To Share or Not to Share: Feature Analysis of Smart Home Management Systems to Assess Access Control with External Users

Leena Alghamdi[1], Jinkyung Katie Park[2], Heather Lipford[3], and Pamela Wisniewski[2]

[1] University of Central Florida, Orlando FL 32816, USA,
[2] Vanderbilt University, Nashville TN 37235, USA,
[3] University of North Carolina at Charlotte, Charlotte NC 28223, USA
le631195@ucf.edu, jinkyung.park, pamela.wisniewski@vanderbilt.edu, richter@uncc.edu

Abstract. In the smart home landscape, there is an increasing trend of homeowners sharing device access outside their homes. This practice presents unique challenges in terms of security and privacy. In this study, we evaluated the co-management features in smart home management systems to investigate 1) how homeowners establish and authenticate shared users' access, 2) the access control mechanisms, and 3) the management, monitoring, and revocation of access for shared devices. We conducted a systematic feature analysis of 11 Android and iOS mobile applications ("apps") and 2 open-source platforms designed for smart home management. Our study revealed that most smart home systems adopt a centralized control model which necessitates shared users to utilize the primary app for device access, while providing diverse sharing mechanisms, such as email or phone invitations and unique codes, each presenting distinct security and privacy advantages. Moreover, we discovered a variety of access control options, ranging from full access to granular access control such as time-based restrictions which, while enhancing security and convenience, necessitate careful management to avoid user confusion. Additionally, our findings highlighted the prevalence of comprehensive methods for monitoring shared users' access, with most systems providing detailed logs for added transparency and security, although there are some restrictions to safeguard homeowner privacy. Based on our findings, we recommend enhanced access control features to improve user experience in shared settings.

Keywords: Smart home management systems, Access control, Privacy, Security, Feature analysis

1 Introduction

According to a recent report, there will be approximately 13.5 billion smart home devices in active use by 2025 [38]. These devices have become an essential

component of modern living [25] for diverse facets of everyday life such as energy savings, in-home healthcare, and enhanced living environments [37]. The contemporary landscape of smart home ecosystems has witnessed a notable shift, expanding their functionality beyond traditional residential spaces to sharing devices with individuals outside the home [24]. Empirical evidence suggests that smart home users are increasingly extending access to their smart devices to individuals residing outside their homes to assign the responsibility of overseeing home safety, security, and the well-being of occupants to a reliable group of family and friends [24]. The convenience of remote device management and the trust placed in family members or other trusted individuals for access emerge as pivotal motivations for sharing smart home devices [36,31].

Recent advances and existing research on shared smart homes management has set the groundwork for understanding the complexities of device management and access control in those connected environments [30,23,8,55]. For example, He et al. [8] explored access control and authentication mechanisms in shared smart home environments, proposing a capability-centric model and emphasizing the need for flexibility in authentication. Despite progress, several challenges and unsolved problems remain in the field of sharing smart home devices. Key issues include ensuring secure and private access to shared devices, as unauthorized access or data breaches can lead to significant privacy concerns. Additionally, managing who has access to which devices and when can be complex, especially with multiple users and varying access needs [55]. Furthermore, users require systems that are both secure and convenient to manage, making it critical to balance these aspects for effective smart home management. Yet, none of the prior works presented a systematic review of the trend in multi-user access control features in existing smart home systems. Our study addresses this gap by conducting a comprehensive feature analysis study to gain insights into the existing access control mechanisms in terms of sharing smart home devices beyond the home. We focused on understanding the functionality and limitations of these mechanisms, paving the way for the development of effective solutions that enhance the overall shared smart home experience.

In this work, we systematically analyzed co-management features in various smart home management systems focusing on access control mechanisms in terms of sharing (i.e., user-level permissions, device sharing, notification sharing, access scheduling, remote access, security, privacy measures, and customization options). The primary goal of our work is to assess the effectiveness of access control mechanisms within these systems, focusing on how they ensure privacy, and cater to diverse user needs when sharing smart home devices beyond household. Additionally, we identified shortcomings or limitations in the co-management features and access control mechanisms of the smart home management systems. Based on our review, we provided comprehensive recommendations to both smart homeowners and smart home management systems designers to enhance user experiences, address identified gaps, and improve the overall effectiveness of access control mechanisms in smart home environments. The research questions that guided our work include:

- RQ1: What methods do smart home management systems employ to facilitate the setup and authentication of shared users' access, and how do these systems enable remote device access for shared users?
- RQ2: What access control mechanisms are currently employed in smart home management systems when sharing smart home devices with individuals residing outside the home?
- RQ3: How is access control managed, monitored, and revoked for shared devices when using smart home management systems?

To answer the research questions, we systematically analyzed 11 Android and iOS mobile applications ("apps") and 2 open-source platforms based on reputable and reliable sources. Overall, our findings highlighted a trend in smart home device-sharing practices towards enhanced flexibility and accessibility. While the majority implement a centralized control mechanism, as evidenced by the need to access shared devices through the same app as the homeowner or web interface, if provided, and sharing is initiated by the homeowner, we have also identified exceptions in which access requests are initiated by the shared user, enhancing more interactive environments within smart homes. Additionally, various authentication methods, including account-based and phone number verification, aim to balance accessibility and security (RQ1). We also observed variations in access control mechanisms for shared users, providing flexibility through unrestricted full access, partial access by device, property, or user role, temporary access settings, and geofencing control. While these options enhance convenience and security, they require careful consideration to mitigate potential complexity and user confusion (RQ2). We revealed varied methods in smart home systems for managing, monitoring, and revoking shared device access, with most systems featuring detailed logs for transparency and security, though some limit log access to protect homeowner privacy. Various revocation methods, including full, device-level, and shared user-initiated options, alongside access expiry features, enhance system security and flexibility (RQ3). Based on our results, we provided design recommendations for a secure, privacy-preserving, and easy-to-use device-sharing experience for homeowners and shared users.

Our research encourages the FTC research community to think critically about the design of smart home management systems for device sharing to ensure the privacy and security of the homeowner, as well as to provide convenience in smart home device co-management. Specifically, through this work, we significantly advance our understanding of the evolving landscape of shared smart home security and privacy, paving the way for more effective solutions by demonstrating potential trade-offs between convenience and security and presenting best practices to optimize the balance between the two in smart home access control systems. In addition, we provide design recommendations and practical insights for designers and developers to enhance the user experience and safety of smart home management systems for shared devices.

The rest of this paper is structured as follows: Section 2 reviews the related work, highlighting existing research on smart home management systems and access control mechanisms. Section 3 details the methods employed for data

collection and analysis, emphasizing the comprehensive evaluation and practical relevance of our approach. Section 4 presents the findings categorized into key themes, including shared user access methods, access control mechanisms, and privacy-aware management. Section 5 discusses the implications and potential challenges identified, offering design recommendations for enhancing smart home management systems. Finally, Section 6 concludes the paper.

2 Related Work

2.1 Managing Smart Home Devices and Addressing Intra-Household Dynamics

Smart home systems are widely used for managing diverse household devices such as thermostats, lights, and locks through interfaces such as mobile and web apps [42,33]. They inherently serve as multi-user platforms, accommodating various individuals such as partners, roommates, parents, children, guests, and household employees who seek the capability to utilize and configure smart devices within the household. Previous research (e.g., [34,7,56]) has highlighted the emergence of potential conflicts and tensions among these stakeholders, even in households where there is no malicious intent. For instance, tech-savvy individuals may limit access to home functions like thermostats, leading to conflicts among household members [7,56]. Studies have also identified privacy concerns and breaches that may arise among co-occupants [35,7], as well as the potential for harassment through remote control of devices [35].

Meanwhile, the majority of smart home platforms employ a coarse-grained, all-or-nothing access control system [3]. For instance, Amazon Echo's basic access mechanisms allow any household member to access the primary user's information or make purchases if linked to a credit card [1]. However, system access from household members beyond the desired level can contribute to trust problems within households, invoking home privacy issues [33]. Recognizing such challenges, researchers highlighted that offering differentiated access to cater to diverse user needs is crucial for managing intra-household dynamics [33,30]. For example, parents might limit their children's device usage, while roommates could seek privacy in their spaces. In a recent study, He et al. conducted a comprehensive user study representing participants desired fine-grained access control in shared smart home environments, with preferences varying based on the relationship between users and the specific capabilities being controlled [8].

