Exploring End Users' Perceptions of Smart Lock Automation Within the Smart Home Environment

HUSSEIN HAZAZI, King Saud University, Saudi Arabia
MOHAMED SHEHAB, University of North Carolina at Charlotte, USA

Unlike their conventional counterparts, smart locks have the ability to communicate with other smart home devices which enables a level of integration and automation previously unimaginable. For instance, smart locks can exchange information with video doorbells, allowing homeowners to set up automation scenarios where the door automatically unlocks upon recognizing a familiar face. While some users might find it convenient, others might consider it a security vulnerability that could lead to unauthorized access to the house. This study employs a mixed-methods approach to explore user perceptions of creating smart home automation scenarios involving smart locks. 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. Our analysis provides an overall understanding of how setting up such automation scenarios affects several aspects of the smart home environment 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' perceived security or privacy advantages and disadvantages associated with setting up such automation scenarios.

CCS Concepts: • **Security and privacy** → **Usability in security and privacy**; • **Human-centered computing** → *Human computer interaction (HCI).*

Additional Key Words and Phrases: Smart locks, Smart home automation, Usable security, End user concerns, Factors affecting automation

ACM Reference Format:
Hussein Hazazi and Mohamed Shehab. 2024. Exploring End Users' Perceptions of Smart Lock Automation Within the Smart Home Environment. In *The 2024 European Symposium on Usable Security (EuroUSEC 2024), September 30-October 1, 2024, Karlstad, Sweden.* ACM, Karlstad, Sweden, 20 pages. https://doi.org/10.1145/3688459.3688480

1 INTRODUCTION

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 [9]. 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 [27].

Authors' Contact Information: Hussein Hazazi, hhazazi@ksu.edu.sa, King Saud University, Riyadh, Saudi Arabia; Mohamed Shehab, mshehab@charlotte.edu, University of North Carolina at Charlotte, Charlotte, North Carolina, USA.

Manuscript submitted to ACM

Online workflow automation platforms like IFTTT (If This Then That) and Zapier are also utilized by some homeowners for similar purposes [1, 2]. Research indicates that most users can easily create such automation scenarios with these systems, even without any programming knowledge [26]. Home automation serves many purposes within the smart home such as increasing convenience and managing redundant tasks [24]. Some studies have also proven its positive impact on home resource management [13, 17, 21]. However, some smart homeowners have shown security concerns regarding home automation [16]. Similarly, prior work has shown that end users often face several technical challenges when creating automation scenarios for smart home devices. One significant challenge is the compatibility between different devices and platforms, as not all devices can seamlessly communicate with each other [6]. Additionally, users may struggle with the complexity of setting up and configuring automation rules, especially if the interfaces are not user-friendly or require programming knowledge [19]. Troubleshooting issues that arise from conflicting rules or unexpected behavior of devices can also be daunting [4].

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 [15]. 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 [3, 5, 20]. Given the fact that the main function of smart locks is to secure the home and prevent unauthorized access, it's crucial to evaluate end users' privacy and security concerns associated with creating automations that include those locks. Similarly, it's also extremely important to understand the perceived security and privacy advantages of setting up and executing smart home automation scenarios that include the smart lock. Therefore, the main objectives of this work are:

- Identifying and categorizing the primary motivations for users integrating smart locks into home automation scenarios.
- Assessing the impacts of smart home automation scenarios that include smart locks on the overall security, awareness, and convenience levels within the home.
- Investigating the main concerns of users when setting up smart home automation scenarios with smart locks.
- Analyzing the factors influencing end users' decisions to adopt automation scenarios that include smart locks.

Prior research has studied the effectiveness of creating smart home automation scenarios in improving the smart home experience [7, 8, 10, 28]. However, this paper aims to categorize the automation scenarios that specifically include the smart lock based on the users' motivation to create them and the purpose they serve within the home environment. 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 especially the positive or negative effect those automations have on the smart home. 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?

