP as highly secure methods for provisioning Wi-Fi on smart locks ($\bar{x} = 4.07$ and $\bar{x} = 4.06$, respectively). However, correlation analysis indicated that participants with greater experience in setting up smart home devices tended to assign lower security scores to BLE, although this correlation did not reach statistical significance (r= -0.149, p=0.255, α= 0.05). While previous research [31, 86, 29, 54, 75] has identified some security and privacy vulnerabilities in both provisioning methods, it appears that end users generally express satisfaction with the provided security levels.

Effect on Other Phone Functions. The smart locks provisioning process entails establishing a connection between the user's smartphone and the device, either through Bluetooth or Wi-Fi. This connection allows the phone and device to communicate and exchange the necessary information to complete the task. This interaction can potentially impact other phone functions and applications, such as a temporary loss of internet connectivity when the phone is linked to the temporary access point while using the SoftAP method [4, 74]. However, as this impact is limited to the provisioning process's duration, it largely went unnoticed by the majority of participants. Therefore, the difference in the participants' answers to the survey question "I feel this provisioning approach would affect how other apps on my phone function" was not statistically significant (Z= -1.534, p=0.125, α= 0.05).

Reliability. In our survey, we included two 5-point Likert scale questions to gauge the reliability of BLE and SoftAP when it comes to provisioning smart locks. The first question, ”I found this provisioning approach to be effective,” aimed to evaluate the reliability of the provisioning approach itself. Meanwhile the second question,” the system had all the capabilities and functions I needed to provision the lock,” aimed to assess the reliability of the provisioning process through the companion application. A statistically significant portion of the participants found the BLE approach to be more reliable for provisioning the smart lock (Z= -2.602, p=0.009, α= 0.05). Generally, more participants failed to provision the device on their first attempt using SoftAP compared to BLE, which may explain why they found SoftAP less reliable.

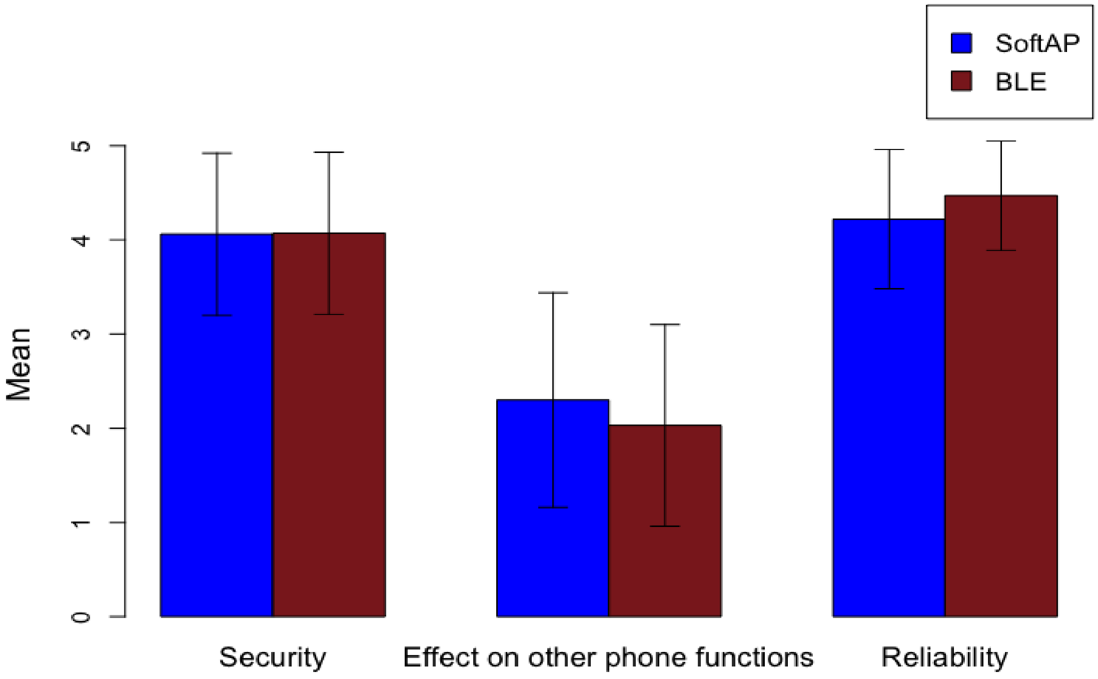
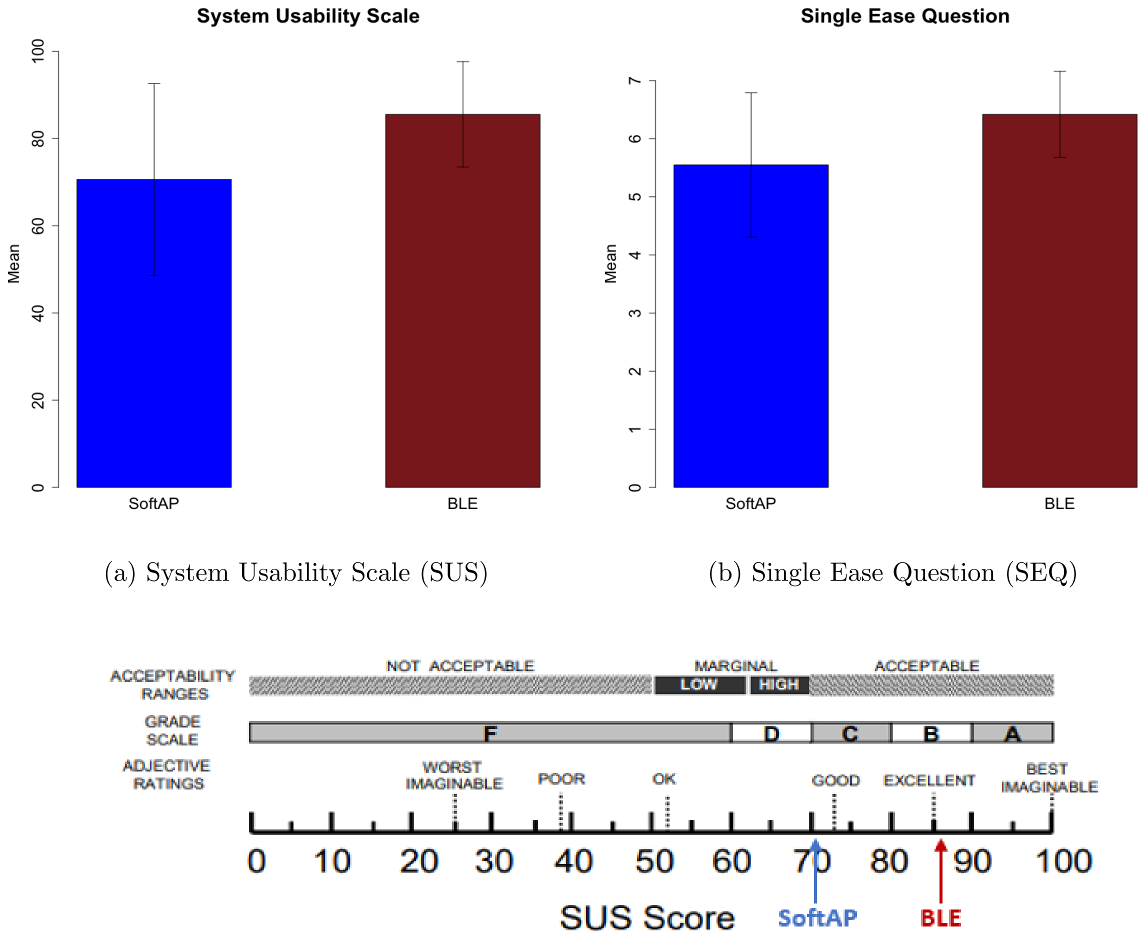


Figure 9: A comparison of the SoftAP and BLE scores for security, effect on other phone functions, and reliability

Usability. We assessed the usability of each of the two approaches using the

System Usability Scale (SUS) score and the Single Ease Question (SEQ) measurement.

The SUS is a widely recognized and robust standardized questionnaire used to gauge and quantify the overall usability of a system. It provides a score ranging from 0 to 100 [17]. Typically, highly effective products tend to yield SUS scores exceeding 90 [12]. To calculate the SUS score for each provisioning method, we relied on participants' responses to the ten 5-point Likert scale SUS-related questions (Appendix B). A majority of participants (N=40) found the BLE approach to be more usable, while only 15 participants favored SoftAP for its usability. However, it's noteworthy that the average SUS score for the SoftAP approach ($\bar{x} = 70.63$) still falls within the borderline acceptable range [11]. In contrast, the BLE approach obtained a mean SUS score of 85.54, indicating its superior usability over SoftAP but also suggesting room for improvement [12]. Spearman-correlation analysis revealed that participants with more experience in installing and configuring smart home devices tended to give higher SoftAP SUS scores (r= 0.293, p=0.023, α= 0.05). Another factor affecting the SoftAP SUS score was the number of attempts made. Participants who successfully provisioned the smart lock using SoftAP in fewer attempts reported higher SoftAP SUS scores (r= -0.268, p=0.039, α= 0.05). We attribute this difference to the skill and experience required for users to connect their smartphones to a temporary access point in the SoftAP provisioning process, in contrast to the more seamless BLE connection procedure, which does not necessitate such changes in settings.



(a) System Usability Scale (SUS)

(b) Single Ease Question (SEQ)

(c) SUS Benchmark [11]

Figure 10: Usability scores for SoftAP and BLE

The ease of use constitutes a crucial aspect of the overall usability of any provisioning method given the fact that easier provisioning can lead to fewer errors and less need for external help while provisioning. To assess this, we had participants answer a Single Ease Question (SEQ) at the end of each survey. The SEQ employs a widely recognized 7-point scale, where participants choose 1 if they found the provisioning approach extremely difficult and opt for 7 if they found it exceedingly easy [77]. The Wilcoxon Signed Ranks Test unveiled a statistically significant difference in the SEQ scores between the two provisioning methods (Z= -4.84, p < 0.001, α=

0.05). Only 3 participants found provisioning the smart lock using SoftAP easier than using BLE, while 21 participants found BLE to be the more straightforward option. Nonetheless, it's important to note that participants generally did not perceive provisioning the device using SoftAP as extremely challenging ($\bar{x} = 5.5$). Notably, Spearman-correlation analysis uncovered a significant connection between the SEQ score and the perceived provisioning time. Participants who deemed the time spent provisioning the device using a specific approach acceptable tended to assign higher SEQ scores to that approach (SoftAP: $r= 0.535$, p=0.001, $\alpha= 0.05$, BLE: $r= 0.298$, p=0.021, $\alpha= 0.05$).

Learning Curve. To assess the learning curve associated with each of the two provisioning methods, we monitored the number of attempts required by each participant to successfully provision the smart lock using each approach, as well as how often participants sought assistance while using each provisioning method. A provisioning approach is deemed to have a steeper learning curve if users find it necessary to seek help to complete the process or if they need multiple attempts to successfully provision the smart lock. Before starting the provisioning process with either approach, participants were instructed to request assistance or retry (i.e., cancel the provisioning process and start over) only if they felt completely stuck and unable to proceed with the given provisioning method. Among the 60 participants, 55 managed to successfully provision the device on their first attempt using BLE, while the remaining 5 participants required two tries to do so. Conversely, when employing the SoftAP approach, only 23 participants successfully provisioned the device on their initial attempt. For some participants (n=3), it took up to 4 attempts to complete the provisioning process using SoftAP, while others succeeded on their second or third attempt (n=24 and n=10, respectively).

A similar pattern emerged in terms of the frequency with which participants sought assistance while provisioning the device using the two methods. The majority of participants (n=56) did not request any help when provisioning the device using BLE, with only the remaining 4 participants seeking assistance once. However, with SoftAP, only 21 participants (35%) completed the provisioning process independently, while 23 participants requested assistance once, and 16 participants asked for help on two occasions in order to finalize the provisioning process.

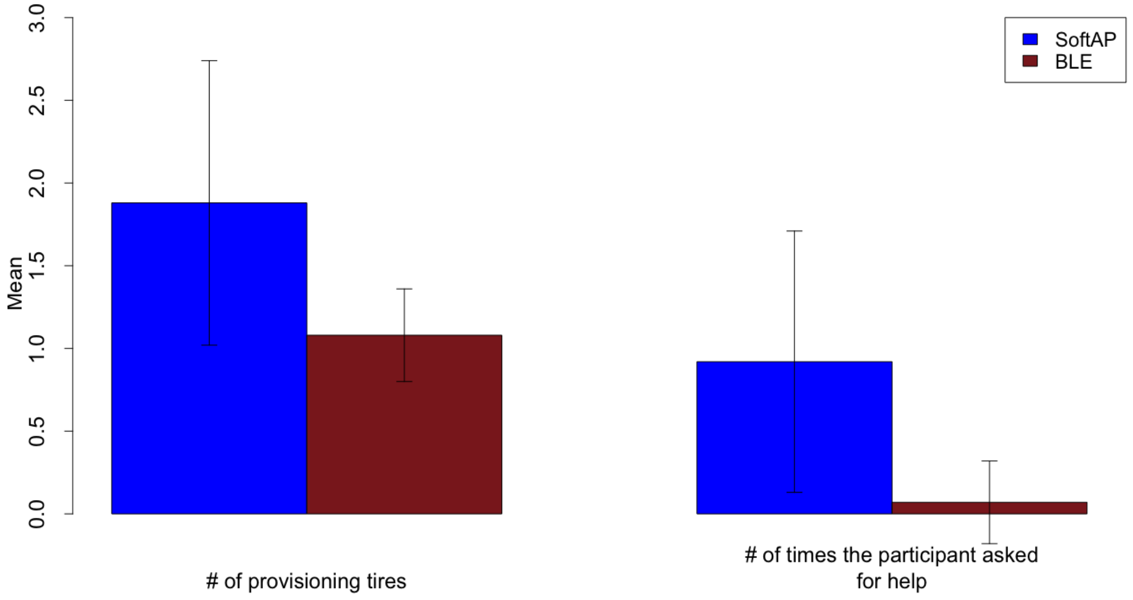
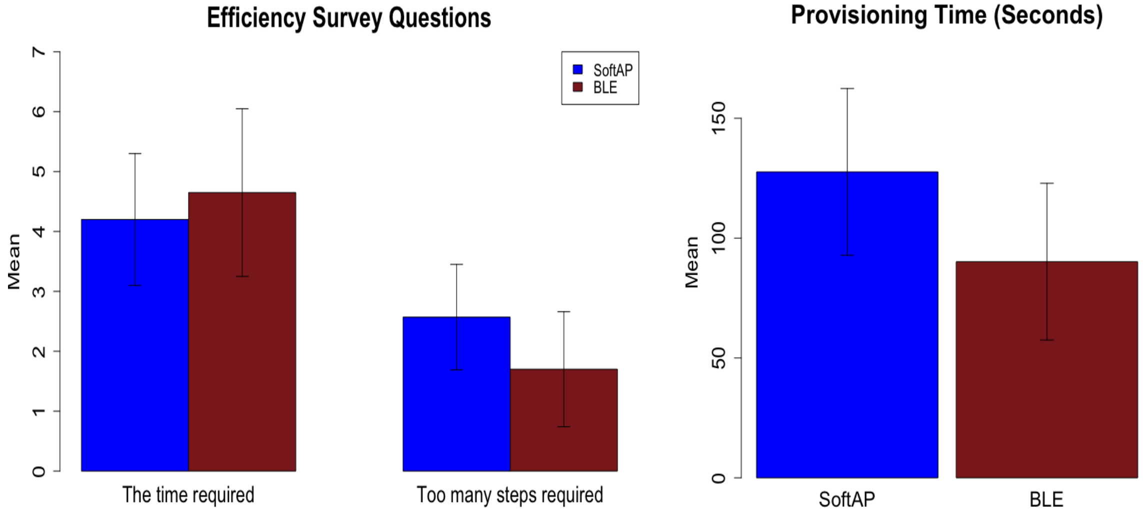


Figure 11: Learning curve

Efficiency. We evaluated the efficiency of employing each of the two methods for provisioning the smart lock by considering three factors: 1) the time taken by participants to complete the provisioning process using each approach during the study, which was measured by the researcher with a stopwatch, 2) participants' perceptions of whether the time required to complete the provisioning process was acceptable, as measured by a 5-point Likert scale survey question, and 3) participants' opinions on whether there were too many steps involved in the provisioning process, also assessed using a 5-point Likert scale survey question.

We kept track of the amount of time (in seconds) each participant needed to provision the device using both methods. On average, participants took approximately 90.17 seconds to complete the provisioning using BLE, whereas it took 127.63 seconds when using SoftAP. Among the 60 participants, only 9 were able to provision the device faster using SoftAP, while the remaining participants (n=51) found BLE to be the faster option. Furthermore, a Wilcoxon Signed Ranks Test revealed statistical significance in favor of BLE regarding participants' satisfaction with the time required to complete the provisioning process (Z= -2.493, p=0.013, α= 0.05). Similarly, a statistically significant portion of the participants believed that provisioning the device using SoftAP involved too many steps compared to BLE (Z= -4.337, p=0.001, α= 0.05).



(a) Efficiency - survey questions

(b) Efficiency - provisioning time

Figure 12: Efficiency scores for SoftAP and BLE

4.3.2 Qualitative Results

In this section, we present our examination of the responses provided by participants to the open-ended questions in the survey. These questions were designed to gain a more comprehensive insight into the difficulties that participants encountered during the provisioning process of both approaches (RQ2).

The User Interface. When asked about what could be done to improve the provisioning process, participants commonly provided feedback related to the companion application. For instance, a portion of participants (10 for SoftAP, 3 for BLE) suggested that the app should provide more comprehensive instructions to assist them throughout the process and prevent errors. Another group of participants (3 for SoftAP, 1 for BLE) recommended using simpler language that would be more accessible to users with less technical knowledge. Meanwhile, 13 participants encountered issues specifically related to Bluetooth discovery and connection speed when using the BLE approach.

> **P4:** *"I think that touching up on the vocabulary used by the UI could be improved. For the average user, they might not know what a PoP is or an SSID is. I think using terms that are more general to the public could be of use and improve speed of completion."*

> **P28:** *"Maybe if more detailed instructions were given about the processes happening on the phone while it is processing to explain to those (like me) who do not understand technology as well what is happening."*

The Provisioning Process. Additionally, we requested participants to share their general impressions of the device provisioning experience using each of the two methods. Most participants expressed overall satisfaction (37 for SoftAP, 55 for BLE). However, 12 participants used terms like "challenging," "unclear," or "not user-friendly" to characterize the SoftAP process. Nine participants found BLE to be more straightforward than SoftAP, while only one participant held the opposite view. Seven other participants noted that BLE was quicker than SoftAP. For instance, participant P19 mentioned regarding the SoftAP provisioning process:

> *"It didn't seem very intuitive and left me feeling unintelligent."*

Nonetheless, participants' least favored aspect of the SoftAP provisioning procedure was the requirement to connect to two separate Wi-Fi networks (reported by 14 participants), followed by the necessity to exit the application to connect to the access point (cited by 9 participants), and 3 participants expressed frustration with manually returning to the companion application after connecting to the access point.

> **P42:** *"Switching between the app itself and the network settings and being told to connect to a certain network versus having that happen automatically I don't think was the best approach, as it took a little while for the device to connect to the network, and I wasn't getting feedback whether it was successfully doing so or not."*

Regarding BLE, 2 participants expressed dissatisfaction with the manual entry of home network credentials for the connection, and another 2 participants indicated reservations about relying solely on PoP as the security measure for BLE provisioning. Overall, most of the grievances about BLE were not centered on the provisioning procedure itself but rather on the perceived intricacies of Bluetooth discovery and connection via the companion application.

Information Exchange. Less than a third of the participants (16 for SoftAP and 18 for BLE) were conscious that the provisioning process entailed transmitting their home network credentials to the smart lock. The majority of participants (32 for both SoftAP and BLE) believed that the data exchange between the lock and the smartphone pertained only to lock or phone-related information (such as IP addresses, MAC addresses, IMEI, and GPS data) and locking/unlocking commands originating from the smartphone. However, when questioned about the purpose of entering the Proof of Possession (PoP) in the companion application, most participants (51 for SoftAP and 49 for BLE) were aware that it served as an additional security measure to verify the legitimate owner during the provisioning process.

4.4 Discussion

SoftAP VS BLE. In summary, the quantitative outcomes of our investigation indicate that BLE surpassed SoftAP in terms of usability, the learning curve, efficiency, and reliability. Analyzing the number of provisioning attempts needed by participants for each approach, we also deduce that SoftAP may result in a higher likelihood of user frustration, particularly among less tech-savvy users. Through our observations and participant feedback, we identified two primary issues with the SoftAP provisioning process that tilted the balance in favor of BLE. The first concern is the requirement for users to connect to two distinct Wi-Fi networks (the home network and the AP), which can be confusing to some users especially since most users did not understand the purpose of connecting to the AP in the first place. The second issue involves exiting the provisioning application (the companion app) to connect to the AP, and then having to manually navigate back to the companion app to complete the provisioning process. This is the case for all commercially available smart locks that use SoftAP since this approach requires connecting to two different Wi-Fi networks and this cannot be done within the companion application. In contrast, the BLE process occurs entirely within the companion app. However, with BLE, pairing with the smart lock via Bluetooth has proven to be inconsistent. Occasionally, the smart lock appears in the list of Bluetooth devices available for connection, but upon selecting the device's name, it suddenly disappears without establishing a connection. Nonetheless, the app features a refresh button that users can click to update the list of devices, and typically, on the second attempt, the phone successfully pairs with the device via Bluetooth.