2.2 Extending Access Control Beyond Household Boundaries

Individuals often share their smart devices with others, beyond their households to manage home safety and well-being, including pet and home monitoring during absences through remote home access and communication with residents [24]. Another compelling dimension of sharing practice beyond households relates to its role in enhancing emergency co-monitoring, ensuring the safety and

well-being of occupants through features like real-time alerts, remote monitoring, and automated emergency responses [28]. The trend of extending smart home access control beyond household boundaries introduces new challenges, necessitating robust mechanisms for secure and privacy-conscious device sharing in complex multi-user contexts. Currently, access control solutions for external sharing are basic and lack comprehensive rule-setting capabilities for diverse environments [8]. While some smart home platforms provide solutions for remote access, these solutions are often device and vendor-specific, limiting their applicability in complex environments with multiple devices and users [21]. Recent research has expanded to consider secondary users and guests [5,4,7], emphasizing the necessity for a more thorough exploration of multi-user concerns related to the use of smart homes [6,7]. For instance, He et al. [8] discovered that the desired access-control policies differ across devices' capabilities, people relationships, and contextual factors, highlighting the complexity of extending access control beyond the home environment. As such, the findings from prior work underscore the need for nuanced access control mechanisms that can account for contextual factors when sharing smart home devices outside the home.

On the other hand, many commercial smart home platforms offer a simple access control system mode, either full access or none at all. For instance, Samsung SmartThings [22] grants equal control to all authorized users, while Apple Home [21] provides remote access and editing options, but still falls short of effectively managing conflicting user demands. In a broader context of the Internet of Things (IoT), a comprehensive survey identified critical requirements for effective access control in smart homes, such as granularity, interoperability, and scalability among others, emphasizing the need for fine-grained, context-aware systems that were scalable, reliable, and lightweight [33]. As such, prior research identified potential challenges associated with extended smart home access control beyond household boundaries and called the need for robust mechanisms for granular device-sharing in multi-user contexts.

In addition, while researchers underscored the benefits of sharing with emergency contacts, they also noted potential personal privacy concerns [28]. Moreover, privacy and security challenges related to the sharing of smart devices have consistently been identified as key factors influencing the decision to share smart home devices with others [26,32]. For instance, smart home device users were willing to share only with those they trust the most or when the risk of privacy breaches is minimized [7,24]. As privacy concerns grow with device sharing, the challenge becomes how to balance the sharing benefits, such as enhanced convenience and collaboration, and potential privacy concerns through access control features. Therefore, our research delved into the examination of existing access control features in smart home systems to understand their capabilities and shortcomings comprehensively. Through this analysis, we aim to provide design recommendations that effectively address privacy concerns while optimizing the benefits of shared smart home environments.

3 Methods

3.1 Data Collection and Scoping Process

We conducted a systematic analysis of smart home management systems; including mobile apps and open-source platforms, aiming to reflect the average smart device user's experience. Our systematic approach involved several steps.

Data Collection Process. Firstly, we identified a comprehensive list of smart home management systems primarily based on the most popular systems of 2023 according to the ZDNet website [9], where some of them are identified as key players companies in the global smart home market [20]. This initial selection comprised four mobile apps (SmartThings, Apple Home, Amazon Alexa, and Google Home), along with the Home Assistant and IFTTT platforms. Additionally, we included some other smart home management systems (i.e., SmartRent, Wink, Hubiata Elevation, and Control4 Home) based on their substantial presence and influence within the smart home ecosystem [10,11,12,13]. Moreover, to address emerging research findings and user preferences [24], and following CNET's expert recommendations for the best smart devices in 2023, we broadened our app selection to encompass specialized apps for various smart home devices, like smart locks [14], smart doorbells [15], smart lights [16], security systems [17], smart indoor and outdoor cameras [18], and smart speakers [19]. This expansion led to the initial inclusion of ten corresponding systems: August, U-tec, Yale, Arlo, Nest, Ring, Wyze, Philips Hue, Xfinity, and Amazon Alexa, resulting in a total of 19 initial systems.

Data Scoping Process. We applied specific criteria to narrow down our selection. These criteria focused on ensuring user accessibility, affordability, and comprehensive management capabilities from any location. Specifically, we prioritized widely used systems that do not require specialized installation or technical expertise, as well as those offering free trials without the need for sensitive financial information. Additionally, we favored systems that allow flexible and convenient management from any location, excluding those with limitations on access and control within the home.

Following our predefined criteria, six apps were removed from the initial selection of 19 systems during the installation process. We removed four apps that required subscription payment, one app that required to be properly set up by a professional person from the same company (i.e., a certified installer), and one app that required its own internet service and subscription payment. Additionally, there was a lack of proper and reliable documentation available for us to review, making it challenging to provide a comprehensive evaluation of these six apps.

Final Dataset. Our final data set comprised 11 smart home management mobile apps and 2 open-source platforms which are; SmartThings [2], Apple Home

[44], Amazon Alexa [45], Google Home [46], August [48], Yale [49], Arlo [50], Ring [51], Wyze [52], Philips Hue [54], and SmartRent [53], and 2 open-source platforms; the Home Assistant [43], and IFTTT [47] platforms. With this list of 13 systems, we conducted a systematic evaluation and analysis of co-management features in smart home management systems.

3.2 Feature Analysis Approach

We conducted our feature analysis by installing each app on an iOS mobile phone and then connecting them to smart home devices newly installed in the first author's house specifically for this study. This setup enabled a thorough exploration of all the features related to sharing smart home devices with external users. Table 1 in Appendix A lists the smart home devices connected to each system, detailing the devices chosen for their relevance and the scope of sharing functionalities they offer. The phone used for the analysis was an iPhone 12 Pro with 128 GB of storage running the iOS version 17.1 operating system.

Owner's Perspective. Each system was coded based on the features it supported in terms of sharing smart home devices with shared users outside of households. We created tables to address our research questions, organizing the various co-management features and corresponding systems in rows and columns. Then, for each app, we indicated the features that are supported by the app for the owners of smart home devices.

Shared User's Perspective Next, to analyze sharing and access control features provided to shared users, we install the same 13 apps on another mobile device to mimic the role of a shared user. The phone used for a shared user role was a Pixel 3a phone with 64 GB of storage running the Android version 12 operating system. After installing all the apps, we analyzed the access and sharing features that are supported by the app for the shared users of smart home devices.

Data Coding. Once the initial coding of features for both the device owners and shared users was complete, an iterative round of coding was performed to identify more detailed information for co-management features that were present. The data coding was performed by the first author with the discussion involving co-authors to form a consensus. Through the data coding process, we were able to inductively create a comprehensive list of the co-management features currently available in the smart home management systems. We identified different levels of access control when sharing smart home devices within all apps in terms of; 1) shared user access methods, authentication, and remote access mechanisms, 2) access control mechanisms, and 3) holistic privacy-aware management of shared users, monitoring, and access revocation. Note that the relationship between features and systems is many-to-many; a single feature may be present in multiple systems, while a system may support multiple features.

Our method offered several advantages; it provided a comprehensive evaluation by including a diverse selection of systems and conducting an in-depth feature analysis from both the owner's and shared user's perspectives. Our approach allowed us to highlight granular control options and customization possibilities, which are often overlooked. By balancing technical rigor with practical insights, our method supported actionable recommendations for enhancing smart home management systems' co-management features, security, and user experience.

4 Findings

We categorize our findings into three primary themes; the shared user access methods, authentication, and remote access mechanisms (RQ1), the granularity of access control mechanisms (RQ2), and the holistic privacy-aware management of shared users, monitoring, and access revocation (RQ3).

4.1 Access-Sharing Methods and Remote Access Management for Shared Users (RQ1)

Facilitating Smart Home Device Sharing: Centralized Control Model with Flexible Sharing Methods. In this subsection, we describe how the trend in smart home device sharing is evolving towards enhanced flexibility and user accessibility.

Accessing Shared Devices. We discovered that the majority of smart home management systems (n=12) require shared users to access shared devices either by utilizing the same app as the homeowner or through a web interface, if available. Shared users typically log in to their accounts either through the app or the web interface provided by the system. Once authenticated, shared users should be able to access and control the shared devices that the homeowner has granted them access to. This effectively establishes a centralized control model, as no companion or dedicated apps are provided for shared users. However, only one app (SmartRent app) grants a temporary access code to a shared user without the need for app installation by every user to enhance accessibility and flexibility.

Access Initiation. When sharing access to smart home devices, the homeowner typically initiates the process in all systems (n=13), ensuring control remains with the primary user. Two apps (n=2) offer shared users the ability to request access, alongside the basic homeowner-initiated sharing. This feature enhances convenience, simplifies access sharing, and improves communication between homeowners and shared users. For example, in the Google Home app, when a homeowner's devices are on a shared or open Wi-Fi network, they appear as "local devices" in others' apps. Shared users can request access, prompting the homeowner to accept or decline via email or app notification. This dual approach to access sharing, combining homeowner control with shared user requests, highlights a potential direction for enhancing interactive features within smart home systems.