2 RELATED WORK

Several user studies have explored users' limitations and requirements associated with creating and setting up smart home devices. Soares et al. [22] 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 paper, 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. [18] 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 [7, 8, 10, 28] 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. This paper 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. [8] highlight real-world challenges and opportunities in home automation, pointing to usability and interaction as significant considerations for users. Moreover, Touqeer et al. [25] 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 [23, 29]. 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 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, and the end user's concerns associated with smart automation scenarios that include the smart lock.

3 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.[11], we asked the participants to use a pen and paper to write their automation scenarios down.

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

Table 1. Participants' demographic information.

3.1 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 do not 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 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.

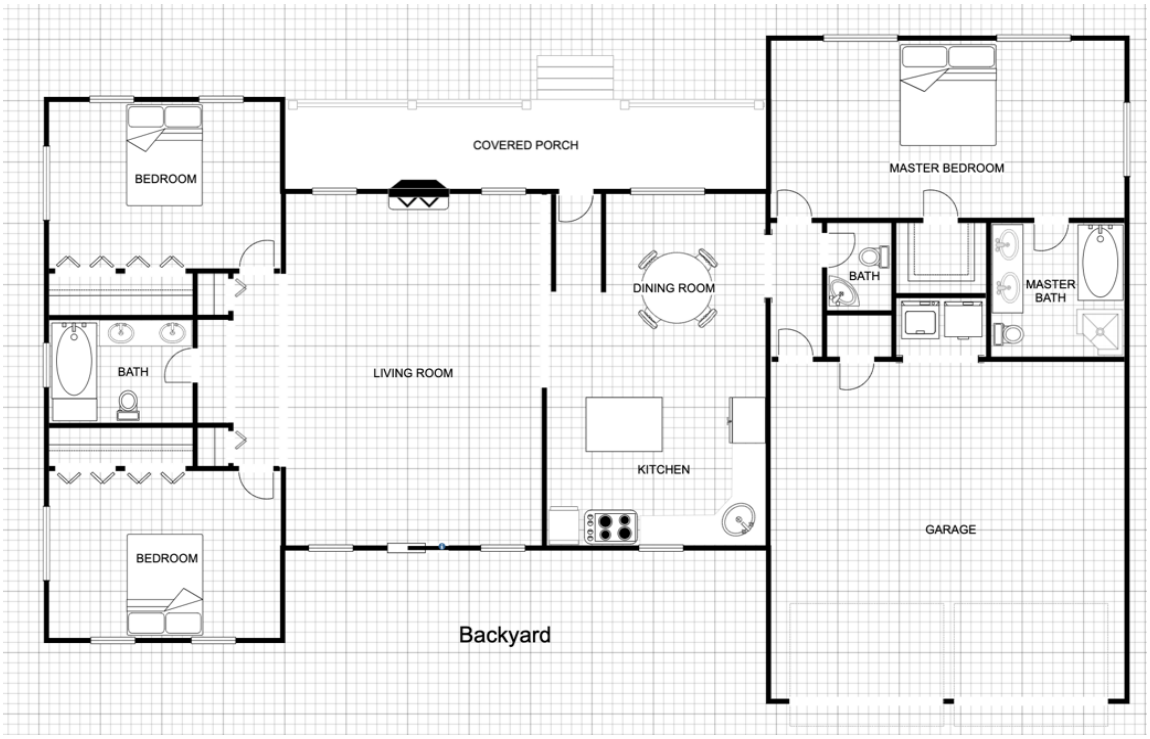


Fig. 1. The house layout used in the study

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

Table 2. Smart home devices and sensors installed inside the house used for the study.