Security. Our results indicated that there wasn't a significant disparity in how participants perceived the security of the two provisioning methods. In general, participants regarded both approaches as reasonably secure. However, our findings also revealed that when provisioning the smart lock, individuals were more likely to seek assistance from others when using SoftAP compared to BLE. This can potentially pose privacy and security concerns, particularly considering that the provisioning process entails the disclosure of home network credentials. Conversely, some participants, particularly those who were more tech-savvy, raised concerns about the security vulnerabilities and limitations associated with sharing home network credentials via Bluetooth in the BLE provisioning process. As a result, they preferred using SoftAP for this reason. It's important to note that prior research has also highlighted that BLE is susceptible to eavesdropping attacks and has weaker encryption [75, 29, 54].

The Companion Application. Provisioning is a relatively infrequent task for smart homeowners, typically only necessary when acquiring a new smart lock or resetting an existing one. Consequently, it's reasonable to assume that end users are often unfamiliar with this process. Our research indicates that most participants lacked awareness regarding the purpose of provisioning and the type of data exchanged between their smartphones and the smart lock. Thus, much of the responsibility falls on the device's companion application to educate users about the provisioning process, regardless of the chosen approach. The aim is to minimize the likelihood of users seeking assistance or becoming frustrated during provisioning due to their limited knowledge. Achieving this goal could involve incorporating comprehensive instructions on each screen of the companion application, particularly for SoftAP, which exhibited higher rates of retries and requests for help. However, our findings reveal that text-based instructions were ineffective in the case of SoftAP, as 37 participants failed to connect to the access point (AP) despite specific on-screen guidance instructing them to connect to a network with a name beginning with "PROV" indicating the AP (Step 2 for SoftAP in figure 6). Utilizing alternative methods for presenting instructions, such as video, audio, or interactive images, might yield more favorable outcomes.

4.5 Limitations

Our study has two primary limitations. Firstly, participants were instructed to configure the smart lock using the companion application installed on the researcher's Android device. This might have been a challenge for some participants accustomed to using iPhones. However, for those who indicated unfamiliarity with Android devices, we adjusted the navigation settings from "navigation bar buttons" to "swipe gestures" to replicate the navigation style of an iPhone. We intentionally avoided requesting participants to install the application on their personal devices to mitigate potential security or privacy concerns related to installing an unfamiliar app on their smartphones. Another limitation is the exclusion of several other provisioning schemes available for smart locks from our comparative analysis. We made this choice to prevent the carryover effect in a within-subjects study, where participants' interactions with the app might have been influenced by multiple provisioning methods, particularly as they progressed through the third or fourth approach. Therefore, we limited our comparison to just two widely recognized and commonly used provisioning methods in the smart home context, SoftAP and BLE.

4.6 Conclusion

With the growing popularity of smart locks, many of which are set up by non-tech-savvy buyers themselves, it becomes imperative to investigate how end users perceive the process of setting up these devices. While there are various methods for configuring IoT devices, SoftAP and BLE stand out as two of the most widely utilized approaches in commercially available smart locks. This chapter presents the results of a study aimed at examining and assessing the disparities in the setup process when employing BLE and SoftAP, as perceived by end users. To achieve this, we conducted interviews with 60 participants, tasking them with configuring both BLE and SoftAP setups. We structured our study to ensure that participants used a single application for both methods, thereby eliminating potential external factors that could influence their evaluation of the two approaches. Our findings indicate that a majority of participants encountered more difficulties when setting up devices through SoftAP, often requiring assistance from someone more familiar with the process. Participants also exhibited a significantly higher rate of re-tries, i.e., restarting the process, when configuring via SoftAP compared to BLE. Furthermore, the participants consistently favored BLE over SoftAP in terms of usability, learning curve, efficiency, and reliability, with statistically significant differences.

CHAPTER 5: EXPLORING END USERS' PERCEPTIONS OF SMART LOCK AUTOMATION WITHIN THE SMART HOME ENVIRONMENT

5.1 Research Purpose

Smart locks have many capabilities that set them apart from their traditional counterparts. One of these capabilities is the ability to communicate with other smart home devices and external services. Thus, several possibilities arise, such as the ability to create and execute automation scenarios based on the exchange of information between the lock and other smart home devices. Automation scenarios are rules that the end user creates so that a smart home device can automatically take action based on information it receives from other home devices [43]. For example, a homeowner can set their smart lock to automatically unlock if the person ringing the video doorbell is identified through face recognition as a resident, without the need to give them the lock's access code or manually unlocking the door for them. In this case, face recognition is done through the video doorbell, while the unlocking of the door is done through the smart lock. Creating such scenarios extends the functionality of smart locks as well as enhances different aspects of the smart home experience. However, creating automation scenarios has several challenges such as device compatibility, process complexity, and security concerns related to the data exchange between the devices [10, 7, 71]. In fact, only 4 out of the 29 participants in our first study stated that they have created automation scenarios that included the smart lock. Therefore, we conducted this study to further explore smart locks users' perceptions and needs when it comes to creating smart home automation scenarios that include the smart lock. Prior research has studied the effectiveness of creating smart home automation scenarios in improving the smart home experience [16, 18, 93, 21]. However, our work aims to categorize the automation scenarios that include the smart lock based on the users' motivation to create them and the purpose they serve. Additionally, we quantitatively compare those automation scenarios within each category to gain a better understanding of their effect on the other aspects of the smart home environment. As part of this study, we investigated the following research questions:

- RQ1: What are the primary motivations for users to integrate smart locks into their home automation scenarios?
- RQ2: How do smart home automation scenarios that include the smart lock impact certain aspects of the smart home such as security, awareness, and convenience?
- RQ3: What are the main concerns of users when setting up smart home automation scenarios that include the smart lock in their homes?
- RQ4: What factors affect the end user's decision to set up automation scenarios that include the smart lock?

5.2 Methodology

To investigate the motivations driving end users to create smart home automation scenarios that include the smart lock as well as the effect of creating such automation scenarios on different aspects of the smart home environment, this study adopts a mixed-methods approach. We utilized the department's usability lab to organize face-to-face sessions with each participant individually. During these sessions, the participants were required to fill out two online surveys using the lab's computers. Additionally, participants were tasked with creating at least four automation scenarios involving a smart lock, set in a theoretical smart home equipped with 11 smart devices and sensors. The participants were given the option to use cue cards to help them create the automation scenarios. Similar to Corno et al.[24], we asked the participants to use a pen and paper to write their automation scenarios down.

5.2.1 Participants

We sought participants who already have smart locks installed in their house and have admin access rights to their smart lock and other smart home devices inside the house. The reason behind such inclusion criteria is that we are interested in participants who have the option of creating automation scenarios in their house which is only possible for those with admin access rights. However, we don't require the participants to have had created automation scenarios in the past. Additionally, all participants must be over 18 years of age. The participants were recruited through a mass email sent to all students and employees at the university. Potential participants were asked to fill out a screening survey to confirm that they meet our eligibility

Table 6: Participants' demographic information - third study

Participant	Gender	Age group	Occupation
P1	Male	18-24	Residential Advisor
P2	Female	18-24	Student
P3	Female	25-34	Librarian
P4	Male	45-54	Lecturer
P5	Male	45-54	Computer systems administrator
P6	Female	18-24	Waitress
P7	Female	25-34	Student
P8	Male	18-24	Graduate student
P9	Female	18-24	Student
P10	Female	25-34	Graduate Student
P11	Male	18-24	Financial Analyst Intern
P12	Male	18-24	Student
P13	Female	25-34	Student
P12	Male	18-24	Student
P13	Female	25-34	Student
P14	Male	45-54	IT
P15	Female	45-54	Student
P16	Female	25-34	Lecturer
P17	Female	18-24	Associate Director of Outreach
P18	Female	25-34	Postdoc
P19	Female	65-74	Director of University Accreditation
P20	Female	45-54	Admin
P21	Male	18-24	Student

criteria. We recruited a total of 21 participants (13 females and 8 were males). The age distribution included 9 participants aged 18-24, 6 aged 25-34, 5 aged 45-54, and 1 participant aged 65-74.

5.2.2 Procedure

Eligible participants, identified through their responses to the screening survey, were contacted to schedule a session for the study. The study was approved by the university's Institutional Review Board (Protocol #23-0704). Each participant was met individually in our department's usability lab. The session began with an

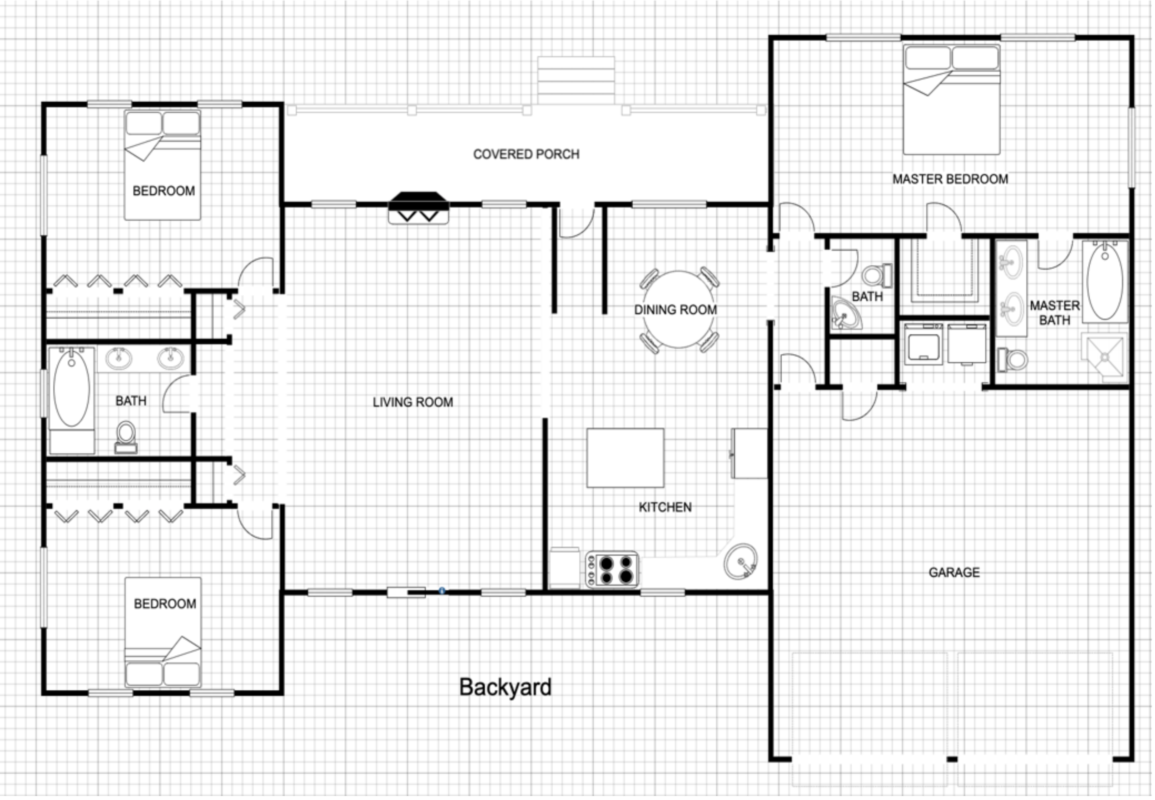


Figure 13: The house layout used in the study

introduction to the concept of smart home automation scenarios, including examples to clarify the concept before asking them to complete the first online survey. This initial (pre-study) survey, completed on the lab's computer, gathered demographic information and inquired about their experience with creating automation scenarios and any security or privacy concerns related to smart home automation.

Following the survey, participants were tasked with creating at least four smart home automation scenarios that include the smart lock within a hypothetical smart home. Similar to Soares et al.[78], we provided the participants with a hypothetical house layout (figure 13) and details about 11 installed smart devices and sensors (table 7). To assist them, we provided a PowerPoint presentation detailing the features of each device and sensor, along with the syntax required for creating scenarios (IF

Table 7: Smart home devices and sensors installed inside the house used for the study

Smart home device or sensor	**Location**
Smart Lock	main entrance
Smart TV	Living room
Home security system	Hallway
Smart video doorbell	Main entrance
Smart lights	Front porch, backyard, and every room inside the house
Home security camera	Front porch and backyard
Smart smoke detector	Every room inside the house
Smart speaker with voice assistant	Living room
Motion sensors	Anywhere inside the house
Contact sensor	Backyard sliding door
Smart garage door opener	Garage

condition THEN *action*). We facilitated the task by offering color-coded cue cards representing each device's features, aiding in the scenario creation process (figure 14). The participants were then required to use a pen and a paper to write down the automation scenarios they created as well as any comments that they might have regarding each of the scenarios.

After creating the automation scenarios, participants filled out another online survey to share insights on the scenarios they created. Upon completing this second survey, each participant was rewarded with a $10 Amazon gift card as a token of our appreciation for their time and contribution.

5.2.3 Data Analysis

We analyzed the qualitative data from the scenario creation phase using inductive thematic analysis to identify common themes and categorize the types of smart home automation scenarios created by participants. The data was coded by one researcher to create the initial codebook. Two researchers then conducted several meetings to

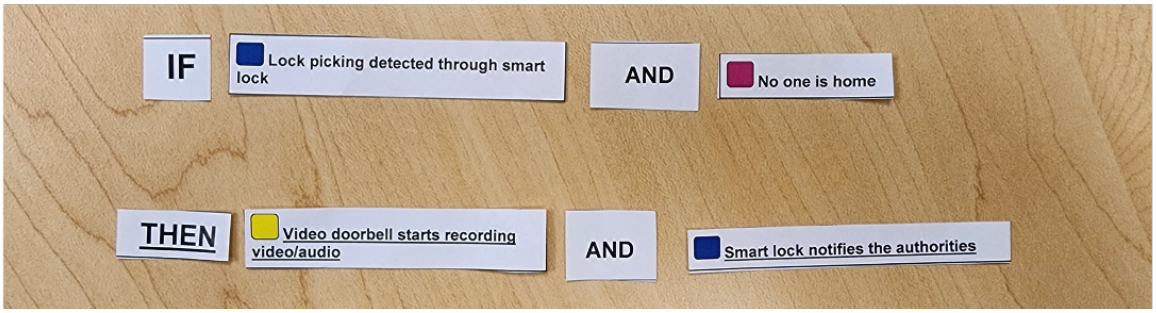

IF
Lock picking detected through smart lock
AND
No one is home
THEN
Video doorbell starts recording video/audio
AND
Smart lock notifies the authorities

Figure 14: An automation scenario created during the study using the cue cards

discuss and finalize the codebook. The quantitative data from the online surveys were analyzed using descriptive statistics to gauge the overall evaluation of the automation scenarios across different dimensions.

5.3 Results

Table 8: Smart home devices the study participants have installed in their home

Smart home device	**Number of participants who have it installed**
Smart Lock	21 participants
Smart TV	17 participants
Smart Thermostat	16 participants
Home security system	14 participants
Smart video doorbell	14 participants
Smart lights	11 participants
Home security camera	9 participants
Smart speaker	9 participants
Smart smoke detector	8 participants
Smart hub	6 participants
Motion sensor	5 participants
Contact sensor	3 participant
Smart dishwasher	1 participant
Smart garage door opener	1 participant

5.3.1 Pre-study Survey

We asked the participants to fill out a pre-study survey in order to explore their use of automation in their homes. Slightly less than half the participants (n=9) stated that they hadn't set up automation scenarios in their homes. The barriers to adoption varied, with four individuals citing a lack of knowledge, two encountering difficulties due to the complexity of the setup process, and others pointing to issues like device incompatibility (n=1), concerns over information privacy (n=2), time constraints (n=2), and a shortage of smart home devices (n=1) as reasons for not setting up any smart home automation scenarios. However, 12 participants reported having successfully set up smart home automation scenarios in their residences, with 10 specifically incorporating smart locks into their automation scenarios.

These participants used various platforms to set up their automation scenarios, including Alexa (n=4), ADT home security (n=2), Google Home (n=1), and One Home (n=1). Out of the 21 participants, 13 expressed no security or privacy concerns related to creating automation scenarios. However, some participants stated some concerns regarding the possibility of unauthorized access (n=2), unexpected results (n=2), and data privacy issues (n=4). When asked about security or privacy concerns specifically related to automation scenarios that include the smart lock, 14 participants reported no concerns. However, others were concerned about unauthorized access (n=4), false positives (n=2), and data privacy leaks (n=1).

Table 9: The mean participants' evaluation of how automation scenarios within each category (first column) would affect different aspects (top row) of their smart home experience on a scale of 1 to 5

Category	Overall security	Security while away from home	Overall convenience	Awareness of home surroundings	Awareness of home inhabitants	Feedback on home monitoring
Threat detection and management	**4.42**	4.39	3.84	4.13	3.68	4.16
Proactive security	**4.42**	4.32	4.32	3.95	3.89	3.79
Convenience	3.08	2.60	**4.80**	3.16	3.56	3.24
Awareness	**4.53**	4.42	4.19	4.25	3.83	4.36
Access management	3.80	3.53	**4.53**	3.93	4.07	3.93
Safety	**4.36**	4.27	4.09	3.36	3.09	4.0

5.3.2 Automation Scenarios

Our user study resulted in 91 automation scenarios created by the participants that all included the smart lock. However, four scenarios were discarded due to issues in their logic. We ended up with 87 automation scenarios on which we based our analysis and findings. The participants were instructed to use the if-then syntax for creating the automation scenarios, which is more preferable to end users, as shown by previous research [27, 78]. In 71 out of the 87 automation scenarios, the smart lock automatically takes action (e.g., lock the door) based on information it receives from other smart home devices. However, in 50 scenarios, other smart home devices automatically take action based on information received from the smart lock (e.g., the door was unlocked using an access code). 24 scenarios contained location constraints (e.g., someone is home) and 21 scenarios contained temporal constraints (e.g., 7 PM).

Through inductive thematic analysis, we divided the 87 automation scenarios into 6 categories reflecting their intended purposes and the benefits they offer to homeowners and residents. Those categories are threat detection and management, proactive security, convenience, awareness, access management, and safety. Some scenarios serve more than one purpose and therefore were put in multiple categories. For example, the automation scenario S9-1 was put in the "threat detection and management" category because the threat (the lock is unlocked and someone is approaching the door) was detected and then managed by locking the door. It was also put in the "awareness" category since it also notifies the homeowner of the issue and increases his/her awareness of the situation.

> **S9-1 - Automation Scenario:** *IF the smart lock status is unlocked for over 10 minutes and the security camera detects human motion* THEN *the smart lock locks the door and notifies the homeowner.*

Threat detection and management. The 31 automation scenarios that belonged to this category were mostly motivated by the need to identify a possible threat to the security or privacy of the household and take action towards managing it either by notifying the household members, sounding an alarm to scare away intruders, or even contacting the authorities. The majority of participants stated that creating such automation scenarios would increase the overall security of their homes, their sense of security when they are away from home, and their feedback on home monitoring ($\bar{x} = 4.42$, $\bar{x} = 4.39$, and $\bar{x} = 4.16$, respectively).

> **S8-3 - Automation Scenario:** *IF the smart lock has detected a lock picking attempt* THEN *the security camera starts recording and the smart*

lock notifies the homeowner.

S8-3 - Motivation: *"I wanted to know if someone is trying to break-in by breaking the lock so that I can inform the authorities and be prepared for what is coming."*

S11-5 - Automation Scenario: *If home security system goes off and no one is home and motion sensor detects motion in any bedroom (master or others)* THEN *smart lock notifies authorities and smart speaker sounds alarm and security camera sends footage with captured video/audio.*

S11-5 - Motivation: *"Security reasons, when families go away on vacation they do not want to worry about the safety of their home."*

Proactive Security. Unlike the automation scenarios in the "threat detection and management" category, the 19 automation scenarios in this category aim to ensure the security of the house even when no threat or danger was detected. The motivation behind creating such scenarios is mostly to ensure the security of the house (e.g., the front door must be locked after a certain hour) through automation without having to rely on the user's memory or judgment. Therefore, some of the scenarios in this category also exist in the convenience category. In fact, in addition to increasing the overall security of the house ($\bar{x} = 4.42$) and the residents' sense of security while away from home ($\bar{x} = 4.32$), the majority of participants also stated that these scenarios increased their convenience level within the home ($\bar{x} = 4.32$).