Sharing Methods. We found that the majority of smart home systems (n=10) initiate access sharing by sending invitations to create or use existing accounts, or by sharing temporary/entry codes, demonstrating significant homeowner control over access. In terms of the specific sharing methods, we found a spectrum of sharing methods ranging from least to most flexible control that support user preferences. At the lower end of the spectrum, access sharing is exclusively done via phone number, potentially excluding users without phones or hesitant to provide personal details. Sometimes, direct sharing of smart home device control is not supported, thus, to share access, shared users may log in using the same account credentials of the homeowners, posing potential security and privacy risks. Moving towards a moderate level of control and flexibility, one system permits homeowners to indirectly invite new members where homeowners create accounts and share details with shared users either as 'Administrators' or 'Users.' Others offer invitation links with expiration periods for added security and privacy, providing a balanced approach between control and user convenience. At the highest degree of control and flexibility, most smart home systems (n=6) enable homeowners to send email invitations to shared users, while others (n=4) offer ephemeral access-sharing features like temporary codes, catering to both persistent and one-time access needs. Moreover, one system (i.e., SmartThings) allows sharing via QR code, representing the highest degree of control and flexibility among all systems.

Overall, when setting up device sharing in smart home management systems, the majority of systems require shared users to access devices through the same app as the homeowner or a web interface if provided, and homeowner-initiated sharing for device access, reflecting a centralized control model. However, innovative exceptions such as temporary access codes enhance user flexibility without app utilization, and other features that enable shared users to request access promote interactive and user-driven environments. These advancements collectively represent an industry focus on systems that are both secure and convenient, catering to the evolving needs of homeowners and shared users alike.

Exploring Authentication and Remote Access in Smart Home Device Sharing. In this subsection, we delve into the intricate processes of authentication and remote access within smart home management systems. Our analysis uncovers the diverse methods employed to ensure secure device sharing and convenient remote control for shared users.

Shared Users Authentication Methods. Next, we found diverse authentication practices for shared users across smart home systems, ensuring secure access to the shared devices. To begin the authentication process, shared users typically receive notifications primarily through either in-app notifications or emails. Upon receiving the invitation, shared users authenticate their access by following the provided link or instructions. In contrast, some apps implement phone number verification, emphasizing simplicity and quick setup through verification codes sent to mobile phones. Similarly, security-focused apps such as Ring, and

Arlo, adopt a rigorous two-step verification process, combining email authentication with subsequent codes sent to associated phone numbers for enhanced protection. Some apps (n=3) utilize OAuth for secure connections. For example, Philips Hue seamlessly integrates with other smart home platforms such as Amazon Alexa, Google Assistant, and Apple Home, requiring users to link their Philips account with these services, often involving OAuth. One app (i.e., Wyze) supports two-factor authentication (2FA) via email verification codes, which can be enabled through the app's account settings. This balance between accessibility and security in authentication underscores the ongoing need for optimized frameworks to adapt to evolving user needs and technology.

Exploring Shared Users' Remote Access in Smart Home Management Systems. We found that while mobile apps are the predominant choice for remote access in smart home management systems (n=13), several systems (n=7) offer additional flexibility with sharing remote access through web-based interfaces. This flexibility expands smart home management system users' control beyond traditional mobile app boundaries (as shown in the codebook in Appendix B). While the two apps offer a web-based interface, they primarily cater to account management rather than device management. The Home Assistant platform, essentially a web-based platform, provides a companion app for remote access. This diversity in interface options underscores the importance of flexibility and accessibility in smart home management systems. Furthermore, the majority of the systems (n=7) that provide remote access through the web-based interface are based on Cloud-based platforms, ensuring seamless and secure connectivity from any location. Meanwhile, other apps (n=5) that provide remote access exclusively via mobile devices tend to require the use of a hub to enable remote access. While using a hub enhances device integration and control, it can introduce potential challenges such as additional cost, setup complexity, and dependency on an additional piece of hardware for remote functionality.

In summary, we found various authentication methods, including account-based, phone number verification, and OAuth, that reflect the ongoing effort to balance accessibility and security in smart home device sharing. Additionally, we observed a trend toward providing remote access through both mobile apps and web-based interfaces, highlighting the importance of flexibility and accessibility in modern smart home management systems. Cloud-based platforms can further enhance connectivity and convenience, while the use of hubs could introduce additional considerations such as cost and setup complexity. Overall, these findings underscore the landscape of smart home device sharing to support enhanced accessibility, security, and user experience.

4.2 Access Control Mechanisms in Smart Home Systems for Device-Sharing (RQ2)

Allowing Shared Users Unrestricted Access with Full Access. We found that most systems allow the shared user full access, providing them with unrestricted control over shared smart home devices. With full access, shared users

can control all devices within the home, including accessing cameras or controlling door locks.

Full Access by Default. Our result revealed that three apps provide shared users full access by default. For instance, the Google Home app offers full access without additional granularity where everyone invited to the shared home management system can view all activity and access all devices and settings, including devices added later. The shared users can also edit all home device settings and add and remove devices, services, and people to the shared home including homeowners. This adds convenience to homeowners, but it also potentially makes the Google Home app vulnerable to privacy concerns and potential security risks. On the other hand, in two systems (i.e., Amazon Alexa, IFTTT), a homeowner cannot directly share control of their smart home devices with other people via the systems' standard features, as they are designed so that each user manages only the devices linked to their individual account. However, if a homeowner wants to allow someone else to control their devices through those systems, one possible workaround is for both parties to log in using the same account credentials. This method gives the shared user full access to the devices registered to that account. It's important to note that this approach requires sharing sensitive login information, which can raise security concerns.

Full Access with Role-based Access (Predefined Permissions). In three systems, shared users are granted comprehensive control over the smart home system based on predefined roles. This approach operates with fixed roles, each role comes with a set of permissions and access levels that are predetermined by the system and not subject to customization by the homeowner. For example, the Home Assistant platform provides "Administrators" roles for shared users with full control over smart home devices, automation, scenes, and dashboards, while "Users" have more limited interaction capabilities. Similarly, the Philips Hue app grants shared users "Administrator" status and provides them with full access, allowing control over permissions, system configurations, and the ability to manage smart home devices and shared members within households. Therefore, a shared user in the Philips Hue app can even remove the homeowners from their homes and change homeowners' permissions which can pose a potential security risk.

Homeowner-Granted Full Access. In some apps (n=3), shared users can only gain full access if explicitly permitted by the homeowner. This grants the homeowner discretion to provide full access based on their judgment or specific circumstances. Two apps impose restrictions on their ability to modify the list of authorized users or add/remove additional shared users to the shared home. For instance, with the SmartThings app (Fig. 1b), shared users can do everything, such as controlling, adding, editing, and deleting devices and automation, except for adding or removing additional shared users to the shared home management systems. By limiting the shared user's ability to modify the list of authorized users, the homeowner maintains better control over who has access to the smart

security system, hence, reducing the risk of unauthorized changes. In contrast, the Apple Home app provides shared users with broader control, allowing them to add and remove accessories, scenes, and even additional users in the shared home, but cannot remove homeowners or edit their permissions.

Overall, most systems we reviewed allow the shared user full access, providing them with unrestricted control over shared smart home devices. Yet, granting unrestricted full access to shared users may result in unintended modifications to the system, compromising reliability and security. While convenient in emergencies, it can pose security risks if credentials are compromised, and some users may find the extensive control unnecessary.

Granular Access Control by Granting Shared Users Partial Access by Device, Property, and User Role. Along with full access, we found that many systems provided features in smart home management systems to support more granular access control by granting shared users partial access including device-level control, property-level control, and role-based access.

Device-Level Control. Several apps (n=6) offer device-level control in which homeowners can specify access rights at the device level for shared users. For instance, in the SmartThings app (Fig. 1b), homeowners can grant shared users access to specific smart home devices, such as lights, thermostats, or security cameras, while restricting access to others. This granular control enables homeowners to tailor access permissions based on the specific needs and preferences of each shared user, enhancing security and privacy within the smart home environment.

Property-Level Control. Two systems offer homeowners the capability to share specific attributes or properties of a smart device with shared users, allowing for fine-grained access control. For example, in the Philips Hue app, homeowners can share access with shared users to change the brightness level of a smart light or the color scene associated with a particular bulb. This granularity of shared access at the property level ensures that homeowners have more precise oversight over the functionality and capabilities shared with shared users, promoting a more secure and customized smart home environment.