3.2 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. Each session lasted for about 40 minutes on average. The session began with an 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

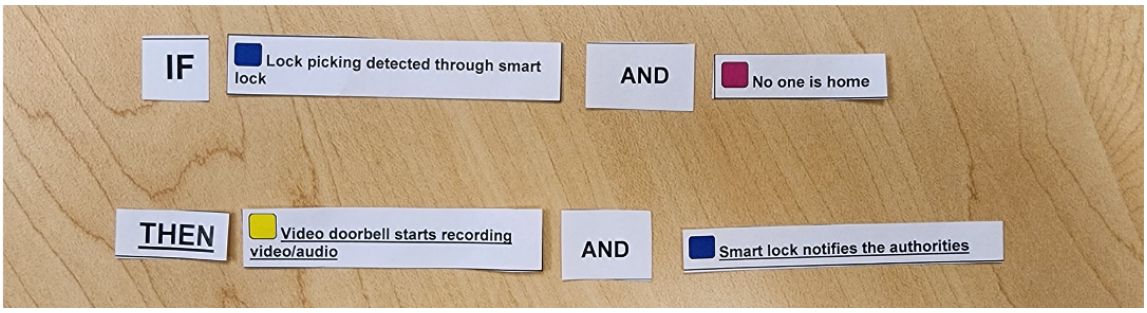


Fig. 2. An automation scenario created during the study using the cue cards

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.[22], we provided the participants with a hypothetical house layout (figure 1) and details about 11 installed smart devices and sensors (table 2). 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 *condition* THEN *action*). While automation scenarios can be created using varying syntax, prior studies have found a preference among users for if-then (or when-then) statement formats [12, 22]. We facilitated the task by offering color-coded cue cards representing each device's features, aiding in the scenario creation process (figure 2). 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.

3.3 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 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.

4 RESULTS

4.1 Pre-study Survey

We asked the participants to fill out a pre-study survey in order to explore their background and use of automation in their homes. Slightly less than half the participants (n=9) stated that they had not 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

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

Table 3. Smart home devices the study participants have installed in their home.

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

Table 4. 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.

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).

4.2 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 [12, 22]. 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.*

We also engaged the participants to understand the effect of setting up such automation scenarios that include the smart lock on different aspects of the smart home environment. To do this, we used a Likert scale that used the following designations: 'strongly disagree', 'somewhat disagree', 'neither agree nor disagree', 'somewhat agree', and 'strongly agree', where 'strongly disagree' corresponded to 1, meaning the participants strongly disagrees that a specific scenario would positively affect a specific aspect of the home environment and 'strongly agree' corresponds to 5 meaning the participant strongly agrees that a specific scenario would positively affect a specific aspect of the home environment. The six aspects of home environment we investigated were the end user's overall sense of security, sense of security while away from home, overall convenience, awareness of home surroundings, awareness of home inhabitants, and feedback on home monitoring. Table 4 shows how the automation scenarios in each category affects those different aspects of the home environment.

4.2.1 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. As depicted in table 4, the majority of participants stated that creating such automation scenarios would greatly 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 - P8:** *"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 - P11: *"Security reasons, when families go away on vacation they do not want to worry about the safety of their home."*

4.2.2 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 - P13: *"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 - P2: *"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."*

4.2.3 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 ($\bar{x} = 2.60$). Prior research [8, 10] has shown that shown that convenience is a major motivation for creating smart home automation scenarios in general. However, in the case of smart locks, we found that such scenarios can have a negative effect on the user's sense of security mainly due to the fact that false positives when smart locks are involved may allow unauthorized access to the home.

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

S1-3 Motivation - P1: *"This one was made strictly for convenience."*

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

S13-1 Motivation - P13: *"Convenience. I don't want to silence the home security system alarm manually every time I enter the house."*

4.2.4 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 - P10:** *"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 - P21:** *"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."*

4.2.5 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 - P3:** *"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 home-owner through smart lock.*
>
> **S8-2 Motivation - P8:** *"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."*

4.2.6 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 - P2: *"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 - P10: *"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."*

4.3 Automation Concerns

4.3.1 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. For instance, an automation scenario that aims to automatically unlock the door everyday at 7 AM on workdays might pose a security risk during vacations if not manually disabled by the homeowner. This concern was also evident in table 4 , where scenarios categorized as convenience-focused received lower scores in enhancing home security, particularly in aspects such as security while away from home ($\bar{x} = 2.60$) or overall security ($\bar{x} = 3.08$). 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 - P8: *"I might feel the security camera recording everyone coming and even me coming as a privacy concern."*