S13-3 - Automation Scenario: IF *it's 10 PM* THEN *lock front door and set alarm to arm stay.*

S13-3 - Motivation: *"Making sure front door is locked and alarm is armed at the end of every night. My parent always does this but sometimes forgets and we have to check (since I don't usually do it but sometimes do), or he takes the dog out after we set the alarm so we have to re-set it."*

S2-1 - Automation Scenario: IF *motion sensor(s) (hallway/kitchen/living room) do not sense anything for 15 minutes AND no one is home* THEN *Smart lock locks the door AND all smart lights off AND turn TV off.*

S2-1 - Motivation: *"I can be a little forgetful sometimes and might forget to lock the door or turn some lights out, so this automation is more of a failsafe in case someone forgets to do something after they leave."*

Convenience. 25 automation scenarios were put in this category. The automation scenarios in this category were mostly created to increase the convenience of the household members by automating the routine and everyday tasks. Examples include scenarios where the door unlocks automatically as the user approaches and the front porch lights turn on to illuminate the pathway into the house. These scenarios were highly valued for their convenience, receiving the highest average score ($\bar{x} = 4.80$) from participants when asked about their potential to improve the smart home's convenience level. However, concerns about the security implications of such scenarios led to a comparatively lower score regarding their ability to enhance security when residents are away from home ($\bar{x} = 2.60$)

S13-1 - Automation Scenario: IF *the smart lock is unlocked using access code* THEN *automatically silence the home security system alarm.*

S13-1 - Motivation: *”Convenience. I don’t want to silence the home security system alarm manually every time I enter the house.”*

S1-3 - Automation Scenario: IF *it is a week day after 7:00 am* THEN *the smart lock unlocks.*

S1-3 - Motivation: *”This one was made strictly for convenience.”*

Awareness. The 36 automation scenarios within this category share a unified goal of enhancing the homeowner’s awareness of events that could impact the smart home or the smart lock itself. Therefore, almost all of the automation scenarios in this category result in sending some sort of notification to the end user either sent through the smart lock or one of the other smart home devices included in the scenario. Notably, a significant portion of automation scenarios in this category (n=14) included smart home devices positioned close to the smart lock, such as the video doorbell and the front porch security camera. Participants reported that implementing these scenarios would enhance their feedback on home monitoring ($\bar{x} = 4.36$), increase the overall security of their smart homes ($\bar{x} = 4.53$), increase their sense of security when away from home ($\bar{x} = 4.42$), and increase their awareness of home surroundings ($\bar{x} = 4.25$).

S10-6 - Automation Scenario: IF *temporary smart lock passcode is used* THEN *send video clip from security cameras to authorized users.*

S10-6 - Motivation: *”If a temporary passcode is given to a cleaner or friend, I would want to know when it’s being used and more importantly who is using it.”*

S21-4 - Automation Scenario: IF *the smoke detector detects fast or slow fire and the smart lock is locked* THEN *notify the owner, emergency contacts, and the authorities.*

S21-4 - Motivation: *"I think that if a fire happens while I am not home, I would appreciate the peace of mind in knowing that the proper people could be alerted."*

Access management. The 15 automation scenarios in this category were mostly created either to automate the access control policies of the smart lock (with the help of other devices such as the video doorbell) or to increase the end user's knowledge of who is trying to access the home through the smart lock. Therefore, the participants stated that these scenarios would massively increase the convenience level within their homes due to automating access control policies ($\bar{x} = 4.36$). Furthermore, according to the participants, these scenarios would also enhance their feedback on home monitoring ($\bar{x} = 4.27$) and increase their awareness of home surroundings ($\bar{x} = 4.53$). Aside from the smart lock, the smart home device that was included the most in these scenarios was the video doorbell (n=11) mainly due to the fact that the video doorbell can play a big role in identifying the person at the door in order to grant them access to the house automatically through the smart lock.

S3-1 - Automation Scenario: IF *a trusted person is identified through video doorbell and it is before 8pm* THEN *the smart lock unlocks the door.*

S3-1 - Motivation: *"Sometimes we get frequent visitors who stop by but* *don't always want to get up and get the door. They normally don't visit after 8pm."*

S8-2 - Automation Scenario: IF *smart lock has multiple failed unlocking attempts* THEN *notify the homeowner through smart lock.*

S8-2 - Motivation: *"When someone sees over lock and tries to recreate that he might fail at just one to two digit so I would want to know if some is trying and failed to unlock."*

Safety. This category comprises 11 automation scenarios, driven by the objective to safeguard the physical well-being of residents by enabling the lock to automatically take action that would lead to preventing the home inhabitants from danger originating from both inside and outside the home. In general, participants believed that such scenarios would increase the overall security of their homes and improve their sense of security while away from home ($\bar{x} = 4.36$, and $\bar{x} = 4.27$, respectively).

S2-2 - Automation Scenario: IF *smart smoke detector detects smoke (in any room really but I said living room for specificity)* THEN *smart speaker notifies household members AND smart lock unlocks the door AND smart lock notifies all authorized users.*

S2-2 - Motivation: *"In case of a fire or smoke themed emergency, I wanted the front door to be easy to exit/enter while also creating alerting the people in the home through the smart speaker."*

S10-8 - Automation Scenario: IF *a panic code is entered into the smart lock* THEN *unlock the front door, begin recording with security cameras AND sound silent alarm.*

S10-8 - Motivation: *"I always think of worst case scenarios like someone following me home or forcing me into my home. Having a panic key would be a good silent alarm trigger. Could also have a key for a loud alarm to scare intruder away."*

5.3.3 Automation Concerns

Privacy and Security. We asked the participants to disclose any security of privacy concerns they have in relation to each automation scenario they created. The feedback revealed that for 78 of the 87 scenarios created, there were no security or privacy issues raised. Nonetheless, a concern among some participants was that scenarios designed solely for convenience could inadvertently compromise household security and privacy. Additionally, some participants were concerned that in automation scenarios created to increase the homeowner's awareness or access management capabilities, the information exchanged between devices might be intercepted by malicious actors. This could potentially grant them access to sensitive information meant only for authorized eyes, such as video footage of house guests recorded by video doorbells or security cameras.

S8-4 - Automation Scenario: IF *video doorbell detects someone known and no one is home* THEN *unlock the door and notify the homeowner of their arrival through smart lock.*

> **S8-4 - Concern:** *"I might feel the security camera recording everyone coming and even me coming as a privacy concern."*

Reliability. Reliability emerged as a significant concern among participants when discussing potential issues related to the setup and execution of automation scenarios. The participants shared their concern regarding reliability for 32 scenarios. Issues with motion sensors were highlighted by some participants, who feared that motion sensors might not effectively differentiate between human and non-human movements, potentially triggering automation scenarios by accident. There were also worries about the accuracy of facial recognition technology in video doorbells and security cameras, which could result in false alarms or hinder the proper execution of some automation scenarios. Furthermore, concerns were voiced about the possibility of devices failing to communicate necessary information to each other, disrupting the intended operation of certain scenarios. Additionally, participants noted that reliability problems with the devices involved in an automation scenario could lead to security risks, especially in scenarios involving smart locks, where such issues could inadvertently facilitate physical access for unauthorized individuals.

> **S2-3 - Automation Scenario:** IF *trusted person identified in video doorbell and lock status is locked and no one is home* THEN *unlock the door AND turn off home security system AND turn on smart lights (hallway, kitchen, dining room).*

> **S2-3 - Concern:** *"It (the video doorbell) could detect someone incorrectly and let them into the home with no security system alarm which could be*

dangerous."

False Alarms. Some participants were concerned about false alarms especially in automation scenarios that involve contacting the authorities or sounding an alarm late at night. False alarms are usually caused by false positives or triggering an automation scenario unintentionally. Participants stated that such instances would startle the residents or cause some inconvenience.

> **S3-4 - Automation Scenario:** IF *a fast burning fire is detected through the smart smoke detector* THEN *the smart lock will unlock and notify the authorities.*
>
> **S3-4 - Concern:** *"authorities being called for a false positive."*

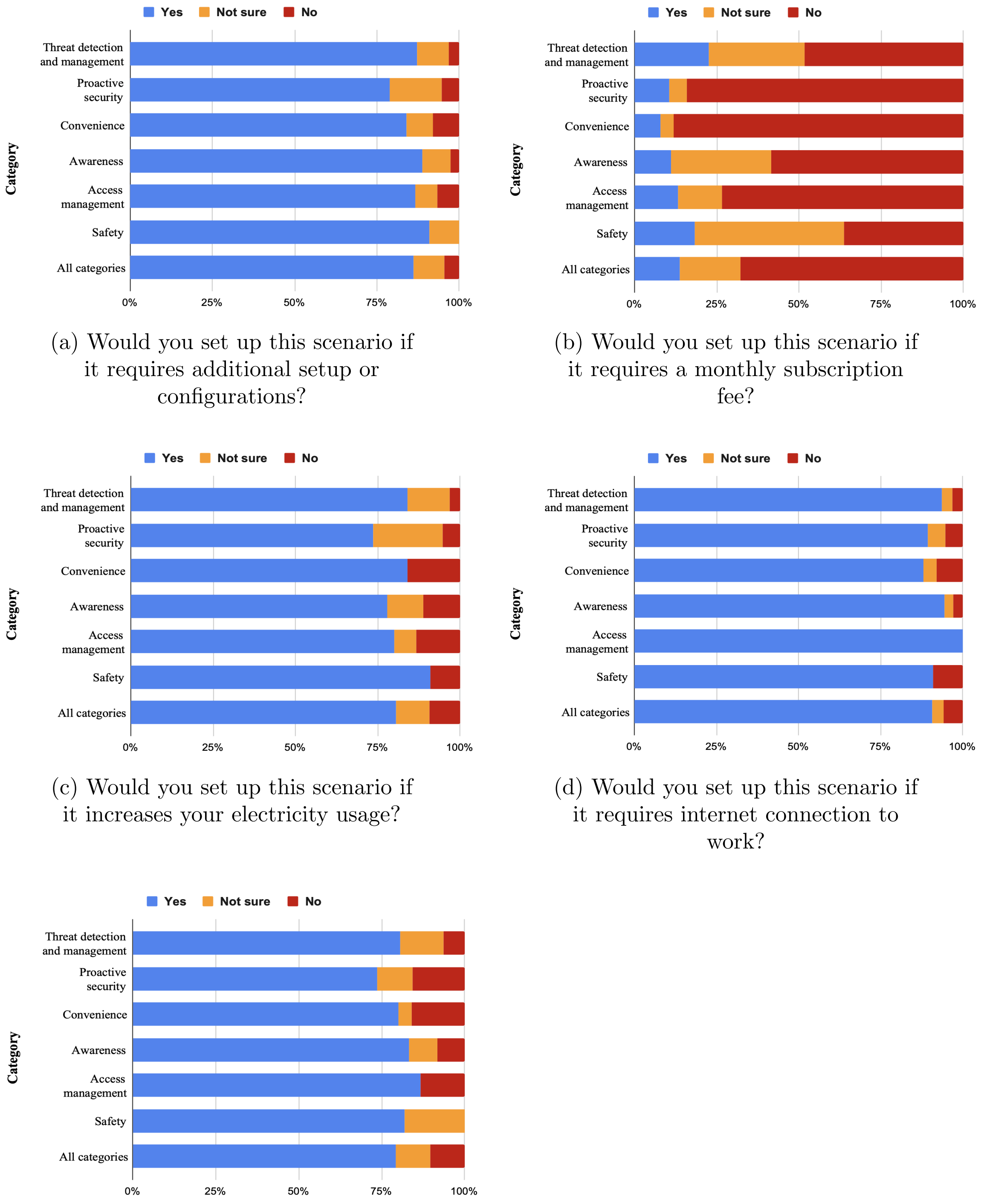
Human Errors. Participants highlighted concerns about the accidental triggering of automation scenarios due to human errors in 12 of the 87 automation scenarios. These errors ranged from other residents simply being unaware of the existence of an automation setup, to instances where a resident might mistakenly input an incorrect access code into the smart lock, potentially activating a security-related automation scenario. Additionally, the presence of children in the home was a significant cause for concern as some participants expressed reluctance to set up certain automation scenarios. This hesitation stems from the concern that children might unintentionally set off these scenarios, leading some participants to consider avoiding the setup of automation scenarios altogether when children are present in the household.

The Occasional Inconvenience. Although many participants felt that incorporating smart locks into automation scenarios could significantly enhance household convenience, there were concerns that certain scenarios (n=11) might result in inconvenience instead. For instance, participants who set up scenarios to automatically unlock the door at a specific time or in response to certain events expressed worries about the potential for accidentally being locked out. Similarly, those who created scenarios to receive alerts when someone attempts to unlock the door at night were concerned about the annoyance it could cause, especially when hosting numerous guests who leave late in the evening.

> **S10-2 - Automation Scenario:** IF *it's 10 PM* THEN *lock front door and set alarm to arm stay*
>
> **S10-2 - Concern:** *"You could go outside, like to walk the dog, and accidentally get locked out and have to disarm the alarm. You'd be able to get back in with the door code, but if for some reason the door code didn't work you likely wouldn't have a hard copy of the key on you."*
>
> **S10-4 - Automation Scenario:** IF *3 failed attempts are entered into the smart lock* THEN *set the home security alarm to arm.*
>
> **S10-4 - Concern:** *"If you had little kids who were just learning how to use the smart lock, they could mess up more often and would be freaked out by the alarm going off."*

5.3.4 Factors Affecting Setting up an Automation Scenario

For each of the scenarios created by the participants, we asked about how different factors might influence their willingness to set up that particular scenario. The factors



(a) Would you set up this scenario if it requires additional setup or configurations?

(b) Would you set up this scenario if it requires a monthly subscription fee?

(c) Would you set up this scenario if it increases your electricity usage?

(d) Would you set up this scenario if it requires internet connection to work?

(e) Would you set up this scenario if it stores data on the cloud and not locally?

Figure 15: Factors affecting setting up an automation scenario

considered included the need for extra setup or configuration, a monthly subscription fee, increased electricity consumption, reliance on an internet connection, and data storage on the cloud versus locally.

The findings, detailed in Figure 15, reveal that the participants were willing to set up most automation scenarios (86.2%) even if they necessitated additional setup steps, such as registering for facial recognition. Similarly, participants also did not mind a possible increase in their electricity bill caused by setting up automation scenarios (80.5%), or the fact that those scenarios will only work when there is internet connection (90.8%), or having their personal data needed to execute those automation scenarios stored and exchanged through the cloud (79.3%).

However, the imposition of a monthly subscription fee was a deterrent for approximately 67.8% of the scenarios, with participants unanimously rejecting to pay a monthly subscription fee for all 22 scenarios designed primarily for convenience. The stance shifted somewhat for scenarios within the "threat detection and management" category, where participants were open to paying a monthly fee for around 22.6% of the scenarios, undecided for another 29%, and opposed to monthly subscription fees for the remaining 48.4%.

5.3.5 False Positive VS False Negative

Several factors can lead to automation scenarios triggering incorrectly (false positives) or failing to trigger when needed (false negatives), with some of these issues highlighted in the "automation concerns" section, including accidental activation by children or reliability problems. We gathered participants' concerns regarding false

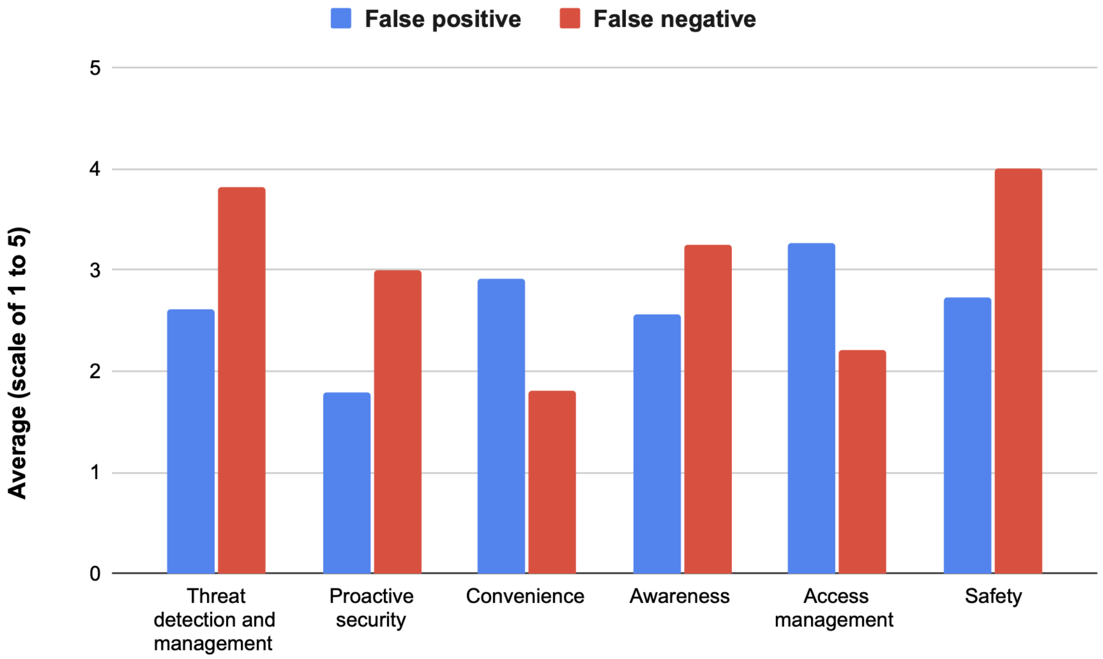


Figure 16: A comparison of the participants' level of concern regarding the possibility of false positives and false negatives associated with each category

positives and negatives across all 87 automation scenarios (figure 16). The findings predominantly indicate heightened concern regarding false negatives within scenarios critical to the home's security and the safety of its inhabitants. Concerns were particularly acute for scenarios within the "threat detection and management" ($\bar{x} = 3.95$) and "safety" ($\bar{x} = 3.8$) categories, designed to address immediate dangers like fires or burglaries. The potential for not detecting or managing a security or safety concern due to untriggered automation scenarios explains the increased concern regarding false negatives within these categories.

Participants were also more concerned about false negatives than false positives in categories aimed at improving home security or enhancing the security awareness of residents, such as "proactive security" and "awareness." The worry here stems from the risk to home security if these critical scenarios fail to activate.

On the other hand, concerns about false positives were more pronounced in scenarios intended to augment household convenience, particularly within the "convenience" and "access management" categories. Participants were wary of scenarios activating unexpectedly, potentially compromising security. For instance, a scenario programmed to unlock the door every weekday at 7AM for convenience might pose a security risk if it mistakenly unlocks at 7PM instead, illustrating the specific concerns associated with false positives in these contexts.

5.4 Discussion

Through a detailed analysis of 87 automation scenarios created by participants, we have gained insights into the primary motivations for integrating smart locks into home automation, the impact of these integrations on aspects such as security, awareness, and convenience, the main concerns users have when setting up such scenarios, and the factors affecting their decisions to implement these automation setups. These scenarios, primarily aimed at improving house security and inhabitant safety, leveraging threat detection, proactive security measures, and heightened awareness, highlight the pivotal role of smart locks in the modern smart home ecosystem.

Motivations for Smart Lock Integration. Our findings demonstrate that the power of integration and automation not only extends the functionalities of smart locks but also amplifies the capabilities of surrounding smart home devices. This synergy between smart locks and other devices facilitates a smarter, more connected, and automated home environment. Furthermore, it addresses specific aspects of the smart home experience from security to convenience. The primary motivations for users to integrate smart locks into their home automation scenarios, as identified through our study, revolve around enhancing safety and security, increasing convenience, and improving awareness of home surroundings. The categorization of automation scenarios into six distinct purposes which are: threat detection and management, proactive security, convenience, awareness, access management, and safety, highlights the multifaceted appeal of smart lock integrations.

Impact on Smart Home Aspects. The automation scenarios created by participants demonstrate a clear intention to leverage smart locks not only as a means of securing the home but also as a tool to enhance the convenience of daily routines and increase the awareness of events within and around the home. The high ratings given to scenarios within the ”threat detection and management”, ”proactive security”, and “safety” categories for their impact on security and users’ physical safety highlight the effectiveness of these integrations in enhancing users’ sense of security. However, the scenarios categorized under ”convenience” received mixed feedback, indicating that while convenience is highly valued, it cannot come at the expense of security. This delicate balance between convenience and security is a critical consideration for the design and implementation of smart lock automation scenarios. Similarly, automation scenarios falling into the “access management” category demonstrated their potential to enhance user convenience and awareness regarding the home inhabitants. However, they also raised security and privacy concerns, primarily due to the concerns regarding false positives, which might inadvertently grant access to unauthorized individuals, and false negatives, which could mistakenly prevent rightful access to the home.

User Concerns. Despite the potential benefits of settings up smart lock automation scenarios, the fear that convenience-oriented scenarios could inadvertently compromise security illustrates the need for careful consideration of the security implications of each scenario. Additionally, reliability issues, false alarms, human errors, and the occasional inconvenience represent significant challenges that need to be addressed to increase user trust and adoption of these technologies. The concerns over reliability, in particular, highlight the importance of ensuring that the smart home devices involved in automation scenarios, especially devices that can send an unlock request to the smart lock, operate with high accuracy and dependability.

Factors Influencing Adoption. The willingness of participants to set up most automation scenarios, even those requiring additional setup or configuration, indicates a strong interest in harnessing the benefits of smart lock integrations. However, the resistance to monthly subscription fees, especially for convenience-oriented scenarios, suggests that cost can be a significant barrier to adoption. The concerns about false positives and negatives further emphasize the importance of accuracy and reliability in the design of automation scenarios, particularly those critical to security and safety. Participants expressed greater concern over false negatives in scenarios related to safety, security, or privacy, where failing to act could have dire consequences. Conversely, false positives, particularly in convenience-oriented scenarios, were seen as potential security and privacy risks, highlighting the intricate balance between enhancing convenience and ensuring security.

5.5 Limitations

This study acknowledges several limitations, including the small sample size and the potential for selection bias given the convenience sampling method. Additionally, the scenario-based approach relies on participants' imagination and understanding of smart home technology, which may not fully capture the complexities of real-world implementation. Future studies could address these limitations by involving a larger, more diverse participant pool and incorporating hands-on experiences with smart home devices.