Partial Access with Role-based Access. Several smart home systems (n=7), including August app (Fig. 1a), provide homeowners with the flexibility to grant role-based access to shared users, allowing them to define specific privileges. For example, the Home Assistant platform provides a "User" role with limited interaction capabilities and an "Administrator" role. Overall, role-based controls allow homeowners to grant predefined permissions for shared users. However, this approach can introduce complexity and confusion, as homeowners must manage different roles and permissions. Moreover, reliance on role-based access may lead to unintended consequences or security vulnerabilities if not carefully managed. Clear communication and robust security measures are crucial to prevent unintended access or security breaches.

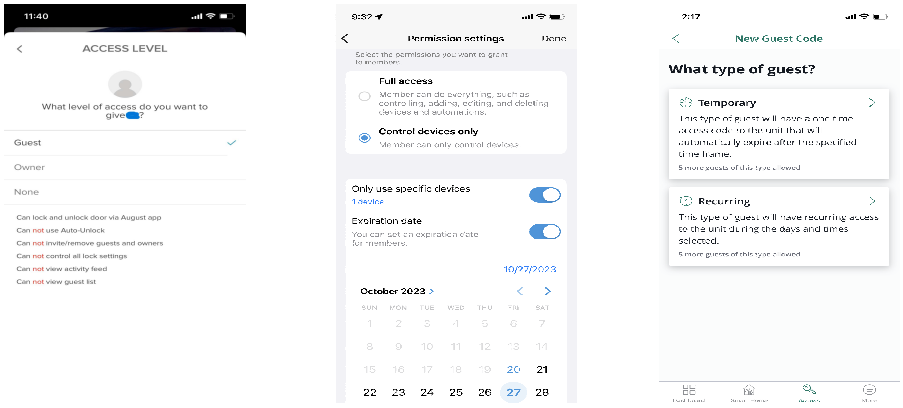
In summary, we noted variations in granting shared users varying levels of access control in smart home systems, including device-level control, property-level control, and role-based access. This variation reflects efforts to provide homeowners with more granular control over shared user permissions, enhancing security and customization in smart home environments. However, the complexity that can be introduced by role-based access underscores the importance of clear communication and robust security measures to mitigate potential risks and ensure a seamless user experience.

Restricting Shared Users Access with Temporary Access Settings. We also observed features in our reviewed smart home management systems to restrict shared users' access with temporary access settings such as time-based control and entry/access code.

Time-Based Control. Some apps (n=4) support time-based access controls. This functionality empowers homeowners to set schedules or expiration dates for shared user access to the different smart home devices. For instance, the Yale app provide homeowners with a more comprehensive suite of options, enabling them to establish schedules for shared user access, with choices like "Always", "Recurring", or "Temporary" access. For the SmartRent app, the homeowner can provide a shared user with a recurring access code during the days and times selected. These time-based access control features empower homeowners to manage access periods, reducing the risk of unauthorized use and ensuring that access is only granted when needed. Overall, time-based access control features can provide a flexible and proactive approach to smart home security, aligning with the dynamic needs of homeowners and their shared users.

Entry/Access Code. Some apps (n=5), such as SmartRent (Fig. 1c), generate unique codes for shared users that expire after single or multiple uses to only access the smart door locks. It is also worth mentioning that, in the Ring app, a homeowner can provide a unique access code only for the security systems so that a shared user can arm and disarm the system using the Ring Alarm keypad. Overall, we observed a focus on temporary access settings, such as time-based controls and entry/access codes, enabling homeowners to specify access periods or create temporary codes for entry. Such approaches to restrict shared users' access with temporary access settings can enhance security by restricting access to authorized times or users, demonstrating a proactive stance in smart home security tailored to evolving needs.

Enabling Shared User Through Geofencing Control. Geofencing control for shared users allows for automated actions or restrictions on smart home devices based on the geographic location of authorized users' smartphones. This feature enhances security and convenience by enabling tailored device interactions depending on the user's physical proximity to the home or other predefined areas. We noticed that some systems provide geofencing control in smart



(a) (b) (c)

Fig. 1. Varied Access Control: (a) August; Nuanced access levels, (b) SmartThings; Flexible access levels, (c) SmartRent; Temproray access

home systems enabling personalized automation based on smartphone locations, enhancing flexibility. However, its availability to shared users varies, reflecting differing priorities in balancing security and usability.

Most systems (n=9) explicitly support geofencing features for both homeowners and shared users. These platforms allow for automation and controls based on the geographic location of users' smartphones, offering a high degree of flexibility and customization in managing home automation. For example, in the Apple Home app, homeowners can enable the shared user to control the shared devices remotely or just within the local network. Thus, when remote access is activated, shared users can control accessories, see when they are being used, and receive notifications while not at home. Conversely, the Ring app offers geofencing capabilities with some limitations. It provides geofencing for reminders, which might not directly control devices but still enhances security through user location awareness. The remaining apps (n=3) have limited support for geofencing among shared users, suggesting a primary focus on homeowner control for their geofencing features. This indicates a more restricted use of geofencing, prioritizing direct user control and security considerations over broader shared access. The absence of geofencing controls for shared users in smart home apps presents both benefits and drawbacks. On the one hand, not extending geofencing features to shared users enhances security and privacy by limiting their ability to control devices based on the homeowner's location. On the other hand, shared users may not have the ability of automated device control based on their proximity to the home, potentially reducing the overall user experience and convenience, especially for tasks like adjusting temperature or lighting upon arrival.

Overall, smart home management systems provide varying access control ranging from extensive to minimal control to support flexibility. Full control access allows shared users, like those residing outside the home, to operate all smart home device functions, offering convenience and flexibility but potentially compromising security and privacy, as shared users gain unrestricted access to all aspects of the smart home system. On the other hand, minimal control, often device-based access or time-based access, limits shared users to specific devices or timeframes, enhancing security but possibly reducing the functionality and convenience for shared users. The balancing act between full and minimal control in smart home systems remains a nuanced challenge, weighing seamless convenience against potential security vulnerabilities.

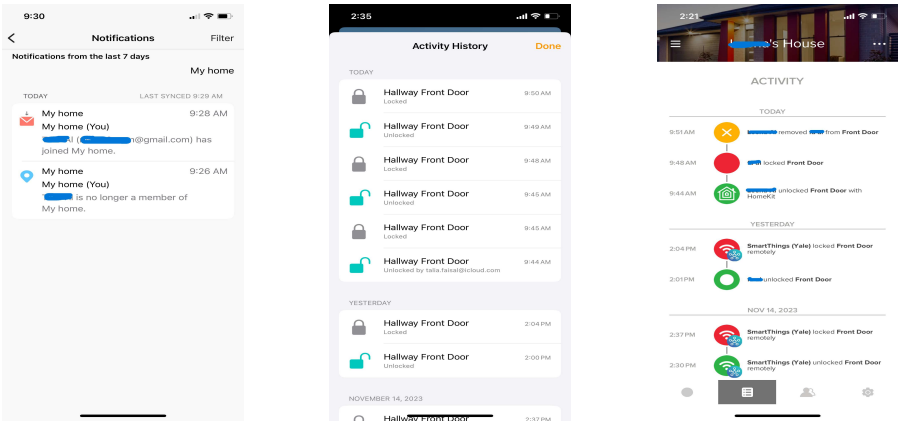
4.3 Privacy-aware Management of Shared Users' Activities and Access (RQ3)

Enhancing Transparency through Shared Users' Activity Logs. We observed that features to log shared users' activities vary across smart home systems ranging from comprehensive logs detailing device actions taken by shared users to no or minimal activity logs.

Comprehensive Activity Logs. We observed that most smart home systems (n=8) document detailed activity logs of shared users, with five apps including SmartThings (Fig. 2a), offer logs that detail the device, date, time, and actions taken by shared users, enhancing transparency and security. These logs, accessible to shared users, foster trust but could potentially reveal sensitive homeowner information. Conversely, August and Yale apps (Fig. 2c) go a step further by offering advanced log details like whether the activity is remote and user changes. However, it restricts shared user access to these logs, prioritizing homeowner privacy and minimizing complexity for shared users. The Home Assistant platform introduces customizable logging through include and exclude filters, allowing homeowners to tailor log entries to their preferences, thus, offering a balance between detailed oversight and privacy.

Minimal or No Activity Logs. Some apps (n=5) provide limited or no activity logs to streamline user interfaces. For instance, the Apple Home app (Fig. 2b) focuses logs on security devices such as door locks, and security cameras, and the SmartRent app tracks only homeowner actions, omitting shared user activities, which could reduce visibility into shared user interactions. The Philips Hue app offers no activity logs, which simplifies the experience but may compromise transparency. Additionally, in systems like Amazon Alexa and IFTTT, where accessing shared devices is via logging into the homeowner's account, distinguishing shared users' actions in logs can be challenging, potentially limiting transparency and accountability in device usage.