S4-4 Automation Scenario: IF *it's morning and someone is home* THEN *unlock front door and turn on front porch lights and turn on MB lights and kitchen lights.*

S4-4 Concern - P4: *"Front door unlocked at wrong time or when on vacation or when only kids are at home."*

4.3.2 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 - P2: *"It (the video doorbell) could detect someone incorrectly and let them into the home with no security system alarm which could be dangerous."*

4.3.3 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 - P3: *"Authorities being called for a false positive."*

4.3.4 Human Errors. Participants highlighted concerns about the accidental triggering of automation scenarios due to human errors in 12 of the 87 automations. These errors ranged from other residents 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.

S13-2 Automation Scenario: IF *a failed access attempt was detected through the smart lock and it's night time* THEN *the smart speaker sounds an alarm.*

S13-2 Concern - P13: *"If a legitimate user enters the wrong access code by mistake then the speaker would be annoying and wake up everyone at night for no reason."*

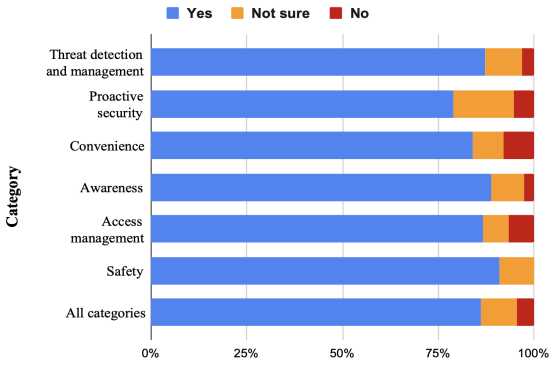
4.3.5 The Occasional Inconvenience. Although many participants felt that incorporating smart locks into automation scenarios could significantly enhance household convenience, there were concerns that certain scenarios (n=11) might result in inconvenience instead. For instance, participants who set up 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*

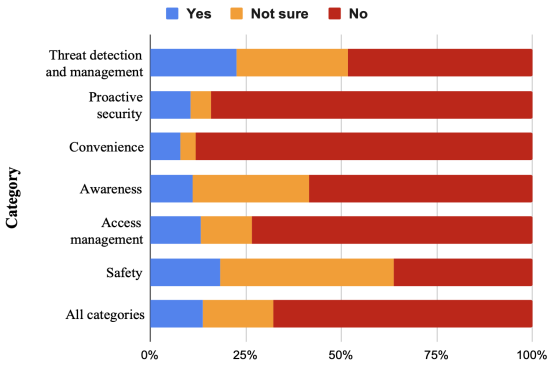
S10-2 Concern - P10: *"You could go outside, like to walk the dog, and accidentally get locked out and have to disarm the alarm. You'd be able to get back in with the door code, but if for some reason the door code didn't work you likely wouldn't have a hard copy of the key on you."*

S10-4 Automation Scenario: IF *3 failed attempts are entered into the smart lock* THEN *set the home security alarm to arm.*

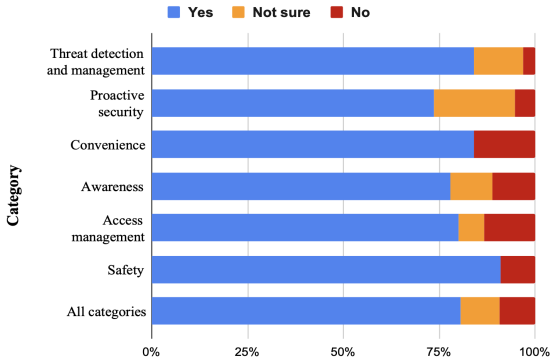
S10-4 Concern - P10: *"If you had little kids who were just learning how to use the smart lock, they could mess up more often and would be freaked out by the alarm going off."*



