Mi Casa es Su Casa ("MiSu"): A Mobile App for Sharing Smart Home Devices with People Outside The Home

Leena Alghamdi
University of Central Florida
Orlando, Florida, USA
Leenaalghamdi@knights.ucf.edu

Mamtaj Akter
Vanderbilt University
Nashville, Tennessee, USA
Mamtaj.Akter@vanderbilt.edu

Cristobal Sepulveda Cardenas
University of Central Florida
Orlando, Florida, USA
Csepulveda7@knights.ucf.edu

Diego Cruces
University of Central Florida
Orlando, Florida, USA
Cruces@knights.ucf.edu

Jason Wiese
University of Utah
Salt Lake City, Utah, USA
Jason.Wiese@utah.edu

Jess Kropczynski
University of Cincinnati
Cincinnati, Ohio, USA
Jess.Kropczynski@uc.edu

Heather Lipford
University of North Carolina at Charlotte
Charlotte, North Carolina, USA
Heather.Lipford@uncc.edu

Pamela Wisniewski
Vanderbilt University
Nashville, Tennessee, USA
Pamela.Wisniewski@vanderbilt.edu

ABSTRACT

As smart devices are becoming commonplace in the home, people have begun sharing access to these devices with people beyond the home. However, the "all-or-nothing" approach to access control taken by most smart home applications may be insufficient for use cases that involve others outside of the home. Therefore, we developed "MiSu" an Android and iOS app that allows smart home homeowners to share their devices (e.g., Ring doorbell, security alarm, smart door lock, smart light bulb) with people outside of their home to control what, when, and how they can engage with the smart devices. MiSu provides options for fine-grain access control, the ability for guests to control smart homes using their own device and login, and provides homeowners real-time logs where they can view all actions taken by guests invited to interact with their smart homes.

CCS CONCEPTS

• **Human-centered computing** → **User interface programming**; **Interactive systems and tools**.

KEYWORDS

Access Control, Smart home, Mobile App Design

ACM Reference Format:
Leena Alghamdi, Mamtaj Akter, Cristobal Sepulveda Cardenas, Diego Cruces, Jason Wiese, Jess Kropczynski, Heather Lipford, and Pamela Wisniewski. 2022. Mi Casa es Su Casa ("MiSu"): A Mobile App for Sharing Smart Home Devices with People Outside The Home. In *Companion Computer Supported Cooperative Work and Social Computing (CSCW'22 Companion), November 8–22, 2022, Virtual Event, Taiwan.* ACM, New York, NY, USA, 4 pages. https://doi.org/10.1145/3500868.3559709

CSCW'22 Companion, November 8–22, 2022, Virtual Event, Taiwan

ACM ISBN 978-1-4503-9190-0/22/11.
https://doi.org/10.1145/3500868.3559709

1 INTRODUCTION

Smart home technologies are becoming increasingly popular around the world. At the end of 2018, almost 45 million smart home devices had been deployed in the United States alone [5]. There are many cases where a homeowner may need another person to have access to their smart devices, such as a pet-sitter or a housekeeper who may need the ability to lock and unlock an entrance at the home and needs access to smart devices such as speakers, lights, or a security alarm [10]. Previous studies explored the idea of sharing smart home devices beyond the home, whether users of these devices would be willing to share them or not, and what motivates the users to share such devices. For instance, early work by Jha et al. [8] found that most people are willing to share their devices, such as smart camera, security system and locks with family members and friends, and the most common reason was that they wanted to allow access to others for emergency situations and home monitoring in case no one is home. However, smart devices owners ultimately choose not to share access with people outside of their home even though such situations are ordinary. A large body of research suggested that security is the main reason they refuse to share devices [12, 13]. Moreover, there are still very few applications that allow users to securely share access to smart home devices with others, especially for specific periods of time or with specific restrictions [10]. Current applications that only offer an "all-or-nothing" access control approach are preventing a large number of smart device owners from fully utilizing their devices and limiting their convenience, which ultimately impact customer satisfaction [10].