5.6 Conclusion

This study aimed to explore end users' motivations and concerns regarding creating smart home automation scenarios that include the smart lock. Additionally, we investigated the factors that affect the users' decision to create such automation scenarios and explore the impact that creating such scenarios has on different aspects of the smart home environment. The significance of this research lies in the central role that smart locks play in numerous smart home automation scenarios due to their strategic installation location within the home and their ability to control physical access to the house. Through the analysis of 87 automation scenarios involving the smart lock created by 21 participants, we have highlighted the significant potential of smart locks to enhance not only the security and safety of homes but also to bring about improvements in convenience and awareness through automation. Furthermore, the willingness of users to accept certain trade-offs, such as increased electricity consumption or reliance on internet connectivity, in exchange for the benefits provided by smart lock automation, indicates a complex landscape of user priorities and acceptance levels. This acceptance, however, is not without its limits, as demonstrated by the concerns regarding privacy, security, reliability, and the potential false alarms. Future research should explore innovative solutions to these challenges, possibly through advanced technologies such as machine learning algorithms for better threat detection and management, or through more user-friendly interfaces that simplify the setup and management of automation scenarios. In conclusion, the integration of smart locks into home automation scenarios presents a promising avenue for enhancing the security, convenience, and awareness of smart homes. However, realizing this potential requires addressing the concerns and factors influencing user adoption. By doing so, we can pave the way for more secure, convenient, and intelligent smart home environments.

CHAPTER 6: EXPLORING THE END USER'S PERCEPTIONS, REQUIREMENTS, AND CONCERNS REGARDING SMART LOCK AUTOMATION SCENARIOS INVOLVING MULTIPLE SMART HOME DEVICES

6.1 Research Purpose

Several commercially available smart home hubs and platforms, such as Apple's home app or Samsung's SmartThings app, give smart locks owners the ability to create automation scenarios that involve multiple smart home devices. Furthermore, users can also create chained automation scenarios where one automation scenario is used to trigger another. Simple automations involving only smart locks (i.e., if it's after 7pm, then the smart lock locks the door) are generally straightforward but can be limiting in terms of functionality. On the other hand, including more smart home devices in those automation scenarios can increase their robustness and help make them more tailored to the user's needs. In fact, the findings from chapter 5 show that about 84% (n=73) of the automation scenarios created by the participants contained at least 2 smart home devices in each scenario. However, prior research shows that such automation scenarios can be susceptible to vulnerabilities such as integrity violation, when one device takes action based on information received from a less trusted device, and feature interaction, when the value of an actuator cannot be determined due to a logical conflict caused by the interaction of multiple rules [95, 79]. Additionally, creating automation scenarios that involve multiple smart home devices usually requires configuring each of the devices individually before setting up the automation scenario. Even though doing so might add to the complexity level of setting up an automation scenario, failing to properly configure the devices may lead to unexpected results or security issues upon executing the scenario. In the case of smart locks, this can include unauthorized access or locking residents out of their homes.

In this study, we conducted semi-structured interviews with a total of 30 participants. During the interviews, we show the participants a series of videos in which we gradually add more triggers, actions, or devices to an automation scenario that aims to automatically unlock the user's home to provide a service to the user (in-home package delivery). The goal is to explore the end user's perceptions of the limitations and security and privacy concerns associated with the triggers, actions, or devices explained in each video. Additionally, we explore the level of user-controlled settings and configuration needed to enhance the robustness of such automation scenarios and improve the end user's level of trust in them. As part of this study, we investigated the following research questions:

- RQ1: How do end users perceive the limitations, pitfalls, and concerns associated with smart lock automation scenarios that involve multiple smart home devices?

- RQ2: What types of configurations and customization options do end users need to have control over while setting up such automation scenarios in order to mitigate those concerns and limitations?

- RQ3: How does incorporating multiple smart home devices and conditions into a smart lock automation scenario affect the level of trust and perceived level of complexity end users have towards such automation scenarios?

6.2 Methodology

We conducted a semi-structured interview study with 30 participants in order to explore the end users' perceptions, requirements, and concerns associated with setting up smart lock automation scenarios that also involve other smart home devices. Semi-structured interviews allowed for an in-depth discussion on the types of configurations or concerns the participants had that might not have been fully captured through structured questionnaires.

6.2.1 Participants

The participants were recruited through Reddit Forums, Craigslist ads, and a mass email sent to the students and employees at the university. Potential participants were asked to fill out a screening survey to verify that they meet our recruitment criteria of being at least 18 years old and live in the United States. A total of 30 participants were recruited. 14 participants were males while 16 were females and all of them live in the United States. The average age of the participants was around 34 years old. The majority of participants self-reported having either an average (n=11) or somewhat above average (n=11) experience when it comes to setting up smart home devices. Additionally, three participants reported having a far above average level of experience, while four participants believed their level of experience was somewhat below average and only one participant was far below average.

Table 10: Participants' demographic information - fourth study

Participant	Gender	Age	Occupation	Experience level
P1	Male	32	Web developer	Somewhat above average
P2	Male	42	Construction worker	Somewhat above average
P3	Male	36	Cyber security analyst	Far above average
P4	Male	31	Surveyor	Average
P5	Female	33	Executive assistant	Far below average
P6	Female	31	Postdoc	Somewhat above average
P7	Female	42	Business coordinator	Average
P8	Male	29	Postdoc	Somewhat above average
P9	Male	19	Student	Somewhat above average
P10	Female	23	Program assistant	Average
P11	Female	30	Postdoc	Somewhat above average
P12	Female	61	Lecturer	Somewhat below average
P13	Male	50	IT Technician	Average
P14	Female	41	Educator	Average
P15	Female	36	Counselor	Average
P16	Female	28	Research assistant	Somewhat below average
P17	Female	30	Student	Average
P18	Female	22	Graduate assistant	Average
P19	Female	28	Student	Average
P20	Male	22	Student	Somewhat above average
P21	Female	27	Student	Somewhat above average
P22	Male	40	Student	Far above average
P23	Male	38	Academic advisor	Far above average
P24	Male	27	Research assistant	Somewhat above average
P25	Male	26	Student	Average
P26	Female	57	Banner programmer	Somewhat above average
P27	Male	46	System administrator	Somewhat below average
P28	Female	37	IT analyst	Somewhat above average
P29	Male	22	Student	Average
P30	Female	23	Student	Somewhat below average

6.2.2 Procedure

We contacted the participants who were eligible to participate in the study based on their answers to the screening survey questions to arrange a date and time to conduct the study. The study was approved by the university's Institutional Review Board (Protocol #24-0404). All of the interviews were conducted virtually through Zoom, an online meeting platform. Each interview was voice recorded using Zoom's meeting recording feature. The interviews started with asking the participants some demographic questions then giving them a brief introduction of the concept of smart home automation and the general purpose of the study.

During the interview, the participants were shown a total of 6 videos. Each video shows the configurations and execution of a part of an automation scenario that enables the smart lock to automatically unlock the home's front door for a delivery driver to deliver a package inside the home. We chose this automation scenario specifically to be presented to study participants for four main reasons:

1. It fulfills a distinct purpose and offers a service to the user by ensuring package security through enabling indoor delivery.

2. It introduces a level of uncertainty regarding the trustworthiness of such an automation scenario, due to the potential for both false positives and false negatives upon execution. This increases the importance of the security measures integrated into the scenario.

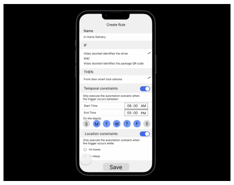
3. It incorporates several smart home devices which are a smart lock, a smart video doorbell, and a security camera.

4. The automation involves processes that occur both outside and inside the house.

By analyzing feedback on specific functionalities that are usually controlled through the other devices involved in the automation, such as facial recognition and QR code scanning, alongside the participants' responses to scenarios involving security breaches and notification protocols, the study can extrapolate how users perceive such automation scenarios in general. Below is a description of the content of each video:

Video 1 - Face recognition and scanning the QR code to unlock the door:

- The delivery driver approaches the door and rings the doorbell.
- The video doorbell recognizes that the driver is holding a package.
- The driver is asked to stand in front of the camera for face recognition.
- The driver is then asked to scan the QR code through the video doorbell camera.



Create Rule

Name

In-home Delivery

IF

Video doorbell identifies the driver

AND

Video doorbell identifies the package QR code

THEN

Front door smart lock unlocks

Temporal constraints

Only execute the automation scenario when the trigger occurs between:

Start Time 08:00 AM

End Time 05:00 PM

On the day(s):

S M T W T F S

Location constraints

Only execute the automation scenario when the trigger occurs while:

○ I'm home

○ I'm Away

Video 2 - Adding temporal and location constraints to the automation scenario:

- The video shows examples of temporal and location constraints.
- The video explains that such constraints can be configured to give the homeowner more control over when the automation scenario can be executed.

Video 3 - The door unlocking:

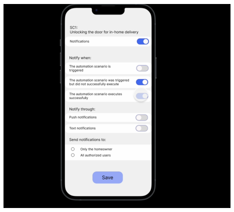
- The video shows the door unlocking for the driver to make the delivery solely based on the three conditions explained in the previous two videos.

Video 4 - The security camera detects the driver inside the house without going beyond the delivery zone:

- The video shows the driver opening the door, stepping into the hallway, and dropping the package inside (all within the delivery zone).
- Once the driver drops the package, he is instructed (through the security camera) to lock the door upon leaving.

Video 5 - The driver goes beyond the delivery zone:

- The video shows the driver opening the door, stepping into the hallway, and going into the home beyond the delivery zone.
- The video shows that a siren will go off and a video will be recorded and sent to the homeowner when the driver goes beyond the delivery zone.



SC1:
Unlocking the door for in-home delivery

Notifications ☑

Notify when:

The automation scenario is triggered □

The automation scenario was triggered but did not successfully execute ☑

The automation scenario executes successfully ☑

Notify through:

Push notifications □

Text notifications □

Send notifications to:

○ Only the homeowner
○ All authorized users

Video 6 - Notifications:

- The video shows how notifications will be configured and what controls are available to the user.

After watching each video, the participants were asked questions to evaluate the part of the automation scenario that was shown in the video, which are:

- Relying on information received from the video doorbell to unlock the home's front door (video 1).
- Adding temporal and location constraints to automation scenarios that involve automatically unlocking the home's front door (video 2).

- Having the home's front door automatically unlocked based solely based on the conditions discussed in videos 1 and 2 without considering other safeguards to control what happens once the door unlocks (video 3).

- Including another smart home device (the security camera) in the automation scenario and having a part of the automation scenario executed inside the house (video 4).

- Incorporating the concept of "consequences" into the automation scenario as a mitigation strategy for security concerns (video 5).

- Exploring the aspect of setting up and configuring notifications for smart lock automation scenarios that involve several smart home devices (video 6).

The last part of the interview was dedicated for overall evaluation questions to explore any residual concerns or limitations perceived by the participants after they had acquired a more thorough understanding of the automation scenarios showcased in the videos. After the interview, each participant was compensated with a $10 Amazon gift card.

6.2.3 Data Analysis

All of the interviews were audio recorded and then transcribed. To analyze the qualitative data, we utilized an inductive coding approach. The data was coded by one researcher to create the codebook. Two researchers then conducted several meetings to discuss and finalize the codebook. During these sessions, the codes were critically evaluated for consistency and relevance, and modifications were made to ensure comprehensive coverage of the data. The finalized codebook served as the foundational framework for the systematic categorization of the data. As for analyzing quantitative data, such as the participants' perceived levels of trust and complexity associated with the automation scenarios, we utilized descriptive statistics as well as Friedman's significance test and Pearson's correlation.

6.3 Results

6.3.1 Concerns and Limitations

In this section, we explore the perceptions of end users regarding the limitations and potential drawbacks of setting up smart lock automation scenarios that involve multiple smart home devices (RQ1). The study revealed in limitations related to technological reliability, operational and practical concerns, and security, privacy, and trust concerns.

6.3.1.1 Technological Reliability

System Accuracy. The participants' concerns regarding system accuracy after watching the videos indicate a general concern towards the reliability and robustness of several devices involved in the automation scenario. After video 1, which demonstrated face recognition and QR code scanning for unlocking the door, a significant number of participants (n=16) expressed doubts about the video doorbell's ability to accurately recognize faces and scan QR codes, especially under less-than-ideal conditions such as poor lighting, facial changes (e.g., shaving a beard), or wearing accessories like hats or masks. Concerns were not only about false negatives (failing to recognize legitimate drivers) but also about false positives (incorrectly recognizing

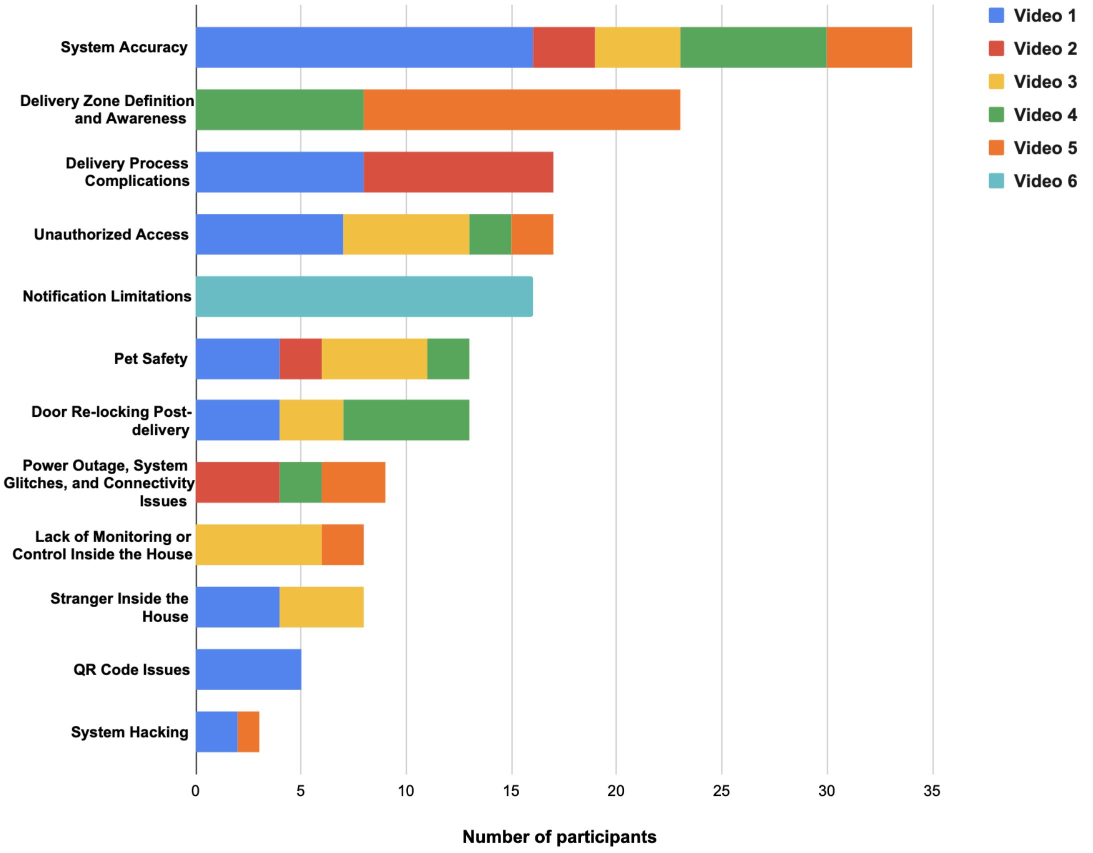


Figure 17: The participants' perceived concerns and limitations after watching each video

someone as a legitimate driver).

> **P30:** *”One big fear for me would be let's say the delivery driver doesn't even come in the house. They just put down the package, and someone else then picks up the package, and the camera doesn't discriminate the way it should.”*

Fewer participants expressed specific concerns about system accuracy after video 2, which focused on adding temporal and location constraints. Only 3 participants mentioned such concerns, primarily focused on the limitations of using phone location as a proxy for the homeowner's absence. The participants mentioned scenarios where the system might fail to accurately assess whether the home is empty or not in order to accurately enforce the location constraints set by the users.

Video 3, which depicted the door unlocking, reignited concerns about facial recognition's accuracy (n=4). These concerns were similar to those raised after video 1, indicating the importance of incorporating accurate biometric identification for the system's integrity.

Concerns shifted slightly for videos 4 and 5, which showed the driver inside the home and the potential for going beyond the delivery zone, respectively. A total of 11 participants across these two videos raised issues regarding the accuracy of package and person detection within specified zones. This lack of accuracy can be due to factors like lighting, camera angles, and motion detection reliability. Overall, the participants were concerned about the system's ability to accurately monitor and enforce the designated delivery boundaries.

QR Code Issues. Some participants (n=5) raised concerns about QR code reliability in video 1. The participants highlighted issues related to QR codes like physical deformities such as scratches or placement issues could prevent the QR code from being scanned correctly. This could potentially bar entry for legitimate deliveries or causing packages to be left outside. These concerns reflect the need for a fail-safe mechanism, such as a digital QR code accessible via a smartphone, to ensure seamless delivery operations despite physical QR code challenges.

Power Outage, System Glitches, and Connectivity Issues. Concerns about power outages, system glitches, and connectivity issues were evident across participants' responses after watching video 2, 4, and 5, though the emphasis and specific concerns varied somewhat from one video to the next.

After video 2, some participants (n=4) expressed concerns about these issues. These issues revolved around the potential for power outages to disrupt the system or glitches to result in accidental unlocking or locking at inappropriate times. Concerns also included the possibility of system resets due to Wi-Fi outages or software updates that could inadvertently alter scheduled automations.

Video 4 prompted concerns from two participants, again highlighting worries about power outages and Wi-Fi reliability affecting the functionality of the security camera and door unlocking mechanism. The emphasis here was on ensuring that essential components like cameras remain operational for the system to function correctly, even suggesting user-configurable options for how the automation should execute during power or connectivity losses.

> **P19:** *"There's always a risk with the more complicated you make something that something is going to go wrong somewhere, and it's not all going to communicate, especially if it relies on Wi-Fi or electricity. If there's a power outage, or if WiFi goes out, this could kill the whole command chain."*

After watching video 5, three participants addressed issues related to internet connectivity, particularly the implications for cloud storage and internal storage options during Wi-Fi outages. Concerns were about ensuring data (video footage) remains accessible and secure even when external factors like power or internet service interruptions occur.

Notifications Limitations. After watching video 6, which discussed configuring notifications for each step of the automation scenario, 16 participants expressed several concerns associated with notifications. Some participants (n=7) expressed concerns regarding the possibility of missing important security notifications due to various everyday circumstances. They highlighted that users might miss critical alerts because notifications can be inadvertently turned off or silenced. Therefore, some of these participants emphasized the importance of offering users the option to receive notifications through phone calls. Other participants (n=4) expressed concerns about potential delays in receiving notifications from the automation system, which could be crucial in security situations like unauthorized access or breaches of delivery zones. Three participants were concerned about potentially receiving an excessive number of notifications from the automation system, which could lead to annoyance and user disengagement. They highlighted the risk of users becoming overwhelmed and possibly muting all notifications, thus missing important alerts. Furthermore, two participants were concerned about the reliability of the smart home system in sending notifications, highlighting scenarios where system glitches or connectivity issues could prevent notifications from being sent. This could also pose significant security risks, particularly if the system fails to alert users of critical events like unauthorized access.

6.3.1.2 Operational and Practical Concerns

Delivery Process Complications. The participants' concerns regarding the complications in the delivery process after watching videos 1, 2, and 3 reveal a nuanced perspective on operational and logistical challenges. After video 1, some participants (n=8) articulated concerns about the practicality of implementing such an advanced delivery system. Those participants focused on the variability in delivery personnel due to factors such as illness, use of third-party delivery services, and logistical changes. These concerns centered on the system's ability to adapt to real-time changes in delivery personnel and the potential slow down in the delivery process due to the additional steps required for verification, which could, in turn, affect the efficiency and convenience of deliveries.

Video 2, which added temporal and location constraints to the delivery process, elicited concerns from 9 participants. Participants worried about the system's inflexibility in cases of unexpected schedule changes, delays in delivery, or the necessity for manual overrides to allow for exceptions. Therefore, the participants were concerned about the system's ability to handle dynamic and unforeseen circumstances without causing inconvenience or necessitating frequent manual interventions to update the automation settings.

Delivery Zone Definition and Awareness. After watching videos 4 and 5, participants expressed significant concerns about the definition and awareness of the delivery zone by the delivery drivers. After watching video 4, some participants (n=8) raised concerns about whether drivers would be aware of and able to identify the designated delivery zone within the home. The concerns focused on the potential ambiguity in the boundaries of the delivery zone and questioned how drivers would know where exactly to place packages without explicit indicators.

Video 5 intensified these concerns, half the participants (n=15) reiterating the issue of driver awareness regarding the delivery zone. The feedback highlighted worries that drivers might inadvertently breach the delivery zone due to lack of clear demarcation, leading to false alarms or unnecessary complications. Some participants (n=7) specifically highlighted the risk of false alarms triggered by such innocuous actions, raising questions about the system's ability to accurately discern genuine security threats from mundane delivery activities. Participants speculated on various impractical solutions, such as marking the floor or relying on technology like projectors to outline the zone, to address this issue.