As such, the majority of smart home systems we reviewed provide options to log comprehensive activities of shared users, which contributes to enhancing transparency. At the same time, giving access to shared users with advanced



(a) (b) (c)

Fig. 2. Activity logs types: (a) SmartThings; detailed device logs, (b) Apple Home; security devices logs, (c) August & Yale; detailed activity logs

log details may raise privacy concerns for homeowners. Conversely, some systems provide minimal or no activity logs to streamline interfaces, potentially compromising transparency but simplifying the user experience.

Effectively Responding to Changes by Revoking Shared User Access. The capacity to revoke shared users' access effectively is crucial for maintaining privacy, security, and operational flexibility. This capability varies significantly across different systems, with some offering more granular control over access than others. Below, we provide details of these features, arranged from the least to the most control and flexibility.

Access Expiry. Initiating with the most basic form of control, we found that some smart home systems (n=4), including SmartThings, August, Yale, and SmartRent provide homeowners with the option to set an expiry date for access. This feature automates the revocation process, ensuring access is time-limited but lacks the granularity for device-specific management.

Full Access Revocation. Advancing in control, a large portion of smart home systems (n=10) empower homeowners to revoke full access from shared users. This approach allows for the swift termination of all device access, aligning well with immediate privacy and security concerns but does not cater to nuanced access needs. In the Home Assistant platform, homeowners also can revoke the shared users' access by removing their accounts or deactivating (temporarily suspending) the "Guest Mode Automation." The ability to revoke shared users' access quickly underscores the flexibility and responsiveness of these systems in meeting evolving needs and ensuring a secure smart home ecosystem.

Guest-Initiated Revocation. Further enhancing flexibility, several smart home systems (n=6) like SmartThings, Apple Home, Google Home, Arlo, Wyze, and Philips Hue offer features of allowing shared users to revoke their access. This not only grants shared users more autonomy but also alleviates some of the administrative burdens from homeowners, marking a step towards more user-centric access control mechanisms.

Device-Level Revocation. At the highest level of control and flexibility, a few systems (n=5), including the Home Assistant platform and apps like SmartThings, Arlo, Ring, and Wyze provide device-level revocation, allowing homeowners to selectively control access to specific devices. This feature offers fine-grained access control, essential for nuanced management of smart home security, though it could lead to increased complexity and possible user confusion.

In summary, our analysis revealed that a few systems only offer full access revocation and access expiry features. While these options enhance security by terminating access in time, they may limit homeowner control and shared user autonomy. An evolving trend we observed was the advanced security and flexibility by offering features to revoke access of shared users via temporary access expiry, guest-initiated revocation, and device-level revocation. This trend emphasizes fine-grained access control in smart home systems, enabling homeowners to customize security measures while managing access complexity.

5 Discussion

In this section, we discuss the implications of our findings and propose design recommendations aimed at bridging these gaps, offering a pathway to more user-centric and flexible sharing of smart home devices.

5.1 Potential Challenges in Current Smart Home Management Systems

Complexity and Rigidity of Sharing Smart Home Devices. Our study highlighted the intricate process of setting up and managing shared access within smart home systems, with some systems having limited sharing options or requiring users to navigate through multiple menus to set up shared access. Yet, such a process can pose challenges including the complexity and rigidity of access-sharing processes and the limited granularity of control available to users, which are documented in prior work [29]. Moreover, our findings revealed a prevalent trend towards centralized control, which could offer advantages to users while potentially introducing complexity, particularly evident in its inherent complexity in the requirement for shared users to install the same app as the homeowner and the homeowner's initiation of access. Prior research has emphasized the importance of centralized control for ensuring secure and manageable smart home environments [57]. Therefore, we suggested that the necessity for shared users to

utilize the same app as the homeowner, while promoting a cohesive access environment, may also lead to increased complexity and potential vulnerabilities due to centralizing access points ([7,57]). Additionally, our study identifies hardware dependencies, such as hubs, as another potential challenge in smart home management systems. While cloud-based platforms offer convenience for remote access, the reliance on specific hardware components may introduce barriers for users [41], hence, calling for the balance between functionality and user burden in smart home ecosystems.

Limited Granularity of Controls. We found that one common feature across various smart home systems when sharing smart home devices is the granting of full access to shared users. This lack of granularity in basic permission settings restricts users to broad access levels, without the ability to fine-tune permissions based on specific contexts or device functionalities. These limitations can pose significant challenges, particularly regarding privacy and security concerns. We suggested that this feature may inadvertently discourage users from sharing their devices due to the associated security risks. This is consistent with the studies that investigated the sharing of smart devices with other people and identified privacy and security challenges [26,32] as factors that influence the decision whether to share smart devices or not. Consequently, smart homeowners may either grant excessive access or avoid sharing devices altogether, resulting in underutilization or potential privacy and security risks.

Lack of Transparency. We found that some smart home systems excel in transparency, explicitly highlighting shared users' activity, including device details, actions, and time. However, others prioritize simplicity, potentially compromising visibility into shared user interactions by lacking comprehensive logs or real-time notifications. Consequently, this lack of transparency may lead to issues and leave homeowners unaware of who has access to their devices and how they are being utilized. This finding aligns with prior work by O'Connor et al., who emphasized the lack of transparency in monitoring shared user access and activities as a significant concern in smart home device sharing [59]. Therefore, enhancing transparency in monitoring shared user access and activities remains a critical area for improvement, ensuring homeowners have full visibility and control over their devices to foster a secure and trusted sharing environment.

5.2 Gaps between User Expectations and Current Features in Smart Home Management Systems

Granularity of Access Controls. Our findings revealed a significant gap between user expectations and the functionalities offered by current smart home systems, particularly in terms of access control. Previous research indicated a strong user preference for device-sharing features that offer granular control over access permissions, allowing device owners to specify who can access their devices, which devices they can access, and under what conditions [24,27,28]. This

preference is reflected in certain smart home systems that provide granularity in access controls, allowing homeowners to define access permissions at an individual device level. However, despite the demand for these advanced features, their availability remains limited, with many systems offering only basic sharing functionalities. For example, role-based access in some smart home systems lacks the flexibility for customization, as they adhere to predefined sets of permissions. This limitation may restrict homeowners from tailoring access rights to specific needs or preferences, potentially requiring careful management to avoid confusion or unintentional access granting. Additionally, the Apple Home provides granular access control through both full access and role-based access control, providing users with comprehensive control over shared smart home devices and a nuanced approach to access management. However, its limitation lies in being primarily designed for Apple users, potentially posing challenges in mixed-device environments. Such limitations may not only hinder the practical utility of smart home device sharing but also raise concerns regarding privacy and security. In conclusion, the existing gap between user needs for sophisticated and granular access control mechanisms and the solutions currently available in the market highlights a critical area for improvement.

Empowering Shared User Autonomy. We discovered that the presence of the guest-initiated revocation feature in apps may contribute to enhancing the guest experience. This feature could empower shared users by granting them autonomy to manage their access, thereby reducing the burden on homeowners. This aligns with the fact that shared user needs in smart home device sharing go beyond mere access to devices; they entail a desire for autonomy and control over their interactions within the smart home environment [58]. Research suggests that shared users seek empowerment through tailored access permissions and personalized device settings [60]. Marikyan et al. [58] also highlighted the psychological benefit of such autonomy, noting an increase in user satisfaction and perceived control over their smart home environments. However, the limited availability of features that empower shared user autonomy is evident in current smart home systems. For instance, while some systems like Ring and Google Home have introduced guest-initiated access features, these advancements remain sparse and not widely adopted. Moreover, our findings suggest that while centralized control mechanisms in smart home systems prioritize security, they may inadvertently constrain user autonomy by limiting shared users' ability to initiate or request access. Therefore, further research and development efforts are needed to prioritize features that promote shared user autonomy and enhance their overall experience in smart home device sharing.

Users' Needs for Convenience and Security. Prior research on smart home device sharing indicated that users require a seamless experience that prioritizes both convenience and security [40,39]. On one hand, users seek the convenience of effortlessly sharing access to smart devices with others, streamlining daily routines, and enhancing collaborative experiences within shared living spaces.