1.1 Gaps within Existing Smart Home Device Sharing Methods

Existing smart home systems usually offer full access to all the devices connected to that system, or offer relatively limited multi-user functionality. In the case of SmartThings, for example, end users can provide many accounts but cannot yet grant them varied levels of information access [1]. Moreover, all-inclusive access approach allows any authorized user to control smart devices, potentially leading to conflicting demands, privacy violations, and unwanted app installation [6]. To solve this problem, some smart home devices allow users to share their devices in a controlled manner. For example, the Ring doorbell has a function that allows the owner to add a user to the device, giving them access to a range of predefined features [2]. Users of the Nest thermostat can add a family member, giving them full access to the device [3]. However, these solutions are device-specific, rather than being broadly applicable across the heterogeneous constellation of devices that make up smart home systems.

Since people's access control preferences for sharing digital devices in their households are generally complex [9, 11], several previous studies conducted among smart home users aimed to better understand user preferences and demands when sharing or managing their smart home devices [4, 7]. He et al. [12] discovered that even within a single device, smart home users needed different access control capabilities for different functionalities. They argue for more complicated access control policies that take into account stakeholder relationships, specific device capabilities, and various contexts such as time, device location, and people. Building on this insight, we decided that a mobile application with a customized access control could be a good way for smart-home-owners to share their devices with various secondary users beyond their homes.

Our main goal in building the MiSu app is to provide an easy-to-use solution for allowing homeowners with smart devices to share access with other people in a controlled and customizable environment to ensure users' privacy and security. The ability to set rules on restrictions is important for achieving the level of customizability a user might expect. MiSu implements many of the features suggested by prior research [8, 10], including, especially rules based on user, time, location and specific devices or permissions. These features afford the homeowner the ability to share their smart devices with others while also feeling secure about what features and data the secondary users have access to. Smart home devices such as Ring Neighborhood or August Smart Lock do not have the additional security features that MiSu provides, such as the ability to revoke or change permissions at any time, individually tailor access levels for different users, or see logs of any activity that users can perform. We expect that these security features will alleviate the major concerns that users have with sharing their devices.

2 MISU DESIGN OVERVIEW

MiSu is an Android and iOS mobile app that provides smart home owners with an interface to manage and share their devices with fine-grain access control, and provides an interface to secondary users to control devices that have been shared with them. MiSu's design enables feature-based access control, rather than all-or-nothing device-based access control, and provides smart-home-owners with the ability to set a schedule when giving access to others to explicitly decide when and where the guest can use these devices. For instance, homeowners can limit access to only being able to lock the front door after a specific time — instead of both lock and unlock, or even give access to use their front doorbell camera when they are more than a chosen distance away from their homes. MiSu includes other features that are not present in many other smart home apps: real-time device updates and logs, the ability to change or completely revoke a secondary user's access to a device. These features are designed to give homeowners even more peace-of-mind that they are in control of their smart homes, and their devices are always secure. MiSu's goal is to streamline the process of sharing smart devices with secondary users while keeping security at the forefront.

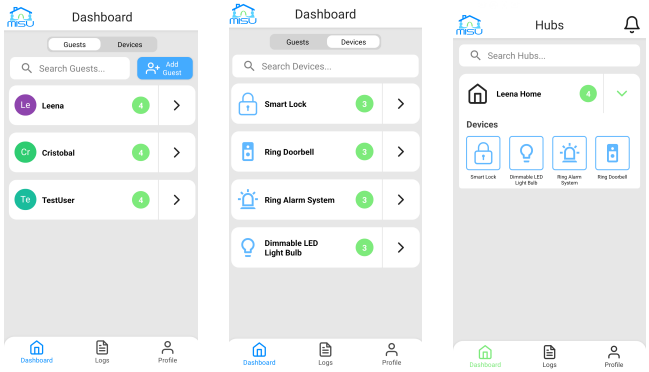
Below we describe the main screens and interface components that comprise MiSu.