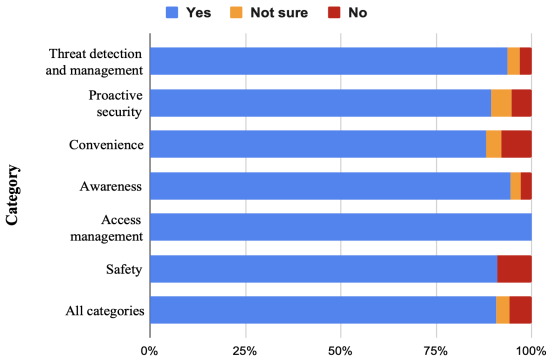
(a) Would you set up this scenario if it requires additional setup or configurations?



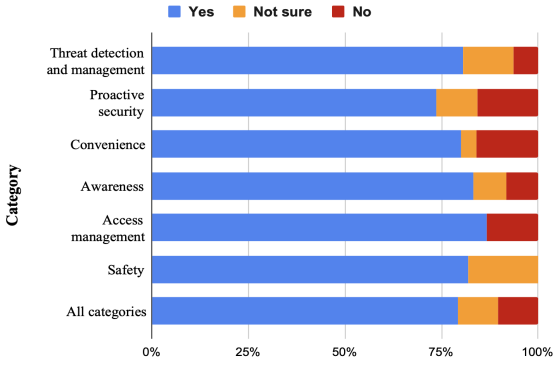
(b) Would you set up this scenario if it requires a monthly subscription fee?



(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?

Fig. 3. Factors affecting setting up an automation scenario

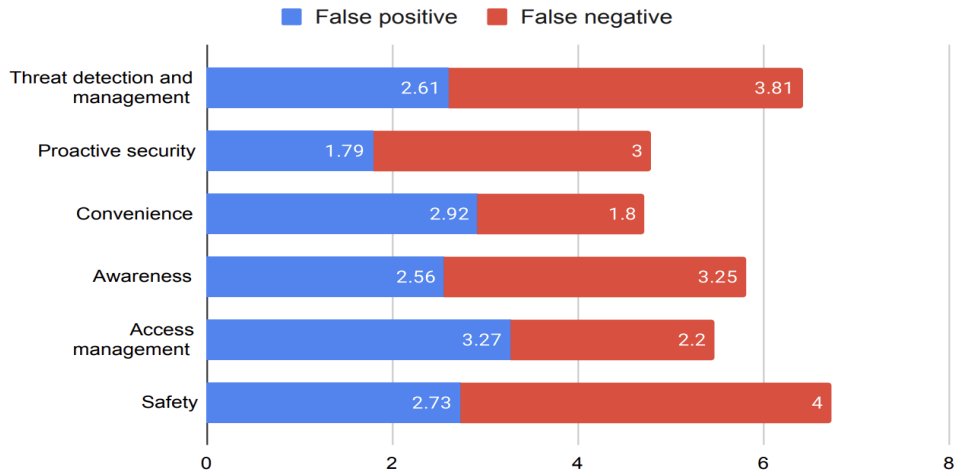


Fig. 4. A comparison of the participants' level of concern regarding the possibility of false positives and false negatives associated with each category

4.4 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 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 3, 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%.

4.5 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 positives and negatives across all 87 automation scenarios on a 5-point Likert scale where 1 corresponds to 'not concerned at all' and 5 corresponds to 'extremely concerned' (figure 4). 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.

> **P19:** *"False positives being sent to the authorities could be costly and lessen their interest in responding to real emergencies."*

5 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.

5.1 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.

5.2 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.

5.3 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. Even though previous work [14] has concluded that there is a general lack of concern regarding security issues associated with smart locks, our findings 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. Prior work [23] 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.

5.4 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 Design Guidelines

Based on the findings from this study, we propose several design guidelines to assist in the development and implementation of smart home automation scenarios involving smart locks.