On the other hand, users are equally concerned about safeguarding their privacy, data, and the integrity of their smart home systems against potential security breaches or unauthorized access [26,32,28]. Yet, the current state of smart home systems revealed significant variations in the availability of features to meet the dual needs of convenience and security. For instance, while simple access control mechanisms found in some systems may improve usability, they could compromise security. On the other hand, complex access control in the other systems may deter users or cause confusion. This narrative is consistent with the broader discourse in smart home device sharing, as highlighted by prior research, underscoring the complexity of balancing between ease of access and the necessity of safeguarding privacy and security [7,24]. Accordingly, bridging the gap between convenience and security in smart home device sharing remains a significant challenge, urging developers and researchers to innovate solutions that can meet user interconnected needs.

5.3 Implications for Designing Smart Home Systems for External Sharing

Implementing Decentralized Privacy Management in Smart Home Systems. Our analysis underscored the importance of integrating robust privacy measures in smart home management systems. Decentralized privacy management emerged as a promising solution, distributing control over user data to enhance security and ensure privacy by design [65]. Therefore, our study advocates for next-generation privacy enhancements like homomorphic encryption and blockchain technology in decentralized privacy management. These advancements significantly bolster user data protection, embedding privacy by design for a secure sharing environment. Incorporating such technologies into smart home systems may mark a novel contribution, ensuring a personalized yet secure sharing experience beyond traditional measures [61,63].

Adaptive Access Management with Context-Aware Security. Developing a smart home system that adapts to varying user relationships and sharing contexts requires an innovative approach to access management [24]. Therefore, we suggested an integration of AI and machine learning algorithms, the system can dynamically adjust access controls in real-time based on the context of sharing, user behavior, and predefined privacy settings. This adaptive approach, utilizing environmental and behavioral sensors, ensures alignment with homeowner intentions and external user needs [63]. Additionally, incorporating context-aware security measures can preemptively identify and mitigate potential security risks, providing a seamless yet secure sharing experience.

Collaborative Communication and System Adaptability Interface. To enhance communication between homeowners and shared users, we suggest developing a collaborative communication feature and a system adaptability interface within smart home systems. These interfaces would facilitate real-time

notifications, customizable permission requests, and transparent sharing policies. Additionally, we highlighted the need for an adaptable system interface that learns from user interactions and feedback to optimize usability and functionality over time. Incorporating natural language processing and visual cues would ensure effective participation in the sharing process by both tech-savvy and non-technical users [62,64].

By focusing on these interconnected design considerations, developers can create smart home systems that not only meet the technical requirements of security and privacy but also enhance the user experience through adaptability, proactive communication, and a deep understanding of user needs. This holistic approach aims to redefine the standards for external sharing in smart homes, making it more intuitive, secure, and aligned with the evolving dynamics of digital living spaces.

5.4 Limitations and Future Work

Our study has some limitations. First, we restricted our analysis to systems that were freely available for download via Android or iOS platforms. Therefore, our list of systems is only a representative sample, and not by any means, exhaustive. Future work could still extend our results by conducting a more in-depth feature analysis of the paid features in some systems. Further, we did not directly engage with any of the key stakeholders in the smart home co-management space. Future research can interact with systems designers to better understand their motivations, and subsequently, the values they implicitly or explicitly chose to embed in their apps. It is also imperative that future research includes more user studies involving homeowners and shared users. Engaging directly with users would provide invaluable insights to help researchers and designers identify commonly shared devices and permissions between homeowners and shared users, pinpointing potential conflicts, and, most importantly, discovering areas to support both homeowners and shared users.

6 Conclusion

As smart devices become commonplace in homes, understanding how current smart home management systems support device sharing is crucial. We analyzed 11 Android and iOS mobile applications ("apps") and two open-source platforms for smart home management systems, focusing on the co-management features in these systems. Our findings highlighted that most systems use a centralized control mechanism, requiring shared users to access devices through the same app or a web interface. We observed diverse authentication methods, including account-based and phone number verification, balancing accessibility and security. Additionally, we discovered that access control mechanisms vary, from full access to granular controls, requiring careful management to avoid user confusion. Finally, for the shared user access revocation, we found multiple methods such as full access revocation, device-level revocation, and access expiry features,

which can provide flexibility and security. Based on our findings, we proposed design recommendations for smart home device-sharing systems, prioritizing robust privacy measures, context-aware security, and enhanced transparency to improve user experience in securely sharing smart home devices.

Acknowledgments

This research was supported by the U.S. National Science Foundation under grants CNS-1814068, CNS-1814110, and CNS-2326901. Any opinions, findings, conclusions, or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the U.S. National Science Foundation.

References

1. Amazon.com: Echo Smart Speakers & Displays: Amazon Devices & Accessories: Smart Speakers, Smart Displays & More. (2023). Retrieved from https://www.amazon.com/b?&node=9818047011&ref=ODS_v2_FS_AUCC_category
2. Your Smart Home Starts With SmartThings — SmartThings. (2023). Retrieved from https://www.smartthings.com/
3. Cecchinato, M. E., & Harrison, D. (2023). Degrees of Agency in Owners & Users of Home IoT Devices.
4. Lau, J., Zimmerman, B., & Schaub, F. (2018, November). Alexa, Are You Listening? Privacy Perceptions, Concerns and Privacy-seeking Behaviors with Smart Speakers. *Proceedings of the ACM on Human-Computer Interaction*, 2(CSCW), 102:1–102:31. https://doi.org/10.1145/3274371
5. Multiple users - can they all see each other? - Apps & Clients. (2017, October). SmartThings Community. Retrieved from https://community.smartthings.com/t/multiple-users-can-they-all-see-each-other/102723?page=3
6. Mennicken, S., & Huang, E. M. (2012). Hacking the Natural Habitat: An In-the-Wild Study of Smart Homes, Their Development, and the People Who Live in Them. In J. Kay, P. Lukowicz, H. Tokuda, P. Olivier, & A. Krüger (Eds.), *Pervasive Computing* (pp. 143–160). Berlin, Heidelberg: Springer. https://doi.org/10.1007/978-3-642-31205-2_10
7. E. Zeng, S. Mare, and F. Roesner, *End User Security & Privacy Concerns with Smart Homes*, Year 2017.
8. Weijia, H., Golla, M., Padhi, R., Ofek, J., Dürmuth, M., Fernandes, E., & Ur, B. (2018, January). Rethinking Access Control and Authentication for the Home Internet of Things (IoT). Proceedings of the 27th USENIX Security Symposium. Retrieved from https://par.nsf.gov/biblio/10095905-rethinking-access-control-authentication-home-internet-things-iot
9. No Author. *The best home automation systems of 2023*, 2023. [Online]. Available: https://www.zdnet.com/home-and-office/smart-home/best-home-automation-system/.
10. No Author. *SmartRent Review: Revolutionizing Property Management*. [Online]. Available: https://www.swiftlane.com/blog/smartrent-review/.

11. No Author. *Best home automation systems of 2023*. [Online]. Available: https://www.techradar.com/best/best-home-automation-systems.
12. Amelia Brooks. *14 Unbelievable Home Automation Hubs For 2023*. [Online]. Available: https://storables.com/articles/14-unbelievable-home-automation-hubs-for-2023/.
13. John Carlsen and Luke Edwards (updated). *Best home automation systems 2023*, January 2021. [Online]. Available: https://www.toptenreviews.com/best-home-automation-systems.
14. No Author. *Best Smart Locks of 2023*. [Online]. Available: https://www.cnet.com/home/security/best-smart-locks/.
15. No Author. *Best Video Doorbell Cameras of 2023 - CNET*. [Online]. Available: https://www.cnet.com/home/security/best-video-doorbell-cameras/.
16. No Author. *What's the Best Way to Brighten Up a Room? Easy, Smart Lights*. [Online]. Available: https://www.cnet.com/home/kitchen-and-household/best-smart-lights/.
17. No Author. *Best Home Security System of 2023*. [Online]. Available: https://www.cnet.com/home/security/best-home-security-system/.
18. No Author. *Best Home Security Camera of 2023*. [Online]. Available: https://www.cnet.com/home/security/best-home-security-camera/.
19. No Author. *Best Smart Speakers for 2023: We Tested Alexa, Google, Apple and Sonos*. [Online]. Available: https://www.cnet.com/home/smart-home/best-smart-speaker/.
20. No Author. *Smart Home Market Size, Share And Trends Report, 2030*, 2023. [Online]. Available: https://www.grandviewresearch.com/industry-analysis/smart-homes-industry.
21. Inc, Apple. *Apple Home*. [Online]. Available: https://developer.apple.com/apple-home/.
22. No Author. *Your Smart Home Starts With SmartThings — SmartThings*. [Online]. Available: https://www.smartthings.com/.
23. Zeng, Eric, and Franziska Roesner. *"Understanding and Improving Security and Privacy in Multi-User Smart Homes: A Design Exploration and In-Home User Study."* 2019, pp. 19. [Online]. Available: file://C:\Users\leena\Zotero\storage\QRIQXSDD\Zeng_and_Roesner_-_Understanding_and_Improving_Security_and_Privacy_i.pdf.
24. Tabassum, Madiha, Jess Kropczynski, Pamela Wisniewski, and Heather Richter Lipford. *"Smart Home Beyond the Home: A Case for Community-Based Access Control."* In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, New York, NY, USA, Apr. 2020, pp. 1–12. ISBN: 978-1-4503-6708-0. [Online]. Available: https://doi.org/10.1145/3313831.3376255.
25. Balakrishnan, Sumathi, Hemalata Vasudavan, and Raja Kumar Murugesan. *"Smart Home Technologies: A Preliminary Review."* In *Proceedings of the 6th International Conference on Information Technology: IoT and Smart City*, ICIT '18, New York, NY, USA, Dec. 2018, pp. 120–127. ISBN: 978-1-4503-6629-8. [Online]. Available: https://doi.org/10.1145/3301551.3301575.
26. Brush, A.J. *"It's Used by Us: Family Friendly Access Control."* Presented at the Microsoft Research, Aug. 2012. [Online]. Available: https://www.microsoft.com/en-us/research/publication/its-used-by-us-family-friendly-access-control/.
27. Jha, Abhiditya, Jess Kropczynski, Heather Richter Lipford, and Pamela J Wisniewski. *An Exploration on Sharing Smart Home Devices Beyond the Home*. IUI Workshops, 2019.