2.1 Registration and On-boarding

The registration page leads new users through an on-boarding process to introduce the features that MiSu provides. The on-boarding process for both homeowners and guests has 3 stages - what the users can do with MiSu, how to set up the app, and an in-app tutorial familiarizing the user with the UI. On the login page, a user can use their MiSu account credentials to log in. MiSu uses Amazon Cognito to facilitate secure account creation and authentication.

2.2 Home Dashboard

The Home Dashboard screen is the first screen that opens after the app has loaded and the user has logged in. The Home Dashboard Screen is for both guests and homeowners; it combines the functionality of these two screens in one place and can toggle between "Guest" and "Device" views with a simple toggle button. The 'Home Dashboard Screen' for a homeowner user is shown in Figure 1.



(a) Guest Screen (Homeowner View) **(b) Devices Screen (Homeowner View)** **(c) Hubs Screen (Guest View)**

Figure 1: Home Dashboard Screens

2.3 Device Permissions Screen

The device permissions screen provides the main access control functionality of MiSu:

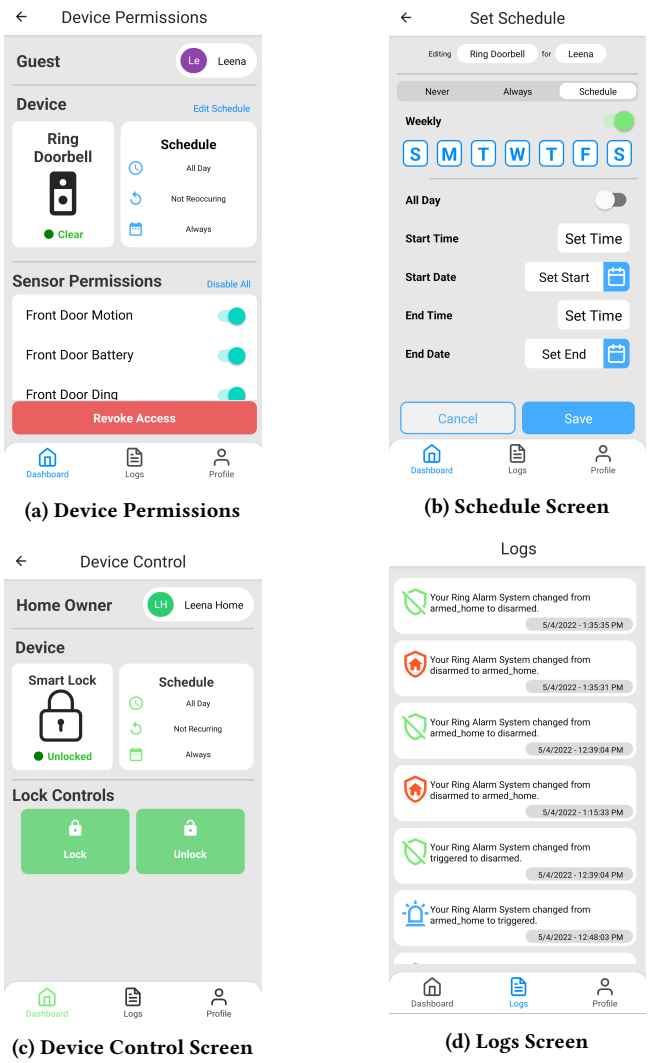
(1) Adding Guests and Devices: Homeowners can add devices and invite guests to their "hub".
(2) Schedule for Devices/Actions:Homeowners can see the specific guest/device pair they are setting a schedule for. They can also by default give someone permanent access, or set specific scheduling criteria, such as giving someone all day access or only during certain start time/end time, what days of the week they have access (Figure-2b).
(3) Toggle Device Action Permissions: Homeowners can toggle the specific actions of a device that they want a guest to have access to. For example, a homeowner can allow a guest to view the camera feed of a Ring Door Lock but restrict access to locking/unlocking the door (Figure-2a).
(4) Geofencing: Homeowners can restrict guests' access to their devices based on the homeowners' location. This would improve the security of one's devices and home since that guest with the permission to access the devices would not be able to control an owner's smart home when the owner is within the vicinity.