> **P24:** *"The driver might not be aware of the package delivery zone. I could perceive a situation where the authorities are called because the user set the delivery zone too small and the driver wasn't aware of that."*

6.3.1.3 Security, Privacy, and Trust Concerns

Unauthorized Access. Concerns about unauthorized access were mentioned by participants after watching videos 1, 3, 4, and 5, reflecting varying degrees of concern about the potential for the system to be manipulated or fail in preventing unwanted entries. After video 1, seven participants were concerned that the reliability issues associated with facial recognition and QR codes might lead to unauthorized individuals being granted access. The primary concern was the system's vulnerability to being tricked, for instance, through the use of a driver's photograph by an unauthorized person, or misidentification due to technological limitations.

After watching video 3, six participants expressed concerns about scenarios where an individual could follow the delivery driver into a home or apartment complex (tailgating), leveraging the automated door-unlocking mechanism to gain entry without authorization. This highlighted a different aspect of security that focuses on the physical act of unauthorized entry following authorized access.

Furthermore, after watching video 4, two participants were concerned about the system's ability to detect and respond to situations where an unauthorized second person enters the house along with the delivery driver, pointing to potential gaps in the system's monitoring capabilities.

Finally, after video 5, two participants reflected on the limitations of alarms in deterring determined intruders. Those participants stated that the presence of an alarm system might not be sufficient to prevent unauthorized access by someone intent on bypassing the system. In this case, while the driver entering the house to deliver the package is authorized, going beyond the delivery zone further into the house is considered here as an unauthorized access.

> **P19:** *"I think the setup is fine. Executing the consequences is fine. But if someone is willing to break the rules in general, I don't think they care about the consequences. So, I don't know how much of a deterrent that may be for someone who really wants to break and steal or whatever they may want to do."*

System Hacking. Concerns about system hacking were explicitly mentioned by participants after watching videos 1 and 5, highlighting fear regarding the security of the smart home automation system against cyber threats. After video 1, two participants expressed worries about the potential for the system to be compromised through hacking. One participant pointed out the inherent risk in online systems, fearing that hackers could manipulate the system to either fail to recognize legitimate entries or falsely recognize unauthorized access. Another participant speculated on the possibility of hacking the QR code used for entry, though they felt that the combination of driver face ID and QR code could offer a reasonable level of security.

P15: *"It's an online system and online systems can oftentimes be hacked."*

However, after video 5, one participant was concerned about hacking the camera system to disable alarms or create the appearance of normalcy to facilitate unauthorized access.

Pets Safety. Participants across videos 1 (n=4), 2 (n=2), 3 (n=5), and 4 (n=2) expressed concerns about pet safety in scenarios involving smart home automation and delivery access. Concerns ranged from pets escaping when doors are left open after the delivery takes place to potential aggressive encounters between pets and delivery personnel. This indicates the need for smart home automation systems that involve unlocking the smart lock to include safety measures that account for pets, suggesting options for pet owners to control or disable automatic door unlocking. Additionally, those systems could provide clear instructions and warnings to the driver about pets being in the house during a scheduled delivery.

Door Re-locking Post-delivery. Concerns about the door re-locking after delivery were highlighted by participants after watching videos 1, 3, and 4, revealing a significant concern regarding the system's reliability in ensuring that the door locks properly once the delivery person leaves. In video 1, some participants (n=5) worried about the delivery driver's potential to leave the door open, either inadvertently or because they might not ensure the door relocks upon them leaving the house. Those participants were concerned about the potential for pets to escape or unauthorized access to occur if the door was left unlocked post-delivery.

> **P18:** *"I have had issues in the past with delivery people and other sort of service people leaving doors open by accident, and my pets have gotten out before."*

After watching video 3, concerns persisted with participants (n=3) questioning whether drivers would remember to lock the door upon leaving and whether they would know how to properly secure it. The idea of providing drivers with instructions on how to securely close and lock the door was mentioned, indicating an understanding that the responsibility of door locking might not be intuitive for all delivery personnel, especially given their varying levels of familiarity with different door mechanisms and their haste during deliveries.

However, after watching video 4, the participants (n=5) focused on ensuring that there was a confirmation mechanism for both the delivery personnel and the homeowner that the door had indeed been locked properly after delivery. Participants suggested additional alarms or notifications to alert drivers if the door wasn't securely closed, reflecting a desire for more direct control or feedback mechanisms that could verify the door's status post-delivery.

Lack of Monitoring or Control Inside the House. Concerns about the lack of monitoring or control inside the house after delivery personnel gain access were expressed by participants after watching videos 3 (n=6) and 5 (n=2). After watching video 3, concerns centered around the inability to see or monitor the delivery person's actions inside the house and a general concern regarding the amount of time a driver spends inside. Participants highlighted the need for more direct oversight, such as CCTV monitoring, to ensure the delivery person exits promptly and does not engage in unauthorized activities.

> **P10:** *"I guess my only concern would be that there is no time on it and the driver is not required to exit the house within a certain amount of time."*

In contrast, the concerns after watching video 5 were more focused on the technical limitations of existing surveillance capabilities of the security camera installed in the hallway. For example, there was a concern about the camera's lack of ability to follow the delivery person's movements within the house. The participants were mainly concerned regarding the inability to track the driver if they moved beyond the predetermined delivery zone. This would leave homeowners uncertain about the handling of the package or the driver's activities once they have gone beyond the delivery zone.

Stranger Inside the House. Concerns about the personal security implications of granting delivery personnel access to one's home were raised by participants after watching videos 1 (n=4) and 3 (n=4). After watching video 1, concerns were broadly focused on the discomfort and unconventional nature of allowing a delivery person, a stranger, into the house, emphasizing the risk of fraud or simply the unease associated with the idea of an untrustworthy individual being inside one's private space without supervision. Participants articulated a general discomfort with the idea, despite recognizing the safeguards in place to prevent unauthorized access.

> **P21:** *"I am not comfortable with having anyone open my door or be inside my apartment when I am not here."*

However, after video 3, the concerns shifted slightly towards more specific worries about the lack of control over what happens once a delivery person is inside the house, emphasizing the potential for theft or other issues due to the inability to monitor the stranger's actions closely. The concerns highlighted include the discomfort with not only the theft risk but also the broader implications of granting such access, such as the psychological discomfort with the idea of any person being able to enter the home when the homeowner is absent, and the desire for confirmation that the person has indeed left the house.

6.3.2 Settings and Configurations

In this section, we explore end users' perceptions regarding the type of customization options needed to help mitigate the limitations and concerns associated with smart lock automation scenarios which involve several smart home devices (RQ2). The study revealed various settings related to security and communication.

6.3.2.1 Security Configurations

Manual Override. One of the configuration options that a significant number of the participants stated they needed to be able to control while setting up the automation scenario was the ability to manually override. This feature would allow homeowners to retain some control over the unlocking process, even in an automated system. After video 1, some participants (n=12) expressed a desire for the system to not automatically unlock the door for the delivery driver without additional verification or approval from the homeowner. They highlighted the importance of receiving a prompt or notification that would enable them to manually approve the unlocking of the door. Such an option enables the homeowner to verify the situation before granting access as well as lowers the possibility of false positives.

Similarly, after video 3, five participants reiterated the significance of having manual control and override features. They emphasized the need for an extra layer of authentication and the ability to manually disable the automation scenario, particularly when no in-home package deliveries are expected. Generally, some participants were particularly concerned about having a fully automated system when the smart lock is involved which shows the desire for a balance between automation and personal oversight.

> **P30:** *"It would be nice to have a pop up on your screen where it's like,this person is at your house with your package. If you are willing to let them in, you see the face and you put yes or no. Have that safeguard. At least have that as an option."*

More Authentication. Upon watching video 1, which showcased face recognition and QR code scanning for unlocking the door, participants expressed some interest in enhancing security measures through improving authentication. A third of the participants (n=10) suggested incorporating multi-factor authentication (MFA) mechanisms, such as push notifications for manual unlock approval, alternative biometric verifications (e.g., fingerprint recognition), the use of verbal or numeric passcodes, and even the possibility of requiring the delivery driver to present their work ID for camera verification. Similarly, after watching video 3, five participants also mentioned the need for an option to add more authentication methods while setting up the automation scenario in order to decrease the possibility of having the door automatically unlocked for anyone impersonating the assigned delivery driver.

> **P2:** *"After facial recognition recognizes the driver and the QR code has been scanned, I think the companies should also have some sort of verification code as part of the recognition system."*

Constraints and Restrictions. Across the responses to videos 1, 3, 4, and 5, a notable number of participants expressed the need for options to add more constraints and restrictions while setting up the automation scenario. After watching video 1, seven participants mentioned the need for time-based restrictions, such as only allowing entry during specific hours, limiting attempts at face recognition, and ensuring the system is activated only when someone who lives in the house is expecting a package.

After watching video 3, four participants emphasized the importance of setting specific time frames for drivers inside the house to prevent them from overstaying and having enough time to engage in unauthorized activities inside the house. One participant also suggested having a delivery zone that the driver is not allowed to cross which is a feature that was introduced in video 4. The need for strict time limits for the delivery process inside the home was also reiterated by a total of 4 participants after watching videos 4 and 5.

> **P26:** *"Let the driver know that they have a certain amount of time as well inside the house before they have to leave."*

Re-locking the Door. Some participants were keen on ensuring that the door automatically re-locks after the delivery process to maintain the security of their homes. After video 1, four participants expressed the need for an automatic door re-locking feature to be included in the automation scenario to ensure that the door unlocks after the delivery is complete.

Furthermore, after watching video 3 (n=4), video 4 (n=4), and video 5(n=1), some participants mentioned the need for a verification process for door locking, suggesting the use of sensors to confirm door closure and even proposing automatic notifications to drivers or emergency calls if the door remains unlocked. Some participants also suggested that the drivers need to scan another QR code upon leaving the house to confirm that the door was properly locked when they left the house.

> **P5:** *The door might not be properly locked after the driver leaves. I think there should be confirmation to the driver that the door has been sufficiently closed and locked.*

Incorporating More Smart Home Devices. After viewing videos 1 and 3, participants expressed a strong interest in the ability to integrate additional smart home devices into their automation scenarios. After video 1, one participant suggested adding a smart speaker to the automation scenario in order to audibly alert household members inside the house when the door is unlocked for a delivery while some residents are home during the delivery.

However, after watching video 3, some participants (n=8) suggested incorporating additional security cameras and smart home security alarms into the automation scenario. The purpose of including the security camera was to ensure visibility inside the house. Participants were interested in live feeds, timestamped delivery confirmations, motion alerts within the home, and the potential for recorded evidence in the event of a theft or unauthorized activity. The addition of a smart home security alarm to the automation scenario was to have it automatically disarmed temporarily when the door is unlocked during the delivery process.

> **P24:** *"Maybe we should add to the automation scenario a smart security camera pointed towards the door that displays a live feed. Just an extra set of precautions then maybe just like a slight recording, just in case anything were to be stolen or swiped. You can look at the camera and go."*

Control the Delivery Zone. After viewing video 4, which focused on the delivery zone, nine participants mentioned the need for more controls when it comes to configuring the delivery zone. Those controls included customizable alerts when a delivery person leaves the designated delivery zone, the capability to tailor the size of the delivery zone to their preferences, and the deployment of alarms to signal unauthorized movements. They also suggested advanced motion detection technologies that could track and follow a delivery person's movements outside the zone. Some participants also called for immediate notifications for any deviations from the delivery zone, an expansion of camera surveillance to monitor and alert on movements beyond this zone, and specific alerts for detecting multiple individuals inside the house during the delivery process.

> **P10:** *"I would like to be able to adjust the area of the delivery zone, so that way, it's not too big. Just enough for the driver to put the package in there and then get back out."*

Control the Consequences. After watching video 5, some participants (n=9) expressed a desire for enhanced control over the timing of security breach consequences. Three participants suggested establishing two distinct zones for delivery, a smaller and a larger one, with drivers receiving alerts upon exiting the smaller zone. However, if they get beyond the larger zone, then the consequences (sounding a siren, uploading a video to the cloud, and notifying the homeowners) should be triggered. Six participants mentioned the need to be able to add "contacting the authorities" as one of the consequences. However, none of the participants wanted this to take place immediately once the driver gets beyond the delivery zone. Instead, they preferred that this measure be taken only after the driver had been previously warned and had been given a certain amount of time (defined by the user) to return to the delivery zone.

6.3.2.2 Communication Configurations

Communication with the Driver. Participants' responses after watching videos 1, 3, 4, and 5 reveal a strong preference for incorporating communication options with the delivery driver into the automation scenario, enhancing both the security and efficiency of the delivery process. After video 1, one participant suggested an app-based method for real-time communication with the driver, like calls or interactive doorbell features, to provide specific directions to the delivery person.

Similarly, after watching video 3, some participants (n=2) proposed giving the user options to send text messages and leave voice recordings for the delivery person to ensure clear instructions are conveyed for package placement within designated areas.

Following video 4, six participants further emphasized the importance of communication, suggesting features such as recording personalized reminders for the driver and using audio instructions to navigate the delivery process. The idea was to record a welcoming voice message that also serves as a reminder that the delivery is being monitored during the delivery process. Other participants mentioned the need for a microphone feature to facilitate direct communication with the driver.

> **P16:** *"Communication with the delivery person and give them instructions, like put the package in here, you're currently being recorded. Maybe the driver starts to go beyond the delivery zone, maybe I can give another instruction, like, please go back to the door and leave the door, something like that. I would want the driver to know that you cannot just walk around."*

After video 5, there was a significant increase in the interest for communication options with fourteen participants discussing various methods to inform the driver of the delivery zone boundaries and expectations. Suggestions included visual displays

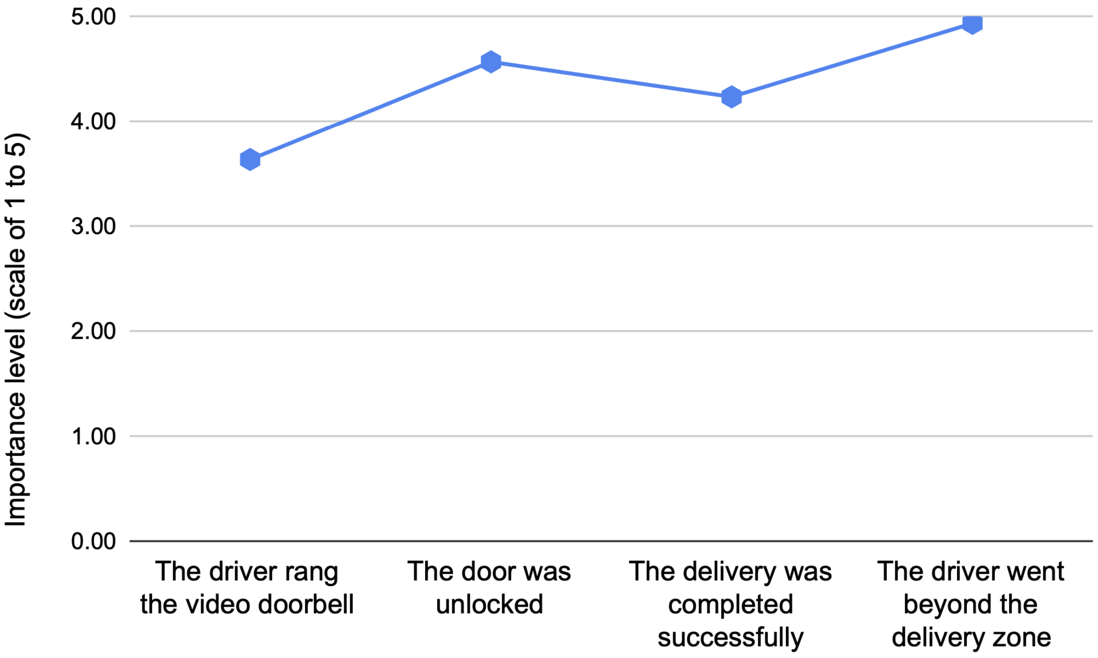


Figure 18: The participants' assessments of the importance of receiving notifications at each stage of the automation process

to delineate the delivery zone, messages alerting the driver upon entering or exiting the zone, and preferences for non-aggressive notifications such as gentle reminders or instructions rather than startling alarms. The idea of two-way communication was also proposed to allow homeowners to directly address drivers who stray beyond the delivery zone, providing an opportunity for clarification before escalating the situation.

Notifications Configuration. Participants, after watching video 6, expressed a clear desire for enhanced notification configurations while setting up the automation scenario which spans several key areas. Five participants stated that there needs to be an option to notify the authorities when the driver goes beyond the delivery zone. Half of the participants (n=15) desired notifications across additional channels such as phone calls, emails, and a continuous vibrate feature. The idea was to ensure that homeowners receive alerts through the most effective means possible which is especially important in cases where there is a security threat. Eight participants highlighted the importance of selective notification preferences to allow homeowners to customize which users are notified about specific events and even create individual notification profiles with priority settings for crucial security alerts. For example, two participants stated that they want such a system to allow them to create a notification profile for their trusted neighbors or emergency contact where they only get notified if the driver goes beyond the delivery zone. Six participants also specifically requested step-by-step notifications for detailed updates at each stage of the delivery process, from arrival to package placement and departure, providing comprehensive yet concise information for peace of mind and transparency. Four participants also suggested notifying the homeowner and the driver in case the driver forgets to re-lock the door properly upon leaving. We also specifically asked each participant, on a scale of 1 to 5, how important it is to get a notification during each step of the automation process. The results, as depicted in figure 18, show that the majority of participants found it important to get notifications for each step of the process. However, as expected, it was more important for the participants to get notified when there is a security concern, such as the door being unlocked ($\bar{x} = 4.57$) or the driver getting beyond the delivery zone ($\bar{x} = 4.93$). Getting real-time notifications in these situations allows the homeowners/ authorized users to be aware of the situation, view live feeds through the security camera, and react in a timely manner based on the circumstances.

We asked the participants about who they think should get a notification during

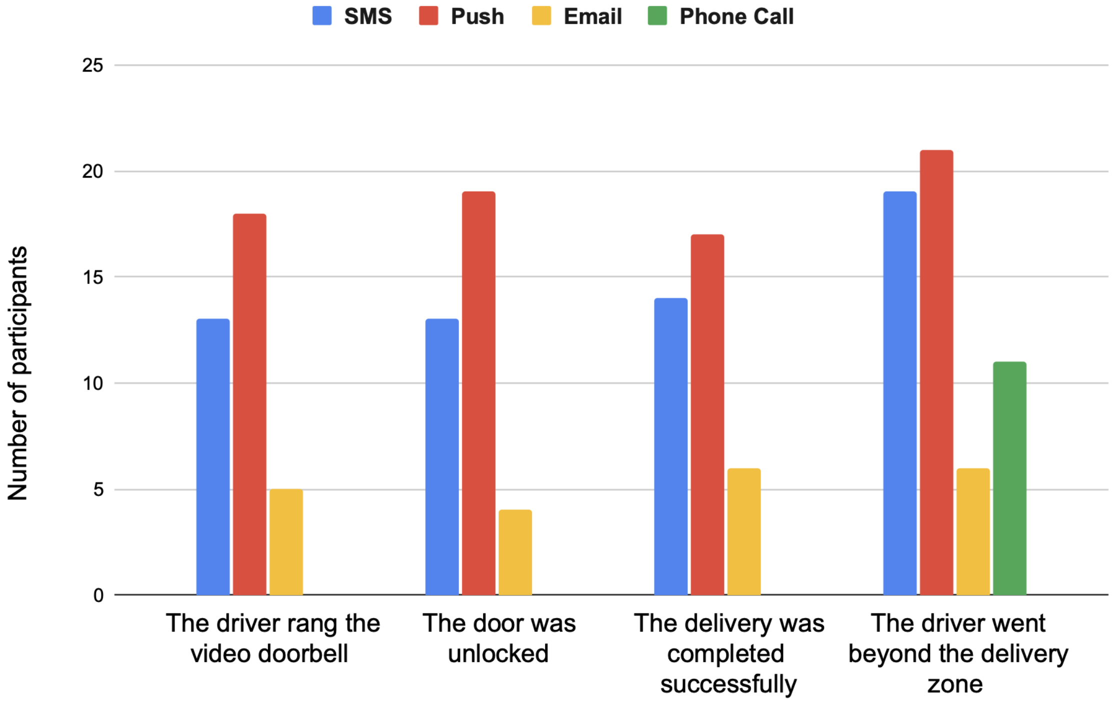


Figure 19: The preferred notification channels for each stage of the automation process

each step of the process. For the majority of participants, either all authorized users or only the homeowner should get notified during each of the steps (when the driver rings the video doorbell, the door is unlocked, the delivery is made successfully). However, if the driver goes beyond the delivery zone, 11 participants mentioned the need to notify non-residents as well, such as the delivery company, the authorities, or the emergency contacts. Three of those participants stated that the non-residents should only be notified if the driver was beyond the zone for a specific amount of time and not immediately as they cross the zone's boundaries. In terms of the content of these notifications, the majority of participants preferred the inclusion of a video or a picture that show the driver when they ring the video doorbell (n=19), place the package inside the house (n=18), or if they go beyond the delivery zone (n=28). As for

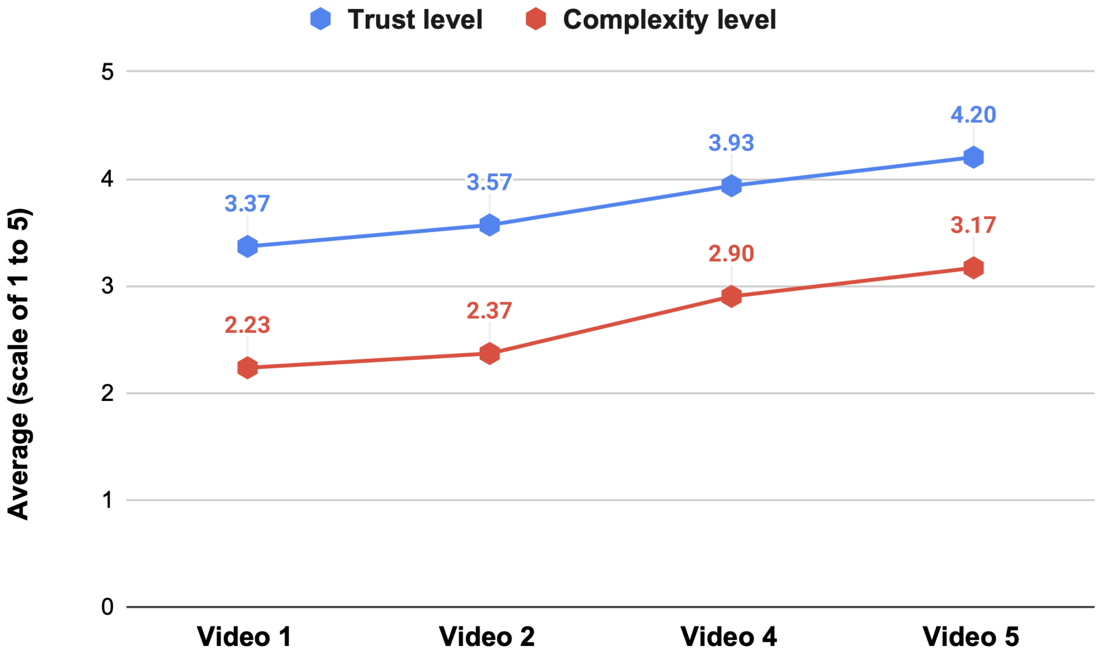


Figure 20: The participants' perceived level of trust and complexity of the automation scenario after videos 1, 2, 4, and 5

the channel through which the participants preferred to receive those notifications, the majority of participants preferred push and/or SMS notifications (figure 19). However, some participants also wanted to get those notifications through email, especially the ones that contain a picture or a video, either to keep it for their records, or to make sure they get those notifications while at work. Some participants (n=11) also wanted to be notified through a phone call if the driver goes beyond the delivery zone. Mostly because this will get them to see the notification faster compared to other notification approaches.