28. Alghamdi, Leena, Mamtaj Akter, Jess Kropczynski, Pamela J Wisniewski, and Heather Lipford. *Co-designing Community-based Sharing of Smarthome Devices for the Purpose of Co-monitoring In-home Emergencies*. Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems.
29. Sikder, Amit Kumar, Leonardo Babun, Z Berkay Celik, Hidayet Aksu, Patrick McDaniel, Engin Kirda, and A Selcuk Uluagac. *Who's controlling my device? Multi-user multi-device-aware access control system for shared smart home environment*. ACM Transactions on Internet of Things, vol. 3, no. 4, 2022.
30. Sikder, Amit Kumar, Leonardo Babun, Z. Berkay Celik, Abbas Acar, Hidayet Aksu, Patrick McDaniel, Engin Kirda, and A. Selcuk Uluagac. *KRATOS: Multi-User Multi-Device-Aware Access Control System for the Smart Home*. [Online]. Available: http://arxiv.org/abs/1911.10186.
31. Matthews, Tara, Kerwell Liao, Anna Turner, Marianne Berkovich, Robert Reeder, and Sunny Consolvo. *"'She'll Just Grab Any Device That's Closer': A Study of Everyday Device & Account Sharing in Households."* In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, San Jose California USA, May 2016, pp. 5921–5932. ISBN: 978-1-4503-3362-7. [Online]. Available: https://dl.acm.org/doi/10.1145/2858036.2858051.
32. Jang, William, Adil Chhabra, and Aarathi Prasad. *Enabling Multi-user Controls in Smart Home Devices*. Nov. 2017. [Online]. Available: https://dl.acm.org/doi/10.1145/3139937.3139941.
33. Mohammad, Ziarmal Nazar et al. *Access control and authorization in smart homes: A survey*. Tsinghua Science and Technology, vol. 26, no. 6, Dec. 2021, pp. 906–917. [Online]. Available: https://ieeexplore.ieee.org/document/9449335.
34. Ur, Blase et al. *Intruders versus intrusiveness: teens' and parents' perspectives on home-entryway surveillance*. Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing, Sep. 2014, pp. 129–139. [Online]. Available: https://dl.acm.org/doi/10.1145/2632048.2632107.
35. *Thermostats, Locks and Lights: Digital Tools of Domestic Abuse*. 2018. [Online]. Available: https://vawnet.org/news/thermostats-locks-and-lights-digital-tools-domestic-abuse.
36. Karlson, Amy K., A.J. Bernheim Brush, and Stuart Schechter. *Can I Borrow Your Phone?: Understanding Concerns When Sharing Mobile Phones*. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Apr. 2009, pp. 1647–1650. [Online]. Available: https://dl.acm.org/doi/10.1145/1518701.1518953.
37. Seo, Eugene et al. *Preference and usability of Smart-Home services and items - A Focus on the Smart-Home living-lab*. Journal of Asian Architecture and Building Engineering, vol. 20, no. 6, Nov. 2021, pp. 650–662. [Online]. Available: https://doi.org/10.1080/13467581.2020.1812397.
38. Price, Chris. *Smart Home devices to exceed 13 billion by 2025*. Nov. 2020. [Online]. Available: https://www.techdigest.tv/2020/11/smart-home-devices-to-exceed-13-billion-by-2025.html.
39. Fernandes, Earlence, Jaeyeon Jung, and Atul Prakash. *"Security Analysis of Emerging Smart Home Applications."* In *2016 IEEE Symposium on Security and Privacy (SP)*, San Jose, California, USA, May 2016, pp. 636–654. [Online]. Available: https://ieeexplore.ieee.org/document/7546527.
40. Edu, Jide. *"Smart Home Personal Assistants: A Security and Privacy Review." ACM Computing Surveys*, vol. 53, Dec. 2020, pp. 116. [Online]. Available: file://C:\Users\leena\Zotero\storage\XS8GU9PA\Edu_-_2020_-_Smart_Home_Personal_Assistants_A_Security_and_Pri.pdf.

41. Zhou, Wei, Jian Xu, and Bin Wang. *"A Smart Home Foundation Scheme Based on Open Source Hardware and Cloud Computing."* International Journal of Internet Protocol Technology, Mar. 2017. [Online]. Available: https://www.inderscienceonline.com/doi/10.1504/IJIPT.2017.083032. Copyright © 2017 Inderscience Enterprises Ltd.
42. R. El-Azab, *Smart homes: potentials and challenges*, *Clean Energy*, vol. 5, no. 2, pp. 302–315, Jun. 2021. https://doi.org/10.1093/ce/zkab010
43. Home Assistant, *Home Assistant*, https://www.home-assistant.io/
44. Home, *App Store*, Apr. 2023. https://apps.apple.com/us/app/home/id1110145103
45. You've received an Alexa Link, https://alexa.amazon.com/?tag=zd-buy-button-20&ascsubtag=6b44d583690241daa9e73796111cd9d7%7C1c95d8d3-bd6f-412f-b4fa-826182825323%7Cdtp
46. *A home that knows how to help.* [Online]. Available: https://home.google.com/welcome/. [Accessed: Feb. 5, 2024].
47. Plans & Pricing, *IFTTT*, https://ifttt.com/plans
48. August App for Android and iPhone — August, https://august.com/pages/app
49. Yale Locks — Official Online Store, *Yale Home*, https://shopyalehome.com/
50. Wireless Smart Home HD Security Cameras, Lights and Doorbells — Arlo, https://www.arlo.com/en-us/
51. Welcome to the Ring App, *Ring Help*, https://support.help.ring.com/hc/en-us/articles/115005267846-Welcome-to-the-Ring-App
52. Wyze, https://www.wyze.com/
53. Resident App & Experience for Smart Home Management, https://smartrent.com/products/resident-app-and-experience/
54. Control lights with smart light apps, *Philips Hue US*, https://www.philips-hue.com/en-us/explore-hue/apps
55. R. Garg and C. Moreno, *Understanding Motivators, Constraints, and Practices of Sharing Internet of Things*, *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 3, no. 2, Jun. 2019.
56. 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*, New York, NY, USA, May 2019, pp. 1–13.
57. Lin, Huichen, and Neil W. Bergmann. *"IoT Privacy and Security Challenges for Smart Home Environments."* Information, vol. 7, no. 3, Sep. 2016, p. 44. [Online]. Available: https://www.mdpi.com/2078-2489/7/3/44. doi: 10.3390/info7030044.
58. Marikyan, Davit, et al. *"A systematic review of the smart home literature: A user perspective."* Technological Forecasting and Social Change, vol. 138, Jan. 2019, pp. 139–154. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0040162517315676.
59. OConnor, TJ, et al. *"HomeSnitch: behavior transparency and control for smart home IoT devices."* Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '19), May 2019, pp. 128–138. [Online]. Available: https://doi.org/10.1145/3317549.3323409.
60. Kanchi, Shravya, and Kamalakar Karlapalem. *"A Multi Perspective Access Control in a Smart Home."* Proceedings of the Eleventh ACM Conference on Data and Application Security and Privacy (CODASPY '21), Apr. 2021, pp. 321–323. [Online]. Available: https://doi.org/10.1145/3422337.3450324.
61. Sathish Kumar, G., et al. *"No more privacy Concern: A privacy-chain based homomorphic encryption scheme and statistical method for privacy preservation of user's private and sensitive data."* Expert Systems with Applications, vol. 234,

Dec. 2023, p. 121071. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0957417423015737.