2.4 Device Control Screen

Figure-2c shows the device control screen and how it appears to a guest user. It has three different sections: Device, Controls and Sensors. The 'Device' section has the device's name, its icon, its state, as well as the schedule that reflects when the guest has access to the device's controls. The States section displays different states of the devices, for instance, unavailable state when a device is unplugged or not connected to Wi-Fi (Figure-2c).

2.5 Real-time Logs Screen

Homeowners can see all the logs regarding usage of devices on their hub, including when one of their devices was used and who used it. Homeowners can also see whenever a guest joins or leaves their hub. Guests can only see logs pertaining to devices and actions they have access to and only when they have access to it, they can also see when a homeowner updates their access/schedule (Figure-2d).



(a) Device Permissions
(b) Schedule Screen
(c) Device Control Screen
(d) Logs Screen

Figure 2: Device Permissions/Control Screens and Logs Screen

3 SYSTEM ARCHITECTURE

The MiSu app has a *React Native* front-end, *Amazon Web Services* back-end, and connects with *Home Assistant*, an open-source platform that allows users to connect many smart home devices, such as light bulbs and locks, to the app and control them in one central hub. The Home Assistant software can be hosted on a computer with minimal specifications, for example it runs on a Raspberry Pi. The MiSu App backend uses Amazon Web Services, including management and logging services, (e.g., AWS CloudWatch), and the backend connects directly to the Home Assistant API.

4 LIMITATIONS AND FUTURE WORK

The current version of MiSu has some limitations that are important to mention. First, much of the functionality and logic has already been implemented on the backend to handle brokering messages to users about their devices/guests. This is how we are able to show logs updating on the app in real-time. However, if a user is not currently running the app, they will not be made aware of these alerts/messages. Second, some minor features for logs were not fully implemented, specifically, users now are unable to filter their logs based on a device or a guest/homeowner.

As the inclusion of push notifications is crucial for the application to be fully complete, the future work will add the push notifications and some other filtering methods that can be added include filter by date/time (oldest to newest, etc.). Moreover, to understand the users' access control needs in sharing smart home devices with people outside the home, we will conduct a lab-based study where participants will interact with the app and express their opinion on different features and help determine how to improve it so that it can be useful for them.

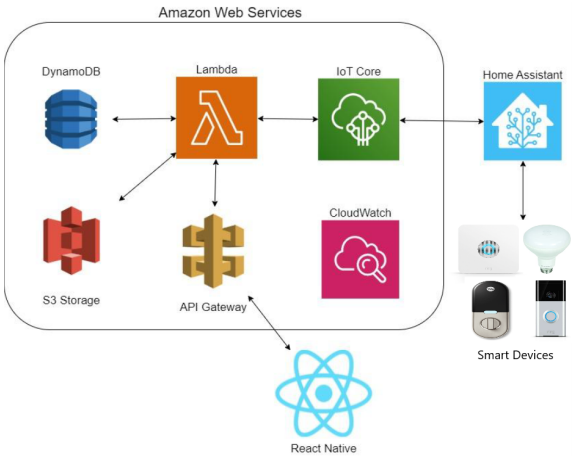


Figure 3: System Architecture Diagram

5 CONCLUSION

As smart devices move beyond early adopters and become more common in most homes, we must critically consider how these technologies are being used and shared by the individuals and their communities whom they trust. We believe that MiSu will yield new insight into how users with smart devices share access to those devices with users outside the home when given an intuitive interface that enables them to do so.