5.5.1 Wider Integration. It's important that smart lock manufacturers ensure that their devices can easily integrate with a wide range of smart home devices and platforms. Many commercially available smart locks still restrict end users from integrating with a wide range of smart home devices to create comprehensive automation scenarios. This limitation hinders users' ability to fully leverage the potential of their smart locks in enhancing overall security, convenience, and awareness within their smart home environment. Without seamless integration capabilities, users may miss out on opportunities to automate tasks such as integrating with video doorbells for enhanced security monitoring or syncing with smart lighting systems for improved convenience. As smart home ecosystems continue to evolve, increasing interoperability among devices remains crucial for maximizing the benefits of smart lock technology.

5.5.2 Automation Templates. It is essential for smart lock systems to allow users to create automation scenarios with flexible conditions and actions to accommodate for diverse needs and preferences. Providing templates for common scenarios enables users to easily implement basic automation. However, supporting customization ensures that advanced users can tailor scenarios to specific situations, such as integrating with security cameras or adjusting based on different family member schedules. This flexibility not only enhances convenience but also empowers users to optimize security measures according to their unique home dynamics and lifestyles.

5.5.3 Educational Resources. Providing comprehensive resources to educate users about automation scenarios involving smart locks is crucial. These resources should outline how such scenarios function, including their potential security implications and the best practices for creating secure and effective automations. By understanding how automation impacts security and privacy, users can make informed decisions when configuring their smart locks. Clear guidelines on setting up access controls, managing data privacy, and integrating with other smart home devices ensure that users maximize the benefits of automation while minimizing risks. Ultimately, these educational efforts promote responsible use and enhance overall user confidence in smart lock technologies.

6 LIMITATIONS

This study acknowledges several limitations, including the small sample size and the potential for selection bias given the convenience sampling method and participants demographics. 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.

7 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.

REFERENCES

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

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

[3] Naba M Allifah and Imran A Zualkernan. 2022. Ranking security of IoT-based smart home consumer devices. *Ieee Access* 10 (2022), 18352–18369.

[4] Adeeb Mansoor Ansari, Mohammed Nazir, and Khurram Mustafa. 2024. Ontology-Based Classification and Detection of the Smart Home Automation Rules Conflicts. *IEEE Access* 12 (2024), 85072–85088.

[5] Suriya Priya R Asaithambi, Sitalakshmi Venkatraman, and Ramanathan Venkatraman. 2021. Big data and personalisation for non-intrusive smart home automation. *Big Data and Cognitive Computing* 5, 1 (2021), 6.

[6] Eileen Becks, Peter Zdankin, Viktor Matkovic, and Torben Weis. 2023. Complexity of smart home setups: a qualitative user study on smart home assistance and implications on technical requirements. *Technologies* 11, 1 (2023), 9.

[7] Julia Brich, Marcel Walch, Michael Rietzler, Michael Weber, and Florian Schaub. 2017. Exploring end user programming needs in home automation. *ACM Transactions on Computer-Human Interaction (TOCHI)* 24, 2 (2017), 1–35.

[8] AJ Bernheim Brush, Bongshin Lee, Ratul Mahajan, Sharad Agarwal, Stefan Saroiu, and Colin Dixon. 2011. Home automation in the wild: challenges and opportunities. In *proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 2115–2124.

[9] Chola Chhetri. 2022. *Designing for Privacy in Smart Home Devices*. Ph. D. Dissertation. George Mason University.

[10] Yi-Shyuan Chiang, Ruei-Che Chang, Yi-Lin Chuang, Shih-Ya Chou, Hao-Ping Lee, I-Ju Lin, Jian-Hua Jiang Chen, and Yung-Ju Chang. 2020. 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*. 1–14.

[11] Fulvio Corno, Luigi De Russis, and Alberto Monge Roffarello. 2022. How do end-users program the Internet of Things? *Behaviour & Information Technology* 41, 9 (2022), 1865–1887.