6.3.3 Trust Vs Complexity

Trust and complexity are two important factors that might affect the end user's decision to set up an automation scenario. While having a high level of trust in the automation and its security capabilities can encourage the end user to set it up, a high level of complexity involved in configuring that automation scenario can be intimidating to some users, especially those who are less familiar with the technology. Therefore, to address our third research question (RQ3), we asked the participants, on a scale of 1 to 5, about the level of trust they have in the automation scenario up to that point as well as the level of complexity they believe might be involved in configuring and setting it up (Figure 20). We asked both questions after each video that included adding more features, conditions, or smart home devices to the automation scenario, which are videos 1, 2, 4, and 5. The Friedman test revealed a statistically significant increase in participants' trust ratings across the four videos (Chi-square= 36.989, *df*=3, p< 0.001, α= 0.05). Similarly, the Friedman test also showed a statistically significant increase in the participants complexity ratings across the four videos (Chi-square= 41.291, *df*=3, $p < 0.001$, α= 0.05). This indicates that participants' perceptions of trust and perceived complexity ratings significantly increased as more triggers, actions, and smart home devices were added to the automation scenarios presented in each video. The initial scenario (video 1), featuring face recognition and QR code scanning for door unlocking, established a baseline with average trust and complexity ratings of 3.37 and 2.23, respectively. Adding temporal and location constraints (video 2) slightly enhanced perceived trust (3.57) and complexity (2.37). A more notable increase in both trust (3.93) and complexity (2.90) was observed with the inclusion of a security camera that monitored the delivery zone and instructed the driver to lock the door upon exit (video 4). The highest levels of trust (4.20) and complexity (3.17) were recorded when the scenario included a security response and consequences to the driver going beyond the designated delivery zone (video 5). The Pearson's correlation test revealed a positive correlation between the complexity of the automation setup and the level of trust users place in it (r= 0.994, p=0.006, α= 0.05). Therefore, it's important to find a balance between user-friendly design and the capabilities required to enhance security and trust in such automation scenarios.

6.3.4 Overall Evaluation

After watching all six videos, the participants had gained a comprehensive understanding of the various automation scenarios presented. Therefore, we allocated the final section of the interview to gather a broad evaluation of the system from the viewpoint of the participants. Our primary aim was to explore any residual concerns and limitations perceived by the participants after they had acquired a more thorough understanding of the automation scenarios showcased in the videos. Furthermore, we wanted to explore the importance of security controls and customization options in improving such automation scenarios and mitigating the participants' concerns. The majority of the concerns participants had after watching all the videos were related to security, including worries about the presence of strangers in their homes (n=4), the risk of unauthorized access through hacking, or the reliability of other devices involved in the automation scenario (n=7). Some participants (n=3) expressed concerns regarding the possibility of the driver stealing or damaging their property, and one participant remained concerned about the door not closing properly post-delivery.

Participants unanimously highlighted the critical role of customizable security and privacy settings in such an automation scenario. Ten participants deemed the capability to receive real-time notifications at every phase of the automation process as the most crucial security feature to mitigate their concerns. Four participants emphasized the necessity of remote control options and the power to disable the automation via an app as fundamental security measures. Other participants (n=3) considered the ability to view a live video feed or cameras as one of the key controls that would help them alleviate their security and privacy concerns. Two participants also mentioned the need for integrating this automation scenario with existing home security systems in order to improve the smart home's response in case of security breaches during the delivery process.

> **P1:** *"I think notifications are the most important security settings that would alleviate my concerns as long as I'm getting notified in real time."*

None of the participants expressed any concerns regarding having several smart home devices involved in the automation scenario. In fact, several participants (n=9) believed that incorporating more devices could enhance the system and address some of its shortcomings. Yet, there were concerns about how the system would function if a device crucial to the automation scenario failed during a delivery. A specific worry for the majority of these participants was a situation where the indoor security camera, dependent on a power connection, failed due to a power outage while battery-powered devices like the smart lock and video doorbell remained operational, allowing the driver access to the home. Only five participants preferred the delivery to proceed under these circumstances, whereas the rest of the participants (n=25) wished for the automation to halt automatically if the security camera was non-functional. However, some of those participants (n=13) indicated that in the event of a camera malfunction, the system should evaluate factors such as the package's value (n=1), the weather conditions (n=1), how urgently the homeowner needs the package (n=2), and the driver's trust level (n=9) before deciding whether to unlock the door. Some were willing to accept the risk of letting a driver inside to deliver a valuable package or a package that contains items sensitive to specific weather conditions rather than leaving it outside. Similarly, other participants stated that they can make an exception in cases where they need the package to be delivered in a timely manner. Additionally, if the participants personally trusted the driver, based on a history of successful indoor deliveries, or if the driver had a high rating in the carrier's system, indicating a track record of successful deliveries without issues, they would be comfortable allowing that driver access even in the absence of a working camera.

> **P13:** *"I think the first part of the scenario is the most important part because that's where all the verification is done. So, if the security camera doesn't work then the driver should still be able to deliver the package. You have already verified the driver and the package. So, the second part of the camera is not that much needed."*

> **P20:** *"I think it would be nice if you could edit someone's profile and add them to a trusted list. Let's say a driver has a strike on his profile, but you've talked to him in person, and you think that it was an error and you trusted him, you should be able to add him as a trusted delivery driver."*

6.4 Discussion

Our study explored user reactions to a series of automation scenarios involving smart locks and additional smart home devices that were presented to the participants through videos. These scenarios revealed significant insights into the user concerns, requirements, and drawbacks associated with such automation scenarios. The six videos shown to the participants represent 3 different phases that can be seen in any automation scenario that involves the smart lock: 1) Pre-unlocking, depicted in videos 1 and 2; 2) Once the door is unlocked, depicted in video 3; and 3) inside the house, illustrated in videos 4 and 5, Video 6 covering notifications which overlap all three phases.

Pre-unlocking. During this phase, the primary concern was about the smart lock granting unauthorized access to the house due to video doorbell reliability concerns. Participants highlighted potential vulnerabilities such as the inaccuracy of facial recognition via the video doorbell and the system's failure to prevent tailgating. Consequently, there was a lack of trust in relying on the video doorbell to control the entire authentication process. The adoption of more secure authentication methods like biometric verification and numeric passcodes was frequently suggested as a way of mitigating such concerns. Implementing such authentication approaches will also involve the smart lock in the verification process and not rely completely on the video doorbell. Additionally, there was a strong preference to implement manual overrides as another method of authentication that gives the end user more control. This would enable homeowners to personally verify the visitor's identity through live video before authorizing the smart lock to unlock. During this phase, the participants also wanted to configure the settings by adding specific constraints related to when the automation should or should not execute and how much time the driver is allowed inside the house before a security notification is sent to the homeowner and the delivery company.

Once Unlocked. The main concern during the second phase was pets' and driver's safety. Given that in-home deliveries often occur in the absence of residents, the constant presence of pets poses unique challenges. Participants worried about potential dangers to both pets, who might either escape, and to the delivery driver, who might be attacked. Therefore, some participants mentioned the need for a feature allowing homeowners to communicate specific pet-related instructions to the delivery driver. One of the limitations the participants noticed with the system during the second phase was the absence of indoor monitoring capabilities, leaving homeowners in the dark about the delivery person's actions once access to the home is granted. This reveals a crucial insight when it comes to setting up smart home automation scenarios that include the smart lock which is the fact that homeowners need to retain control and awareness even after the door has been unlocked.

Inside the House. During the third phase, a significant concern among participants was related to delivery zone definition and awareness. There was a concern that while the delivery zone is known to the system and the homeowner, the driver might not be aware of it. This raises an issue related to creating such automation scenarios which is the discrepancy between what the automation actually does, and what the human beings who interact with the automation expects it to do. This increases the possibility of the delivery driver inadvertently going beyond the delivery zone and triggering false security alerts because they are not aware of what the automation expects them to do or not do. Similarly, the drivers might need to briefly step beyond the delivery zone to deliver a larger package, but the system doesn't account for such instances and will treat it as a security breach. Therefore, there is a need for a two-way communication approach with the driver or the ability to leave them pre-recorded voice messages to guide them through the delivery area. Furthermore, there was a call for giving users the ability to customize the delivery zone. For example, allowing homeowners the flexibility to define dual zones, a primary and an extended one. The system would not sound the siren or notify the homeowner if the delivery driver only crossed into the extended zone and only alert the driver through a voice message. However, if the driver ventures beyond the outer limit, it will be treated as a security breach. Also during this phase, some participants expressed concerns associated with the door not re-locking post-delivery. Even though the system instructs the driver to close the door before leaving so it can automatically lock itself, participants considered situations where the driver might neglect or not hear those instructions. Those participants suggested setting up the system in a way that guarantees the door is locked post-delivery or at least alert the homeowner and the delivery company that the door was left unlocked.

Notifications. In the context of enhancing notification configurations for such automation scenarios, our findings reveal a distinct preference among participants for customizable notification options that prioritize safety and effective communication. Participants expressed the need for providing an option to alert authorities when drivers exit the delivery zone further into the house. Moreover, there was a strong inclination towards diverse notification channels, such as phone calls, emails, and continuous vibration, to ensure timely and effective alert dissemination, especially in security-sensitive situations. There was also a demand for selective notification preferences in order to allow homeowners to tailor alerts for specific events and designate priority for critical security notifications. This emphasizes the importance of flexibility and personalization in the notification systems for such automation scenarios. The study also quantitatively confirmed the high value participants place on receiving immediate and detailed alerts during all stages of the delivery process, particularly for security-related incidents.

Trust and Complexity. Our findings revealed that as more devices and conditions are added to an automation scenario that involves the smart lock, the user's trust in the automation increases alongside complexity of setting up that scenario. Starting from a basic automation setup involving face recognition and QR code scanning, which established baseline trust and complexity ratings, the incremental introduction of advanced features such as temporal and location constraints, security camera oversight, and sophisticated security responses progressively increased both trust and perceived complexity among participants. This positive correlation emphasizes the necessity for a balanced approach in the design of such automation scenarios. Improvements in applications design are needed to enable the integration of advanced security measures to improve trust, while ensuring the complexity remains accessible, especially to the less technologically adept.

6.5 Limitations

While providing valuable insights into user perceptions of the limitations, concerns, and expected configurations associated with setting up smart lock automation scenarios that involve other smart home devices, this study still has two main limitations. First, the study's reliance on video demonstrations may not fully capture the complexity and variability of real-world interactions with smart home automation. Participants' responses could be influenced by their imagination or interpretation of the presented scenarios, rather than actual experience or usage. This might limit the depth of insights regarding user-controlled settings, security, and privacy concerns. Second, the study was conducted with a relatively small sample size of 30 participants. While this number allows for in-depth analysis of individual responses, it may not adequately represent the diversity of potential users of smart home automation systems. Different demographics, cultural backgrounds, and levels of technological proficiency could affect perceptions and concerns regarding such smart lock automation scenarios.

6.6 Conclusion

In automation scenarios that involve granting access to the house, the smart lock is usually responsible for granting that access. However, the act of checking whether the access should be granted or not, and how to account for security issues once the door is unlocked are the responsibility of the other devices included in the scenario. Therefore, in this study, we aimed to explore the end users' perceptions of the limitations of such automation scenarios as well as the level of configuration needed to make them more robust and secure. Through a detailed examination of the feedback of 30 participants on a series of automation scenarios, this study highlights the critical importance of robust security measures, reliable technological performance, and flexible user-centric configuration options in improving user trust and acceptance of such automation systems. Moreover, the study reveals a need for enhanced security features, including multi-factor authentication, manual overrides, and customizable notifications, to mitigate concerns related to unauthorized access, system hacking, and the safety of pets and property. The study also points to a positive correlation between the perceived complexity of an automation scenario and the level of trust users place in it. While users are willing to engage with more complex systems for increased security, there remains a delicate balance to be struck to avoid overwhelming users or compromising usability. In conclusion, while the potential of smart lock automation in enhancing home security and convenience is evident, there is a need to study user concerns and address these through improving the technology and giving the user more control over how to configure these scenarios.

CHAPTER 7: CONCLUSION, DESIGN GUIDELINES, AND FUTURE WORK

7.1 Conclusion, Design Guidelines, and Future Work

7.1.1 Conclusion

The overarching goal of this dissertation was to explore the usability, security, and privacy of smart locks from the perspective of the end user. To achieve this, we conducted a series of user studies that aimed to explore these aspects of the smart lock both when it's used on its own, as well as when it's used as a part of an automation scenario within the smart home environment. First, we started by exploring the end user's perceptions of the usability, security, and privacy of smart locks based on its basic functionality as well as additional features. According to our first study, one of the most frequently used and appreciated features of smart locks was their ability to connect to the internet and being remotely controlled. Therefore, we conducted our second study which aimed to compare two of the most commonly used smart lock provisioning approaches in order to identify the shortcomings of each of the two approaches when used to provision the smart lock, from the end user's perspective. Smart locks can also communicate with other smart devices around the house giving their users the ability to include them in various smart home automation scenarios. Our third study aimed to explore smart locks users' perceptions, motivations, and needs when it comes to creating such smart home automation scenarios that involve the smart lock. The findings of this study showed that even though the unlocking of the door is done through the smart lock when it's included in a smart home automation scenario, most of the configurations and safeguards take place on the other smart home devices included in the automation scenario. Therefore, our fourth and final study focused on exploring the end users' perceptions, requirements, and concerns associated with setting up smart lock automation scenarios that also involve other smart home devices.

Our findings from Chapter 3 showed that smart locks users are generally aware of some of the common security and privacy concerns such as hacking and sharing their personal information with other users. However, there was less awareness about privacy and security concerns specifically related to smart locks such as the log evasion and revocation evasion issues. Despite security concerns, including vulnerabilities smart lock users have, such as shoulder surfing attacks and the risk of losing smartphones, users perceived the benefits of convenience to outweigh potential security risks. The participants' preference for smart locks largely stemmed from the convenience they offer, such as keyless entry and remote access, over traditional locks. According to our findings, trust plays a crucial role in users' attitudes towards smart lock security. Some participants displayed a high level of trust in the lock's other users, the manufacturer, or the installing security company, sometimes to the extent of neglecting basic security practices like checking access logs. Previous studies have indicated that users of smart home devices commonly have varying degrees of concern regarding issues like hacking [35] and excessive data gathering [97]. Our research validated these concerns in the context of smart locks but also identified some issues that are more unique to smart locks. Specifically, we found that the possibility of shoulder surfing attacks can be a big concern for some users. Additionally, there were also concerns regarding the visible wear and tear on the lock's keypad potentially revealing frequently used numbers, which may help attackers guess the correct access code. Similarly, our work has uncovered mitigation strategies end users implement to deal with their security and privacy concerns that are more specific to smart locks. For example, installing a video doorbell next to the smart lock emerged as one of the most popular forms of mitigation as they provide the user with a clear view of events taking place around the lock. Prior work in the field of Wi-Fi provisioning for smart home devices has mostly focused on exploring their security [31, 86] and scalability [15]. However, our work in Chapter 4 aimed to investigate end users perceptions regarding two widely used provisioning approaches, BLE and SoftAP, in the context of provisioning smart locks. Our findings revealed that when it comes to provisioning smart locks, BLE generally outperforms SoftAP in usability, learning curve, efficiency, and reliability. The study identified increased user frustration with SoftAP due to the complexity of switching between Wi-Fi networks and the cumbersome process of navigating between the provisioning app and Wi-Fi settings screen. Despite occasional issues with BLE device pairing, its all-in-app process was found to be more user-friendly. Security concerns between the two methods were similar among the participants. However, some of the participants expressed a preference for SoftAP due to perceived security benefits. Earlier studies [18, 16, 21] have shown that enhancing the security, convenience, and awareness levels within the smart home are key drivers behind creating smart home automation scenarios. Our findings from Chapter 5 confirmed those motivations for creating automation scenarios that specifically include the smart lock. Furthermore, it also uncovered other motivations that are more associated with smart lock automations such as improving the physical safety of house residents and automating the process of managing physical access to the house. The study also revealed some concerns that end users may have in relation to creating automation scenarios which include the smart lock. These concerns include reliability issues, false alarms, and human errors. Additionally, there was a fear among some participants that automation scenarios created to improve convenience or automate access management could possibly lead to physical unauthorized access to the house especially in the case of a false positive. Furthermore, we found a shared concern regarding false positives and false negatives among all automation scenarios. There was greater concern about false negatives for automation scenarios related to safety, security, and privacy. On the other hand, there was more of a concern regarding false negatives in scenarios that aimed to improve convenience and access management. Even though the results from Chapter 3 showed a general lack of concern regarding security issues associated with smart locks, the findings from Chapter 5 revealed that end users are more concerned about such issues when automation is involved. The reason behind this discrepancy could be related to the end user's concerns about the lack of reliability associated with the other smart home devices involved in the automation scenarios. Previous work [79] has referred to this issue as "integrity violation" which is when one device takes action based on information received from a less trusted/reliable device. Our findings from Chapter 6 revealed that adding more triggers and smart home devices to a smart lock automation scenario increases users' trust in that scenario but also increases the complexity of setting it up. Adding other smart home devices to the smart lock automation scenario allows users to verify the identity of individuals for whom the door is unlocked. In addition, it also allows users to control and monitor what happens once the door is unlocked. Similar to Chapter 5, some participants expressed concerns regarding the reliability of the devices involved in the automation scenario such as the video doorbell or the security camera. However, the findings from Chapter 6 showed that giving end users more options to configure those devices can help mitigate their concerns. For example, the ability to add other factors of authentication can alleviate the concerns related to the reliability of facial recognition through the video doorbell. In order to control what happens when the door is unlocked, users need to create a second automation scenario that is triggered only when the first automation scenario (unlocking the door) is executed. This is called a chained automation scenario. One limitation of such automation scenarios is the fact that one of the devices in the second automation scenario might not be available for any reason. This compromises the security of the house. The majority of our participants did not wish for the first automation to execute if the second scenario cannot be triggered. However, other participants still wanted the first scenario to execute in some cases such as when it's a trusted person ringing the video doorbell, or an expensive package is being delivered. The ability to receive notifications regarding each step of the process in such automation scenarios was considered the most critical security control for end users to alleviate their security concerns. While receiving a push notification was optimal in most cases, some participants also wanted the option to get notified through a phone call in case of a possible security breach.

7.1.2 Design Guidelines

Based on the different lessons learned throughout this dissertation, we provide specific design guidelines to help manufacturers improve smart lock end user's experience.

Enhanced security measures:

- Integrate fingerprint scanners or facial recognition technology to provide a more secure and personalized method of authentication. This can significantly reduce the risk of unauthorized access due to stolen codes or keys. Biometric data, being unique to each individual, adds a layer of security that is difficult to replicate or bypass.

- Give users the option to require two or more verification factors to gain access. This could include a combination of something the user knows (a PIN), something the user has (a smartphone or key fob), and something the user is (biometric verification). MFA addresses the limitations of single-factor authentication by adding additional layers of security, making it considerably harder for unauthorized individuals to gain access. This is especially important when the smart lock is incorporated in smart home automation scenarios where the need for a stronger authentication process is crucial.