ACKNOWLEDGMENTS

We acknowledge the contributions of Scott Filetti, Kolbe Benner, Jeffrey Ramos, Nicholas Thiemann, and Kenley Rodriguez who contributed to the MiSu application development. This research was supported by Mozilla Research Grants and the U.S. National Science Foundation under grants CNS-1844881, CNS-1814068, CNS-1814110, and CNS-1814439. Any opinion, findings, and 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] 2017. Multiple users - can they all see each other? - Apps & Clients. https://community.smartthings.com/t/multiple-users-can-they-all-see-each-other/102723

[2] 2022. Controlling Ring devices through multiple smartphones or sharing control with other users. https://support.ring.com/hc/en-gb/articles/211018223-Controlling-Ring-devices-through-multiple-smartphones-or-sharing-control-with-other-users

[3] 2022. Learn about Family Accounts and how to share access to your Nest home - Android - Google Nest Help. https://support.google.com/googlenest/answer/9304271?hl=en&co=GENIE.Platform%3DAndroid

[4] Leena Alghamdi, Ashwaq Alsoubai, Mamtaj Akter, Faisal Alghamdi, and Pamela Wisniewski. 2022. A User Study to Evaluate a Web-Based Prototype for Smart Home Internet of Things Device Management. In *HCI for Cybersecurity, Privacy and Trust*, Abbas Moallem (Ed.). Springer International Publishing, Cham, 383–405.

[5] Michael Caccavale. 2018. Council Post: The Impact Of The Digital Revolution On The Smart Home Industry. https://www.forbes.com/sites/forbesagencycouncil/2018/09/24/the-impact-of-the-digital-revolution-on-the-smart-home-industry/ Section: Leadership.

[6] Geeng Christine and Roesner Franziska. 2019. Who's In Control?: Interactions In Multi-User Smart Homes. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. ACM, Glasgow Scotland Uk, 1–13. https://doi.org/10.1145/3290605.3300498

[7] Zeng Eric and Roesner Franziska. 2019. Understanding and improving security and privacy in multi-user smart homes: a design exploration and in-home user study. In *Proceedings of the 28th USENIX Conference on Security Symposium (SEC'19)*. USENIX Association, USA, 159–176.

[8] Abhiditya Jha, Jessica Kropczynski, H. Lipford, and P. Wisniewski. 2019. An Exploration on Sharing Smart Home Devices Beyond the Home. In *IUI Workshops*.

[9] Vassilios Lekakis, Yunus Basagalar, and P. Keleher. 2012. Don't Trust Your Roommate. https://www.semanticscholar.org/paper/Don%E2%80%99t-Trust-Your-Roommate-Lekakis-Basagalar/3e965f9265a1b99ae0ef13c003e140c5d3b3a915

[10] Tabassum Madiha, Kropczynski Jess, Wisniewski Pamela, and Lipford Heather Richter. 2020. 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*. ACM, Honolulu HI USA, 1–12. https://doi.org/10.1145/3313831.3376255

[11] Michelle L. Mazurek, J. P. Arsenault, Joanna Bresee, Nitin Gupta, Iulia Ion, Christina Johns, Daniel Lee, Yuan Liang, Jenny Olsen, Brandon Salmon, Richard Shay, Kami Vaniea, Lujo Bauer, Lorrie Faith Cranor, Gregory R. Ganger, and Michael K. Reiter. 2010. Access Control for Home Data Sharing: Attitudes, Needs and Practices. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (2010), 645–654. https://doi.org/10.1145/1753326.1753421 Publisher: ACM.

[12] He Weijia, Golla Maximilian, Padhi Roshni, Ofek Jordan, Dürmuth Markus, Fernandes Earlence, and Ur Blase. 2018. Rethinking Access Control and Authentication for the Home Internet of Things (IoT). *Proceedings of the 27th USENIX Security Symposium* (Jan. 2018). https://par.nsf.gov/biblio/10095905-rethinking-access-control-authentication-home-internet-things-iot

[13] Celik Z. Berkay, McDaniel Patrick, and Tan Gang. 2018. *Soteria: Automated IoT Safety and Security Analysis.*