[12] Anind K Dey, Timothy Sohn, Sara Streng, and Justin Kodama. 2006. iCAP: Interactive prototyping of context-aware applications. In *Pervasive Computing: 4th International Conference, PERVASIVE 2006, Dublin, Ireland, May 7-10, 2006. Proceedings 4*. Springer, 254–271.

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

[14] Hussein Hazazi and Mohamed Shehab. 2023. 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)*. 559–577.

[15] Waheb A Jabbar, Tee Kok Kian, Roshahliza M Ramli, Siti Nabila Zubir, Nurthaqifah SM Zamrizaman, Mohammed Balfaqih, Vladimir Shepelev, and Soltan Alharbi. 2019. Design and fabrication of smart home with internet of things enabled automation system. *IEEE access* 7 (2019), 144059–144074.

[16] Kim J Kaaz, Alex Hoffer, Mahsa Saeidi, Anita Sarma, and Rakesh B Bobba. 2017. Understanding user perceptions of privacy, and configuration challenges in home automation. In *2017 IEEE Symposium on Visual Languages and Human-Centric Computing (VL/HCC)*. IEEE, 297–301.

[17] Jean-Nicolas Louis, Antonio Calo, Kauko Leiviskä, and Eva Pongrácz. 2015. Environmental impacts and benefits of smart home automation: Life cycle assessment of home energy management system. *IFAC-PapersOnLine* 48, 1 (2015), 880–885.

[18] Andrea Mattioli and Fabio Paternò. 2023. Understanding User Needs in Smart Homes and How to Fulfil Them. In *International Symposium on End User Development*. Springer, 125–142.

[19] Pavle Mićović, Marija Antić, Ištvan Pap, and Dušan Davidov. 2022. User Interface for the Creation of Smart Home Automation Rules. In *2022 IEEE Zooming Innovation in Consumer Technologies Conference (ZINC)*. IEEE, 186–190.

[20] S Pradeep, T Kousalya, KM Aarsha Suresh, and Jebin Edwin. 2016. IoT and its connectivity challenges in smart home. *International Research Journal of Engineering and Technology* 3, 12 (2016), 1040–1043.

[21] Mihály Sági, Dejan Mijic, Dejan Milinkov, and Bojan Bogovac. 2012. Smart home automation. In *2012 20th Telecommunications Forum (TELFOR)*. IEEE, 1512–1515.

[22] Danny Soares, João Pedro Dias, André Restivo, and Hugo Sereno Ferreira. 2021. 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*. Springer, 512–525.

[23] Milijana Surbatovich, Jassim Aljuraidan, Lujo Bauer, Anupam Das, and Limin Jia. 2017. 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*. 1501–1510.

[24] Olutosin Taiwo, Lubna A Gabralla, and Absalom E Ezugwu. 2020. 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*. Springer, 878–894.

[25] Haseeb Touqeer, Shakir Zaman, Rashid Amin, Mudassar Hussain, Fadi Al-Turjman, and Muhammad Bilal. 2021. Smart home security: challenges, issues and solutions at different IoT layers. *The Journal of Supercomputing* 77, 12 (2021), 14053–14089.

[26] Blase Ur, Elyse McManus, Melwyn Pak Yong Ho, and Michael L Littman. 2014. Practical trigger-action programming in the smart home. In *Proceedings of the SIGCHI conference on human factors in computing systems*. 803–812.

[27] Qi Wang, Pubali Datta, Wei Yang, Si Liu, Adam Bates, and Carl A Gunter. 2019. Charting the attack surface of trigger-action IoT platforms. In *Proceedings of the 2019 ACM SIGSAC conference on computer and communications security*. 1439–1453.

[28] Rayoung Yang and Mark W Newman. 2013. 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*. 93–102.

[29] Svetlana Yarosh and Pamela Zave. 2017. Locked or not? Mental models of IoT feature interaction. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. 2993–2997.

A APPENDICES

A.1 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?

A.2 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.

A.3 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)