Physical Security Upgrades:

- Implement sensors that detect tampering or forced entry attempts on the lock. This could include detecting lock picking, physical damage, or any attempts to remove the smart lock from the door. Upon detection, the system should alert the homeowner immediately through their mobile application.

- Design smart locks with robust materials that resist physical attacks. This includes making the lock body and components from strong metals and applying finishes that are resistant to drilling, cutting, and prying. Ensuring the lock's physical integrity is vital in preventing burglars from bypassing the smart features by attacking the lock itself.

Transparent Data Practices:

- Clearly communicate what data is collected, how it is used, and who it is shared with. This transparency builds trust with users and allows them to make informed decisions about their privacy.

- Provide users with control over their data, including the ability to view, edit, and delete their data. Additionally, offer options to opt-out of data sharing with third parties, ensuring users have full control over their privacy.

User Education Programs:

- Develop comprehensive tutorials and guides that inform users about potential security threats, such as hacking or social engineering attacks, and how to mitigate them. This could be integrated into the smart lock app as interactive tutorials or sent to users as periodic security tips.

- Offer guidance on managing access controls effectively, creating strong passwords, and the importance of regularly updating the lock's firmware to protect against vulnerabilities. Educating users on these best practices can significantly enhance the security ecosystem of smart homes.

- Offer resources to educate users about how automation scenarios work, potential security implications, and best practices for creating secure and effective automations.

Granular Access Controls:

- Allow users to set conditions under which access is granted, such as time-based access for guests or service providers. This feature can also include environmental conditions, such as allowing access only when no one is detected in the home, adding a layer of privacy protection.

Improve the provisioning process:

- For SoftAP, streamline the process of switching networks and returning to the app to reduce confusion and the likelihood of errors. For BLE, enhance device discovery and connection stability to minimize pairing issues.
- Leverage various instructional mediums (videos, audio, interactive images) within the companion app to provide clear, comprehensive guidance, especially for processes that users find complex or unintuitive.

Improve smart locks automation:

- Ensure that smart locks can easily integrate with a wide range of smart home devices and platforms, allowing users to create automation scenarios that improve the overall levels of security, awareness, and convenience within the house. For example, a smart lock could automatically activate the home's security cameras when locked from the outside.

- Allow users to create automation scenarios with flexible conditions and actions, catering to a wide range of needs and preferences. Offer templates for common scenarios while also supporting customization.

- Incorporate immediate feedback mechanisms to show users the potential impact of their automation scenarios before they are saved and activated.

- Take into consideration the human beings involved in the automation scenarios and offer ways to provide them clear instructions about what is considered as a security breach by the automation scenario.

- Facilitate simpler and more transparent methods of creating chained automation scenarios. This should include explaining the dependencies between the automation scenarios to the end user and how the system would behave if one of the devices in a chained automation scenario is not available. Our findings show that more secure smart lock automation scenarios account for the three stages of unlocking the door (pre-unlocking, once unlocked, and inside the house while the door is unlocked). Therefore, a way of simplifying the creation of smart lock automation scenarios is to provide the user with a template that covers all three phases. The user in this case has to choose the triggers and actions within each phase.

- Allow users to design automation scenarios that provide convenience without compromising security, such as granting access based on time of day, location, or presence of residents, with fallbacks for manual verification when needed.
- Allow users to customize the trade-off between security and convenience according to their preferences and risk tolerance, with clear guidance on the implications of their choices.
- Develop a nuanced notification system that offers real-time, step-by-step updates throughout the automation process, customizable according to user preferences and criticality of the automation steps to ensure that users remain informed and in control at all times.

7.1.3 Future Work

Our work uncovered several limitations and concerns related to smart locks and their integration with other smart home devices. However, future research needs to focus on proposing solutions to overcome some of these limitations. For example, we found that once the battery of smart locks starts depleting, the motor responsible for automatic re-locking starts getting weaker which can be a huge security issue potentially leading to unauthorized access. More work needs to be done to test different solutions for this issue such as proposing ways to improve the battery life or requiring the user to replace the batteries before they start affecting the motor. It is also imperative to further investigate user interface (UI) and user experience (UX) design improvements that simplify the process of provisioning smart locks and managing smart home automation scenarios. Specifically, addressing the complexity and user frustration associated with the SoftAP provisioning method by exploring alternative approaches that offer both security and ease of use. Furthermore, our findings revealed that adding more conditions and devices to an automation scenario that includes the smart lock increases the level of trust in that scenario. However, it also increases the complexity of setting it up. Thus, future research should focus on simplifying the creation of these automation scenarios, making them more user-friendly and less complicated.

REFERENCES

[1] August smart locks privacy policy — keeping your home & data locked down. https://august.com/pages/privacy-policyproduct. Accessed: 2023-04-26.

[2] IFTTT - Home Security Applets. https://ifttt.com/search/query/home20security. Accessed: 2023-05-03.

[3] Zapier - Automation that moves you forward. https://zapier.com/. Accessed: 2023-05-03.

[4] Wi-fi onboarding technologies for connected products. https://www.ashb.com/wp-content/uploads/2020/04/IS-2019-110.pdf, 2019. Accessed: 2023-05-24.

[5] August Smart Lock - 3rd Generation. https://august.com/products/august-smart-lock-3rd-generation, 2023. Accessed: 2023-05-03.

[6] ESP32 - ESP-IDF Programming Guide. https://docs.espressif.com/projects/esp-idf/en/latest/esp32/get-started/, 2023. Accessed: 2023-05-03.

[7] N. M. Allifah and I. A. Zualkernan. Ranking security of iot-based smart home consumer devices. *Ieee Access*, 10:18352–18369, 2022.

[8] D. C. Aluri. Smart lock systems: An overview. *International Journal of Computer Applications*, 177(37):40–43, 2020.

[9] M. Amiribesheli and A. Bouchachia. Smart homes design for people with dementia. In *2015 International Conference on Intelligent Environments*, pages 156–159. IEEE, 2015.

[10] S. P. R. Asaithambi, S. Venkatraman, and R. Venkatraman. Big data and personalisation for non-intrusive smart home automation. *Big Data and Cognitive Computing*, 5(1):6, 2021.

[11] A. Bangor, P. Kortum, and J. Miller. Determining what individual sus scores mean: Adding an adjective rating scale. *Journal of usability studies*, 4(3):114–123, 2009.

[12] A. Bangor, P. T. Kortum, and J. T. Miller. An empirical evaluation of the system usability scale. *Intl. Journal of Human–Computer Interaction*, 24(6):574–594, 2008.

[13] C. Bapat, G. Baleri, S. Inamdar, and A. V. Nimkar. Smart-lock security re-engineered using cryptography and steganography. In *International Symposium on Security in Computing and Communication*, pages 325–336. Springer, 2017.

[14] S. BJARTMAR HYLTA and P. SÖDERBERG. Smart locks for smart customers?: A study of the diffusion of smart locks in an urban area, 2017.

[15] I. Boškov, H. Yetgin, M. Vučnik, C. Fortuna, and M. Mohorčič. Time-to-provision evaluation of iot devices using automated zero-touch provisioning. In *GLOBECOM 2020-2020 IEEE Global Communications Conference*, pages 1–7. Ieee, 2020.

[16] J. Brich, M. Walch, M. Rietzler, M. Weber, and F. Schaub. Exploring end user programming needs in home automation. *ACM Transactions on Computer-Human Interaction (TOCHI)*, 24(2):1–35, 2017.

[17] J. Brooke et al. Sus-a quick and dirty usability scale. *Usability evaluation in industry*, 189(194):4–7, 1996.

[18] A. B. Brush, B. Lee, R. Mahajan, S. Agarwal, S. Saroiu, and C. Dixon. Home automation in the wild: challenges and opportunities. In *proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 2115–2124, 2011.

[19] G. Chalhoub and I. Flechais. "alexa, are you spying on me?": Exploring the effect of user experience on the security and privacy of smart speaker users. In *HCI for Cybersecurity, Privacy and Trust: Second International Conference, HCI-CPT 2020, Held as Part of the 22nd HCI International Conference, HCII 2020, Copenhagen, Denmark, July 19–24, 2020, Proceedings 22*, pages 305–325. Springer, 2020.

[20] C. Chhetri. *Designing for Privacy in Smart Home Devices*. PhD thesis, George Mason University, 2022.

[21] Y.-S. Chiang, R.-C. Chang, Y.-L. Chuang, S.-Y. Chou, H.-P. Lee, I.-J. Lin, J.-H. Jiang Chen, and Y.-J. Chang. Exploring the design space of user-system communication for smart-home routine assistants. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, pages 1–14, 2020.

[22] E. Cho, S. S. Sundar, S. Abdullah, and N. Motalebi. Will deleting history make alexa more trustworthy? effects of privacy and content customization on user experience of smart speakers. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, pages 1–13, 2020.

[23] J. Choi, J. Hur, and S. Bahk. Push your password: Secure and fast wifi connection for iot devices. In *2021 IEEE Wireless Communications and Networking Conference (WCNC)*, pages 1–6. IEEE, 2021.

[24] F. Corno, L. De Russis, and A. Monge Roffarello. How do end-users program the internet of things? *Behaviour & Information Technology*, 41(9):1865–1887, 2022.

[25] A. Coskun, G. Kaner, and İ. Bostan. Is smart home a necessity or a fantasy for the mainstream user? a study on users' expectations of smart household appliances. *International Journal of Design*, 12(1):7–20, 2018.

[26] L. de Camargo Silva, M. Samaniego, and R. Deters. Iot and blockchain for smart locks. In *2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, pages 0262–0269. IEEE, 2019.

[27] A. K. Dey, T. Sohn, S. Streng, and J. Kodama. icap: Interactive prototyping of context-aware applications. In *Pervasive Computing: 4th International Conference, PERVASIVE 2006, Dublin, Ireland, May 7-10, 2006. Proceedings 4*, pages 254–271. Springer, 2006.

[28] C. Geeng and F. Roesner. Who's in control? interactions in multi-user smart homes. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, pages 1–13, 2019.

[29] M. R. Ghori, T.-C. Wan, and G. C. Sodhy. Bluetooth low energy mesh networks: Survey of communication and security protocols. *Sensors*, 20(12):3590, 2020.

[30] C. Glaser and A. P. Alvarez. Extending battery life in smart e-locks.

[31] D. Granata, M. Rak, G. Salzillo, U. Barbato, et al. Security in iot pairing & authentication protocols, a threat model, a case study analysis. In *ITASEC*, pages 207–218, 2021.

[32] Y. B. Hamdan et al. Smart home environment future challenges and issues-a survey. *Journal of Electronics*, 3(01):239–246, 2021.

[33] J. Haney, S. M. Furman, M. Theofanos, Y. A. Fahl, et al. Perceptions of smart home privacy and security responsibility, concerns, and mitigations. 2019.

[34] J. M. Haney, Y. Acar, and S. Furman. " it's the company, the government, you and i": User perceptions of responsibility for smart home privacy and security. In *USENIX Security Symposium*, pages 411–428, 2021.

[35] J. M. Haney, S. M. Furman, and Y. Acar. Smart home security and privacy mitigations: Consumer perceptions, practices, and challenges. In *International Conference on Human-Computer Interaction*, pages 393–411. Springer, 2020.

[36] H. Hazazi and M. Shehab. Exploring the usability, security, and privacy of smart locks from the perspective of the end user. In *Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023)*, pages 559–577, 2023.

[37] 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 *USENIX Security Symposium*, pages 255–272, 2018.

[38] W. He, J. Martinez, R. Padhi, L. Zhang, and B. Ur. When smart devices are stupid: negative experiences using home smart devices. In *2019 IEEE Security and Privacy Workshops (SPW)*, pages 150–155. IEEE, 2019.

[39] R. Heartfield, G. Loukas, S. Budimir, A. Bezemskij, J. R. Fontaine, A. Filippoupolitis, and E. Roesch. A taxonomy of cyber-physical threats and impact in the smart home. *Computers & Security*, 78:398–428, 2018.

[40] G. Ho, D. Leung, P. Mishra, A. Hosseini, D. Song, and D. Wagner. Smart locks: Lessons for securing commodity internet of things devices. In *Proceedings of the 11th ACM on Asia conference on computer and communications security*, pages 461–472, 2016.

[41] K.-H. Hsu, Y.-H. Chiang, and H.-C. Hsiao. Safechain: Securing trigger-action programming from attack chains. *IEEE Transactions on Information Forensics and Security*, 14(10):2607–2622, 2019.

[42] Y. Huang, B. Obada-Obieh, and K. Beznosov. Amazon vs. my brother: How users of shared smart speakers perceive and cope with privacy risks. In *Proceedings of the 2020 CHI conference on human factors in computing systems*, pages 1–13, 2020.

[43] W. A. Jabbar, T. K. Kian, R. M. Ramli, S. N. Zubir, N. S. Zamrizaman, M. Balfaqih, V. Shepelev, and S. Alharbi. Design and fabrication of smart home with internet of things enabled automation system. *IEEE access*, 7:144059–144074, 2019.

[44] S. Jahnavi and C. Nandini. Smart anti-theft door locking system. In *2019 1st International Conference on Advanced Technologies in Intelligent Control, Environment, Computing & Communication Engineering (ICATIECE)*, pages 205–208. IEEE, 2019.

[45] K. J. Kaaz, A. Hoffer, M. Saeidi, A. Sarma, and R. B. Bobba. Understanding user perceptions of privacy, and configuration challenges in home automation. In *2017 IEEE Symposium on Visual Languages and Human-Centric Computing (VL/HCC)*, pages 297–301. IEEE, 2017.

[46] J. S. Kumar and D. R. Patel. A survey on internet of things: Security and privacy issues. *International Journal of Computer Applications*, 90(11), 2014.

[47] F. Laricchia. Global smart lock market size 2016-2027, Feb 2022.

[48] J. Lau, B. Zimmerman, and F. Schaub. Alexa, are you listening? privacy perceptions, concerns and privacy-seeking behaviors with smart speakers. *Proceedings of the ACM on human-computer interaction*, 2(CSCW):1–31, 2018.

[49] C. Li, Q. Cai, J. Li, H. Liu, Y. Zhang, D. Gu, and Y. Yu. Passwords in the air: Harvesting wi-fi credentials from smartcfg provisioning. In *Proceedings of the*

11th ACM Conference on Security & Privacy in Wireless and Mobile Networks, pages 1–11, 2018.

[50] H. Lin and N. W. Bergmann. Iot privacy and security challenges for smart home environments. *Information*, 7(3):44, 2016.

[51] H. Liu, C. Li, X. Jin, J. Li, Y. Zhang, and D. Gu. Smart solution, poor protection: An empirical study of security and privacy issues in developing and deploying smart home devices. In *Proceedings of the 2017 Workshop on Internet of Things security and privacy*, pages 13–18, 2017.

[52] H. Liu, J. Li, and D. Gu. Understanding the security of app-in-the-middle iot. *Computers & Security*, 97:102000, 2020.

[53] Y. Liu, K. Hao, J. Zhao, L. Wang, and W. Zhang. A novel smart lock protocol based on group signature. *International Journal of Network Security*, 24(1):130–139, 2022.

[54] A. M. Lonzetta, P. Cope, J. Campbell, B. J. Mohd, and T. Hayajneh. Security vulnerabilities in bluetooth technology as used in iot. *Journal of Sensor and Actuator Networks*, 7(3):28, 2018.

[55] J.-N. Louis, A. Calo, K. Leiviskä, and E. Pongrácz. Environmental impacts and benefits of smart home automation: Life cycle assessment of home energy management system. *IFAC-PapersOnLine*, 48(1):880–885, 2015.

[56] N. Malkin, J. Deatrick, A. Tong, P. Wijesekera, S. Egelman, and D. Wagner. Privacy attitudes of smart speaker users. *Proceedings on Privacy Enhancing Technologies*, 2019(4), 2019.

[57] S. Mamonov and R. Benbunan-Fich. Unlocking the smart home: exploring key factors affecting the smart lock adoption intention. *Information Technology & People*, 34(2):835–861, 2020.

[58] S. Mare, L. Girvin, F. Roesner, and T. Kohno. Consumer smart homes: Where we are and where we need to go. In *Proceedings of the 20th International Workshop on Mobile Computing Systems and Applications*, pages 117–122, 2019.

[59] A. Mattioli and F. Paternò. Understanding user needs in smart homes and how to fulfil them. In *International Symposium on End User Development*, pages 125–142. Springer, 2023.

[60] M. H. Mazhar. *Improving the Safety of IoT Systems With Usable Policy Enforcement.* PhD thesis, The University of Iowa, 2023.

[61] V. Michal. Bezpečnost iot zařízení na platformě esp32. Master's thesis, České vysoké učení technické v Praze. Vypočetní a informační centrum., 2020.

[62] P. Moh, P. Datta, N. Warford, A. Bates, N. Malkin, and M. L. Mazurek. Characterizing everyday misuse of smart home devices. In *2023 IEEE Symposium on Security and Privacy (SP)*, pages 2835–2849. IEEE, 2023.

[63] L. Nemec Zlatolas, N. Feher, and M. Hölbl. Security perception of iot devices in smart homes. *Journal of Cybersecurity and Privacy*, 2(1):65–73, 2022.

[64] S. Nikou. Factors driving the adoption of smart home technology: An empirical assessment. *Telematics and Informatics*, 45:101283, 2019.

[65] L. Oliveira, A. May, V. Mitchell, M. Coleman, T. Kane, and S. Firth. Pre-installation challenges: classifying barriers to the introduction of smart home technology. 2015.

[66] D. Pal, S. Funilkul, V. Vanijja, and B. Papasratorn. Analyzing the elderly users' adoption of smart-home services. *IEEE access*, 6:51238–51252, 2018.

[67] S. Palle. *Smart Locks: Exploring Security Breaches and Access Extensions*. PhD thesis, Oklahoma State University, 2017.

[68] V. Pandit, P. Majgaonkar, P. Meher, S. Sapaliga, and S. Bojewar. Intelligent security lock. In *2017 international conference on trends in electronics and informatics (ICEI)*, pages 713–716. IEEE, 2017.

[69] B. Patil, P. Vyas, and R. Shyamasundar. Secsmartlock: An architecture and protocol for designing secure smart locks. In *International Conference on Information Systems Security*, pages 24–43. Springer, 2018.

[70] S. J. Philip, T. J. Luu, and T. Carte. There's no place like home: Understanding users' intentions toward securing internet-of-things (iot) smart home networks. *Computers in Human Behavior*, 139:107551, 2023.

[71] S. Pradeep, T. Kousalya, K. A. Suresh, and J. Edwin. Iot and its connectivity challenges in smart home. *International Research Journal of Engineering and Technology*, 3(12):1040–1043, 2016.

[72] R. Reda, A. Carbonaro, V. de Boer, R. Siebes, R. van der Weerdt, B. Nouwt, and L. Daniele. Supporting smart home scenarios using owl and swrl rules. *Sensors*, 22(11):4131, 2022.

[73] G. Reiter. A primer to wi-fi® provisioning for iot applications. *Texas Instruments White Paper*, 2014.

[74] À. Rodríguez Navas. Design and implementation of a secure standalone 433mhz rf iot gateway. B.S. thesis, Universitat Politècnica de Catalunya, 2023.

[75] M. Ryan. Bluetooth: With low energy comes low security. In *7th {USENIX} Workshop on Offensive Technologies ({WOOT} 13)*, 2013.

[76] M. Sági, D. Mijic, D. Milinkov, and B. Bogovac. Smart home automation. In *2012 20th Telecommunications Forum (TELFOR)*, pages 1512–1515. IEEE, 2012.

[77] J. Sauro and J. S. Dumas. Comparison of three one-question, post-task usability questionnaires. In *Proceedings of the SIGCHI conference on human factors in computing systems*, pages 1599–1608, 2009.

[78] D. Soares, J. P. Dias, A. Restivo, and H. S. Ferreira. Programming iot-spaces: A user-survey on home automation rules. In *Computational Science–ICCS 2021: 21st International Conference, Krakow, Poland, June 16–18, 2021, Proceedings, Part IV*, pages 512–525. Springer, 2021.

[79] M. Surbatovich, J. Aljuraidan, L. Bauer, A. Das, and L. Jia. Some recipes can do more than spoil your appetite: Analyzing the security and privacy risks of ifttt recipes. In *Proceedings of the 26th International Conference on World Wide Web*, pages 1501–1510, 2017.

[80] M. Tabassum, T. Kosinski, and H. R. Lipford. " i don't own the data": End user perceptions of smart home device data practices and risks. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*, pages 435–450, 2019.

[81] M. Tabassum and H. Lipford. Exploring privacy implications of awareness and control mechanisms in smart home devices. *Proceedings on Privacy Enhancing Technologies*, 1:571–588, 2023.

[82] O. Taiwo, L. A. Gabralla, and A. E. Ezugwu. Smart home automation: taxonomy, composition, challenges and future direction. In *Computational Science and Its Applications–ICCSA 2020: 20th International Conference, Cagliari, Italy, July 1–4, 2020, Proceedings, Part VI 20*, pages 878–894. Springer, 2020.

[83] H. Touqeer, S. Zaman, R. Amin, M. Hussain, F. Al-Turjman, and M. Bilal. Smart home security: challenges, issues and solutions at different iot layers. *The Journal of Supercomputing*, 77(12):14053–14089, 2021.

[84] B. Ur, J. Jung, and S. Schechter. Intruders versus intrusiveness: teens' and parents' perspectives on home-entryway surveillance. In *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, pages 129–139, 2014.