62. Zheng, Song, et al. *"Combining a Multi-Agent System and Communication Middleware for Smart Home Control: A Universal Control Platform Architecture."* Sensors, vol. 17, no. 9, Sep. 2017, p. 2135. [Online]. Available: https://www.mdpi.com/1424-8220/17/9/2135.
63. Eliwa, Waleed. *"AI-Driven Smart Homes: Challenges and Opportunities."* Journal of Intelligent Systems and Internet of Things, vol. 8, Jan. 2023, pp. 54–62. [Online]. Available: https://doi.org/10.54216/JISIoT.080205.
64. Gellert, Edgar, and Matthias Böhmer. *"Collaborative Homes: Exchange of Learned Interaction Patterns to Support Networked Living."* [Online]. Available: https://www.semanticscholar.org/paper/Collaborative-Homes%3A-Exchange-of-Learned-Patterns-Gellert-B%C3%B6hmer/f2b7a8e4bf33a4c7e7a9983479d38127702152d0.
65. Mbarek, Bacem, et al. *"Blockchain-Based Access Control for IoT in Smart Home Systems."* Database and Expert Systems Applications, 2020, pp. 17–32. [Online]. Available: https://doi.org/10.1007/978-3-030-59051-2_2.

Appendices

A Connected Smart Home Devices to the Smart Home Systems

Table 1. Connected devices to the smart home management systems

App Name	Connected Smart Home Devices
SmartThings App	Ring Doorbell + Samsung Smart TV + Yale Door Lock + Sengled Light
Home Assistant Platform	Ring Doorbell + Ring Security System + Yale Door Lock + GoControl Light
Apple Home App	Apple HomePod Mini + Yale Door Lock + Philips Hue Light
Amazon Alexa App	Ring Doorbell + Ring Security System + Yale Door Lock + Sengled Light
Google Home App	Blurams Cam + Google Home mini speaker + iRobot Vacuum + Yale Door Lock + Sengled Light + Wyze Cam v3
IFTTT Platform	Ring Doorbell + Blurams Cam
August App	Yale Door Lock
Yale App	Yale Door Lock
Arlo App	Arlo Cam
Ring App	Ring Doorbell + Ring Alarm System
Wyze App	Wyze Cam v3
Philips Hue App	Philips Hue Bridge + Philips Hue Light
SmartRent App	Honeywell Thermostat + Yale Door Lock + Alloy Smart Plug

B RQs Codebooks

Themes	Codes/Subcode	Apps/Systems
RQ1: What Methods Do Smart Home Management Systems Employ to Facilitate the Setup and Authentication of Shared Users' Access, and How Do These Systems Enable Remote Device Access for Shared Users?		
Facilitating Smart Home Device Sharing: The methods for granting access to smart devices, including app installation requirements, access initiation, and various sharing methods.	**Accessing Shared Devices:**	
	Utilizing the Primary App/ Web-interface **(n=12, 92),**	SmartThings, Home Assistant, Apple Home, Amazon Alexa, Google Home, IFTTT, August, Yale, Arlo, Ring, Philips Hue, Wyze
	Primary App Not Required **(n=1, 8%)**	SmartRent
	Access Initiation:	
	Access-Initiation by a Homeowner **(n=13, 100%)**	SmartThings, Home Assistant, Apple Home, Amazon Alexa, Google Home, IFTTT, August, Yale, Arlo, Ring, Philips Hue, Wyze, SmartRent
	Access-Initiation by a Shared User **(n=2, 15%)**	Google Home, Ring
	Sharing Methods:	
	Email Invitations **(n=6, 46%)**	SmartThings, Apple Home, Google Home, Arlo, Ring, Wyze
	Temporary/Unique Entry Code **(n=4, 31%)**	SmartThings, August, Yale, SmartRent
	Invitation via Phone Number **(n=2, 15%)**	August, Yale
	Invitation Link with Expiration **(n=2, 15%)**	SmartThings, Philips Hue
	Sharing via QR Code **(n=1, 8%)**	SmartThings
	Direct Account Sharing **(n=3, 23%)**	Home Assistant, Amazon Alexa, IFTTT
Enhancing Accessibility and Security in Smart Home Devices Sharing: Different practices for shared user authentication and diversity in interface options and network connectivity for remote access.	**Shared Users Authentication Methods:**	
	Account-based Authentication **(n=4, 31%)**	SmartThings, Apple Home, Amazon Alexa, Google Home
	Phone Number Verification **(n=2, 15%)**	August, Yale
	Two-step Verification **(n=2, 15%)**	Ring, Arlo
	OAuth Secure Connections **(n=3, 23%)**	Philips Hue, Home Assistant, IFTTT
	Two-factor Authentication (2FA) **(n=1,8%)**	Wyze
	Interface Type & Network Connectivity:	
	Mobile/Web-based, and Cloud-based **(n=6, 46%)**	SmartThings, Google Home, IFTTT, Arlo, Ring, Wyze,
	Mobile/Web-based, and Hub-based **(n=2, 15%)**	Home Assistant, SmartRent
	Mobile, and Hub-based **(n=4, 31%)**	Apple Home, August, Yale, Philips Hue
	Mobile, and Cloud-based **(n=1, 8%)**	Amazon Alexa

Themes	Codes	Apps/Systems
RQ2: What Access Control Mechanisms Are Currently Employed in Smart Home Management Systems When Sharing Smart Home Devices with Individuals Residing Outside the Home?		
Empowering Shared Users with Full Access: Shared users have full access, including editing settings and adding/removing devices and people.	Full Access by Default **(n=3, 23%)**	Google Home, Amazon Alexa, IFTTT
	Full Access with Role-based Access (Predefined Permissions) **(n=4, 31%)**	Home Assistant, Philips Hue, August, Yale
	Homeowner-Granted Full Access **(n=3, 23%)**	SmartThings, Arlo, Apple Home
Granting Shared Users Partial Access: Homeowners can customize access for shared users by specifying device-level rights, sharing specific device attributes, or implementing role-based access control	Device-Level Control **(n=6, 46%)**	SmartThings, August, Yale, Ring, Arlo, Wyze,
	Property-Level Control **(n=2, 15%)**	Philips Hue, Home Assistant
	Partial Access with Role-based Access (Predefined Permissions) **(n=7, 54%)**	Apple Hom
Restricting Shared User Access with Temporary Access Settings: The system enables homeowners to set schedules or expiration dates for shared user access or generates unique, and expiring codes.	Time-Based Control **(n=4, 31%)**	SmartThings, August, Yale, SmartRent
	Entry/Access Code **(n=5, 38%)**	SmartThings, August, Yale, SmartRent, Ring
Enabling Shared User Through Geofencing Control: The system enables automation and controls based on users' smartphone locations or offers geofencing for reminders.	Geofencing Control **(n=9, 69%)**	SmartThings, Home Assistant, Apple Home, Amazon Alexa, Google Home, IFTTT, August, Yale, Philips Hue
	Geofencing for Reminders **(n=1, 8%)**	Ring

Themes	Codes/Subcodes	Apps/Systems
RQ3: How Is Access Control Managed, Monitored, and Revoked for Shared Devices When Using Smart Home Management Systems?		
Privacy-aware Management of Shared Users **Logging:** The process of recording all actions taken by the shared users within the app, such as device control or settings changes, and the ability to remove a shared user's access from the smart home system	**Shared Users' Activities:**	
	Comprehensive Activity Logs **(n=8, 62%)**	SmartThings, Home Assistant, Google Home, August, Yale, Arlo, Ring, Wyze
	Minimal or No Activity Logs **(n=5, 38%)**	Apple Home, Amazon Alexa, IFTTT, Philips Hue, SmartRent
	Removing Guest Access:	
	Full Access Revocation **(n=11, 85%)**	SmartThings, Home Assistant, Google Home, IFTTT, August, Yale, Arlo, Ring, Wyze
	Device-Level Revocation **(n=5, 38%)**	SmartThings, Home Assistant, Arlo, Ring, Wyze
	Guest-initiated Revocation **(n=6, 46%)**	SmartThings, Apple Home, Google Home, Arlo, Wyze, and Philips Hue apps
	Access Expiry **(n=4, 31%)**	SmartThings, August, Yale, SmartRent