[85] B. Ur, E. McManus, M. Pak Yong Ho, and M. L. Littman. Practical trigger-action programming in the smart home. In *Proceedings of the SIGCHI conference on human factors in computing systems*, pages 803–812, 2014.

[86] J. Valente and A. A. Cardenas. Security & privacy in smart toys. In *Proceedings of the 2017 Workshop on Internet of Things Security and Privacy*, pages 19–24, 2017.

[87] A. Viderberg. Security evaluation of smart door locks, 2019.

[88] Q. Wang, P. Datta, W. Yang, S. Liu, A. Bates, and C. A. Gunter. Charting the attack surface of trigger-action iot platforms. In *Proceedings of the 2019 ACM SIGSAC conference on computer and communications security*, pages 1439–1453, 2019.

[89] X. Wang, Y. Sun, S. Nanda, and X. Wang. Looking from the mirror: Evaluating iot device security through mobile companion apps. In *USENIX Security Symposium*, pages 1151–1167, 2019.

[90] Z. Xin, L. Liu, and G. Hancke. Aacs: Attribute-based access control mechanism for smart locks. *Symmetry*, 12(6):1050, 2020.

[91] J. Yang. *Eden: An Interactive Home Network Management System*. Georgia Institute of Technology, 2009.

[92] J. Yang and W. K. Edwards. Icebox: Toward easy-to-use home networking. In *Human-Computer Interaction–INTERACT 2007: 11th IFIP TC 13 International Conference, Rio de Janeiro, Brazil, September 10-14, 2007, Proceedings, Part II 11*, pages 197–210. Springer Berlin Heidelberg, 2007.

[93] R. Yang and M. W. Newman. Learning from a learning thermostat: lessons for intelligent systems for the home. In *Proceedings of the 2013 ACM international joint conference on Pervasive and ubiquitous computing*, pages 93–102, 2013.

[94] Y. Yao, J. R. Basdeo, S. Kaushik, and Y. Wang. Defending my castle: A co-design study of privacy mechanisms for smart homes. In *Proceedings of the 2019 chi conference on human factors in computing systems*, pages 1–12, 2019.

[95] S. Yarosh and P. Zave. Locked or not? mental models of iot feature interaction. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, pages 2993–2997, 2017.

[96] M. Ye, N. Jiang, H. Yang, and Q. Yan. Security analysis of internet-of-things: A case study of august smart lock. In *2017 IEEE conference on computer communications workshops (INFOCOM WKSHPS)*, pages 499–504. IEEE, 2017.

[97] E. Zeng, S. Mare, and F. Roesner. End user security and privacy concerns with smart homes. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, pages 65–80, 2017.

[98] E. Zeng and F. Roesner. Understanding and improving security and privacy in {Multi-User} smart homes: A design exploration and {In-Home} user study. In *28th USENIX Security Symposium (USENIX Security 19)*, pages 159–176, 2019.

[99] S. Zheng, N. Apthorpe, M. Chetty, and N. Feamster. User perceptions of smart home iot privacy. *Proceedings of the ACM on human-computer interaction*, 2(CSCW):1–20, 2018.

[100] W. Zhou, C. Cao, D. Huo, K. Cheng, L. Zhang, L. Guan, T. Liu, Y. Jia, Y. Zheng, Y. Zhang, et al. Reviewing iot security via logic bugs in iot platforms and systems. *IEEE Internet of Things Journal*, 8(14):11621–11639, 2021.

[101] W. Zhou, C. Cao, D. Huo, K. Cheng, L. Zhang, L. Guan, T. Liu, Y. Zheng, Y. Zhang, L. Sun, et al. Logic bugs in iot platforms and systems: A review. *arXiv preprint arXiv:1912.13410*, 2019.

APPENDIX A: Supplementary data for Chapter 3

Screening Survey

- What is your first name?
- What is your email address?
- What age group do you belong to?
- What is your gender?
- What is your level of education?
- What is your current occupation?
- How many smart locks do you have installed where you live?
- Which smart lock(s) do you have installed where you live?
- Who installed the lock(s)?
- How long have you been using it (them)?
- How does your smart lock connect to the internet?
- How many people do you share access to the lock(s) with?
- Which virtual meeting platform do you prefer for conducting the interview?

Interview Questions

Smart Locks Usability

- What made you move from using a traditional lock to using a smart lock?

- Did you hesitate before making the move from using traditional locks to smart locks? Why?

- Do you have your smart lock connected to your video doorbell? Why?

- What would you say the top features of your smart lock that you mostly use?

- Who else can operate the smart lock, and what are their access levels?

- How easy do you find it to share keys with others? And how reliable?

- How easy do you find it to revoke other people's keys? And how reliable?

- Do you have notifications turned on for your smart lock app? Why?

- Do you connect your smart lock to other smart devices in your home using services like IFTTT? If yes, please talk more about the scenarios you have set up?

- Which aspects of the smart lock do you dislike or wish they would have been implemented differently?

- Compared to a traditional lock, how do you rate the locking/unlocking experience using a smart lock?

- In terms of locking/unlocking the door, how reliable is the smart lock compared to a traditional lock?

- How often do you find yourself checking the smart lock app on your phone to see if your door is locked/unlocked? (never, seldom, sometimes, frequently, always)

- How often do you find yourself checking the smart lock app on your phone to see the access logs? (never, seldom, sometimes, frequently, always)
- How often do you use your smart lock's auto lock feature? (never, seldom, sometimes, frequently, always)
- How often do you use your smart lock's auto unlock feature? (never, seldom, sometimes, frequently, always)
- How often do you control your smart lock using voice commands? (never, seldom, sometimes, frequently, always)
- Can you think of more features that you would like smart locks to have?

Privacy and Security Concerns Related to Smart Locks:

- What security or privacy related concerns do you have with your smart lock? How do you mitigate (deal with) those concerns?
- How concerned are you that your smart lock may malfunction and lock you out one day? (not concerned, slightly concerned, concerned, very concerned, extremely concerned)
- Has the smart lock ever locked you out of your home by accident? What was the reason?
- Would having a smart lock installed in your home make you feel safer compared to having a conventional lock? Why?

- How concerned are you that your smart lock might store your personal information and know your location at all times? (not concerned, slightly concerned, concerned, very concerned, extremely concerned)
- How concerned are you that the smart lock will keep a log of every time the lock is used along with the information of the person who used it? (not concerned, slightly concerned, concerned, very concerned, extremely concerned)
- How concerned are you that your smart lock might give others (such as your landlord) information about when you or your family members are home and when you are not? (not concerned, slightly concerned, concerned, very concerned, extremely concerned)
- How concerned are you that data collected by your smart lock might be shared with other parties? (not concerned, slightly concerned, concerned, very concerned, extremely concerned)
- How concerned are you that your smart lock might be hacked which allows unauthorized access to your home? (not concerned, slightly concerned, concerned, very concerned, extremely concerned)
- How concerned are you that the key revocation process might not be working correctly which allows others whose keys you have revoked to still have access to your home? (not concerned, slightly concerned, concerned, very concerned, extremely concerned)
- How concerned are you that some locking/unlocking activities might not appear

on the smart lock's access logs? (not concerned, slightly concerned, concerned, very concerned, extremely concerned)

- What other security or privacy related concerns do you have with your smart lock?
- Do you use any other gadgets/ devices to increase the security of your smart lock?
- Does the app you use to control the smart lock allow you to use multi-factor authentication (MFA)? If yes, what form of MFA does the app offer? and how often do you use it?
- Do you think the companies that manufacture smart locks should add more features to make them more secure and increase the user's privacy? Could you give examples of such features?
- What other concerns do you have in regards to smart locks security and privacy?

Security Awareness

Each question listed below was asked twice, once for the revocation evasion security issue and another time for the log evasion security issue.

- Did you already know that this issue existed?
- On a scale of 1 to 5, how serious do you think this issue is?
- On a scale of 1 to 5, how concerned are you that your smart lock might be affected by this issue?

- Would this issue cause you to go back to using a traditional lock instead of a smart lock?

APPENDIX B: Supplementary data for Chapter 4

Survey Questions

- What is the study ID that was assigned to you?
- What is your age?
- What gender do you identify with?
- What is your highest level of education?
- What is your current occupation?
- Which option do you think most accurately describes your level of experience with setting up smart home devices? (far above average, somewhat above average, average, somewhat below average, far below average).
- Once you have provisioned the device, can you still browse the internet on your smartphone immediately? If not, how did you regain internet access?
- What information do you think is being transmitted between the phone and the lock during the provisioning process using this provisioning approach?
- Why did the app ask you for a proof of possession?
- How do you think this provisioning process can be improved?
- How would you describe the overall experience of provisioning the smart lock using this provisioning approach?

- What did you like the least about the provisioning process using this provisioning approach?

- System Usability Scale (SUS) Questions:

  1. I think that I would like to use this provisioning approach frequently (strongly disagree, somewhat disagree, neither agree nor disagree, somewhat agree, strongly agree).

  2. I found this provisioning approach unnecessarily complex (strongly disagree, somewhat disagree, neither agree nor disagree, somewhat agree, strongly agree).

  3. I thought it was easy to use this provisioning approach (strongly disagree, somewhat disagree, neither agree nor disagree, somewhat agree, strongly agree).

  4. I think that I would need the support of a technical person to be able to use this system (strongly disagree, somewhat disagree, neither agree nor disagree, somewhat agree, strongly agree).

  5. I found the various functions in this system were well integrated (strongly disagree, somewhat disagree, neither agree nor disagree, somewhat agree, strongly agree).

  6. I thought there was too much inconsistency in using this provisioning approach (strongly disagree, somewhat disagree, neither agree nor disagree, somewhat agree, strongly agree).

7. I would imaging that most people would learn to use this provisioning approach very quickly (strongly disagree, somewhat disagree, neither agree nor disagree, somewhat agree, strongly agree).
8. I found the system very cumbersome to use to provision the IoT devices (strongly disagree, somewhat disagree, neither agree nor disagree, somewhat agree, strongly agree).
9. I felt very confident using this provisioning approach (strongly disagree, somewhat disagree, neither agree nor disagree, somewhat agree, strongly agree).
10. I needed to learn a lot of things before I could get going with this system (strongly disagree, somewhat disagree, neither agree nor disagree, somewhat agree, strongly agree).

- This system has all the functions and capabilities I expect it to have (strongly disagree, somewhat disagree, neither agree nor disagree, somewhat agree, strongly agree).

- I thought there were too many steps required to use this provisioning approach (strongly disagree, somewhat disagree, neither agree nor disagree, somewhat agree, strongly agree).

- I can effectively use this approach to provision IoT devices (strongly disagree, somewhat disagree, neither agree nor disagree, somewhat agree, strongly agree).

- I thought the time required to complete the provisioning process was acceptable (strongly disagree, somewhat disagree, neither agree nor disagree, somewhat agree, strongly agree).

- I feel this provisioning approach would affect how other apps on my phone function (strongly disagree, somewhat disagree, neither agree nor disagree, somewhat agree, strongly agree).

- I feel this provisioning approach is secure (strongly disagree, somewhat disagree, neither agree nor disagree, somewhat agree, strongly agree).

- I feel the information transmitted between my phone and the lock during the process is kept secure and private (strongly disagree, somewhat disagree, neither agree nor disagree, somewhat agree, strongly agree).

- Singe Ease Question (SEQ): Overall, I am satisfied with how easy it is to use this system (a scale of 1 to 7, 1 being extremely difficult and 7 extremely easy).

Demographics

Table 11: Participants' demographic information - second study

Participant	Gender	Age group	Education	Experience level in setting up smart home devices
P1	Male	25-34	Advanced degree	Somewhat above average
P2	Female	45-54	Advanced degree	Somewhat above average
P3	Male	18-24	Some college	Somewhat above average
P4	Male	18-24	Some college	Somewhat above average

P5	Male	25-34	College graduate	Far above average
P6	Male	18-24	Some college	Somewhat above average
P7	Male	18-24	Advanced degree	Far above average
P8	Male	18-24	College graduate	Somewhat above average
P9	Male	18-24	Some college	Average
P10	Male	18-24	Some college	Far above average
P11	Female	18-24	Advanced degree	Far above average
P12	Male	18-24	High school	Far above average
P13	Female	45-54	Advanced degree	Somewhat above average
P14	Female	18-24	Some college	Somewhat below average
P15	Female	18-24	Some college	Somewhat below average
P16	Female	18-24	College graduate	Average
P17	Female	25-34	Some college	Somewhat above average
P18	Female	18-24	Some college	Average
P19	Female	35-44	Advanced degree	Average
P20	Female	18-24	High school	Average
P21	Male	25-34	Advanced degree	Far above average
P22	Male	25-34	Advanced degree	Somewhat below average
P23	Female	18-24	Some college	Far below average
P24	Female	18-24	Some college	Average
P25	Female	25-34	College graduate	Somewhat above average
P26	Male	18-24	Some college	Somewhat above average
P27	Female	18-24	Some college	Average

P28	Female	18-24	High school	Average
P29	Female	35-44	Advanced degree	Average
P30	Male	18-24	Some college	Average
P31	Male	25-34	Advanced degree	Somewhat above average
P32	Male	18-24	Some college	Far below average
P33	Male	18-24	Some college	Average
P34	Male	18-24	Some college	Average
P35	Female	18-24	Some college	Average
P36	Male	18-24	High school	Far above average
P37	Male	18-24	Some college	Somewhat below average
P38	Male	35-44	Some college	Far above average
P39	Female	18-24	Some college	Average
P40	Female	25-34	College graduate	Somewhat above average
P41	Female	18-24	Some college	Average
P42	Male	18-24	Some college	Somewhat above average
P43	Male	18-24	Some college	Somewhat above average
P44	Prefer not to say	18-24	Some college	Somewhat above average
P45	Prefer not to say	18-24	Some college	Far below average
P46	Female	18-24	Some college	Somewhat above average
P47	Female	55-64	Advanced degree	Far below average
P48	Female	18-24	Some college	Far below average

P49	Male	35-44	Advanced degree	Somewhat above average
P50	Female	18-24	High school	Average
P51	Female	18-24	Some college	Average
P52	Female	18-24	Some college	Far above average
P53	Female	18-24	Some college	Average
P54	Female	18-24	Some college	Far below average
P55	Female	18-24	High school	Average
P56	Female	18-24	Some college	Far below average
P57	Female	18-24	Some college	Average
P58	Female	18-24	High school	Far below average
P59	Female	18-24	Some college	Average
P60	Male	25-34	Advanced degree	Somewhat above average

APPENDIX C: Supplementary data for Chapter 5

Screening Survey Questions

- Do you have a smart lock installed where you live (a smart lock is a door lock that you can connect to and control through an application on your smart phone)?
- Do you have admin capabilities on the smart lock and any other smart home devices in your home?
- Are you above 18 years of age?

Pre-study Survey Questions

- What is your study ID (provided to you by the researcher)?
- How old are you?
- What gender do you identify with?
- What is the highest education level you have attained?
- What is your current occupation?
- Aside from the smart lock, what smart home devices do you have in your house?
- Overall, how many smart home automation scenarios do you have set up in your house?
- What prevented you from setting up any automation scenarios?
- What platform do you use for creating smart home automation scenarios?
- How many smart home automation scenarios do you currently have set up that include the smart lock?

- What are those automation scenarios that you currently have set up which include the smart lock?
- What prevented you from setting up any automation scenarios that include the smart lock?
- Do you have any privacy or security concerns regarding setting up automation scenarios in your smart home? If yes, please include them in the text box below.
- Do you have any privacy or security concerns specifically related to setting up automation scenarios that include the smart lock? If yes, please include them in the text box below.

Main study Survey Questions

- What is you study ID (provided to you by the researcher)?
- Please, enter the automation scenario you created in the text box below:
- What motivated you to create this scenario?
- Do you have any security or privacy concerns specifically related to setting up this scenario?
- Based on the available technology, do you think setting up such a scenario is feasible?
- What do you think can go wrong (either while setting up the scenario or when it's being executed)?
- In what circumstances would you recommend not using this scenario?
- Will you be willing to set up this scenario if it:

  - Requires additional setup or configuration (user registration, device configuration, etc.)
  - Requires a monthly subscription fee
  - Increases electricity usage
  - Requires internet connection to work
  - Stores data on the cloud and not locally

- I believe setting up this scenario would:
  - Increase the overall security of my smart home
  - Increase my sense of security when I'm away from home
  - Increase the convenience level in my smart home
  - Increase my awareness of home surroundings
  - Increase my awareness of home inhabitants
  - Enhance my feedback on home monitoring

- If you set up this scenario, how concerned would you be about:
  - The security of your house in the case of a false positive (the scenario executes when it's NOT supposed to execute)
  - The security of your house in the case of a false negative (the scenario does NOT execute when it's supposed to execute)

APPENDIX D: Supplementary data for Chapter 6

Screening Survey Questions

- How old are you?
- Do you live in the United States? (yes, no)
- Are you above 18 years of age?

Interview Questions

Demographics

- What gender do you identify with? (Male, Female, Non-binary/third gender, Prefer not to say)
- What is your highest level of education? (8th grade graduate, High school graduate, Some college, College graduate, Advanced degree)
- What is your current occupation?
- Which option do you think most accurately describes your level of experience with setting up smart home devices? (Far above average, Somewhat above average, Average, Somewhat below average, Far below average)

After Watching Video 1

- How do you feel about relying on information received from the video doorbell to unlock your home's front door?
- Are there specific settings you would like to configure on the video doorbell to control the unlocking of the smart lock?

- Can you foresee any limitations, concerns, or potential issues with this aspect of the scenario? How would you mitigate those issues?
- On a scale of 1 to 5, how much would you trust this scenario? Why or why not? (I don't trust it at all, I slightly trust it, I somewhat trust it, I moderately trust it, I strongly trust it)
- On a scale of 1 to 5, how would you rate the level of complexity involved in setting up this scenario? (Not complex, Slightly complex, Somewhat complex, Complex, Very complex)

After Watching Video 2

- How do you feel about adding temporal or location constraints to this scenario?
- What temporal or location constraints would you add to this scenario, and why?
- Can you foresee any limitations, concerns, or potential issues with this aspect of the scenario? How would you mitigate those issues?
- On a scale of 1 to 5, how much would you trust this scenario? Why or why not? (I don't trust it at all, I slightly trust it, I somewhat trust it, I moderately trust it, I strongly trust it)
- On a scale of 1 to 5, how would you rate the level of complexity involved in setting up this scenario? (Not complex, Slightly complex, Somewhat complex, Complex, Very complex)

After Watching Video 3

- Overall, how do you feel about the automation unlocking the door based on these conditions?

- Can you think of any security or safety concerns associated with automatically unlocking the door based on these conditions?
- What safeguards or features would you expect to be in place to ensure the door is only unlocked when it's appropriate?
- Are there any other settings or customizations you would like to have control over in order to increase the level of trust in this automation scenario?

After Watching Video 4

- How do you feel about adding in a new device (security camera) that will be involved in the scenario?
- Unlike the first event, this part of the scenario will take place inside the house. How do you feel about that? Would that mean requiring different levels of control or different kinds of expectations?
- What kind of configurations and customizations would you like to have control over within the security camera in this scenario?
- Can you foresee any limitations, concerns, or potential issues with this aspect of the scenario? How would you mitigate those issues?
- On a scale of 1 to 5, how much would you trust this scenario? Why or why not? (I don't trust it at all, I slightly trust it, I somewhat trust it, I moderately trust it, I strongly trust it)
- On a scale of 1 to 5, how would you rate the level of complexity involved in setting up this scenario? (Not complex, Slightly complex, Somewhat complex, Complex, Very complex)

After Watching Video 5

- There is a variety of consequences that could occur if the driver goes beyond the delivery zone, such as sounding a siren and uploading a video to the cloud. How do you feel about configuring such consequences?
- What customization options or parameters would you like to see in the system settings for controlling these consequences?
- Can you foresee any limitations, concerns, or potential issues with this aspect of the scenario? How would you mitigate those issues?
- On a scale of 1 to 5, how much would you trust this scenario? Why or why not? (I don't trust it at all, I slightly trust it, I somewhat trust it, I moderately trust it, I strongly trust it)
- On a scale of 1 to 5, how would you rate the level of complexity involved in setting up this scenario? (Not complex, Slightly complex, Somewhat complex, Complex, Very complex)

After Watching Video 6

- When it comes to notifying authorized users, what configurations or customization options do you think should be available in the system settings?
- For each of the scenarios, who do you think should get notified, what should be the content of the message, and through what communication channels should they be notified? (go through each scenarios where a notification is needed)
- How important is it to get a notification when the driver rings the video doorbell?

(Not important at all, Slightly important, Somewhat important, Important, Very important)

- How important is it to get a notification when the door is unlocked for the driver to make the delivery? (Not important at all, Slightly important, Somewhat important, Important, Very important)
- How important is it to get a notification when the driver makes the delivery zone and leaves the house? (Not important at all, Slightly important, Somewhat important, Important, Very important)
- How important is it to get a notification when the driver is detected beyond the delivery zone? (Not important at all, Slightly important, Somewhat important, Important, Very important)

Overall Evaluation

- What do you think about the overall automation scenario described?
- How concerned are you about the security and privacy aspects of this automation scenario? How would you mitigate those concerns?
- How important are customizable security and privacy settings in a scenario like this? What settings or features would help alleviate your concerns?
- Finally, are there any other limitations, pitfalls, or considerations you'd like to share regarding this scenario?