Enhancing Physical and Cyber Security of Smart Homes using Co-Monitoring of IoT Devices

Dev Agrawal
Research Assistant
School of Information Technology
University of Cincinnati
agrawadv@mail.uc.edu

Rahul Bhagwat
Research Assistant
School of Information Technology
University of Cincinnati
agrawadv@mail.uc.edu

Rajdeep Bandopadhyay
Research Assistant
School of Information Technology
University of Cincinnati
agrawadv@mail.uc.edu

Vineela Kunapareddi
Research Assistant
School of Information Technology
University of Cincinnati

Jess Kropczynski, PhD
Assistant Professor
School of Information Technology
University of Cincinnati
jess.kropczynski@uc.edu

ABSTRACT

Devices in the Internet of Things (IoT) have enhanced our ability to automate functions in smart homes and increased our ability to monitor day to day activities regardless of whether we are in our home. Despite these benefits of IoT devices, it is the case that notifications about threats to our home when we are away are typically only sent to one or two people within the home. We proposed enhanced monitoring of threats by allowing temporary access to IoT devices to extended networks of homeowners in situations where primary IoT device owners are not able to address a smartphone notification quickly.

IT Research Symposium’19 Extended Abstracts, April 9, 2019, Cincinnati, Ohio, USA.

KEYWORDS

Internet of Things; Smart device; Smart home; Access control; Permission management; Authentication; Emergency situations; Privacy

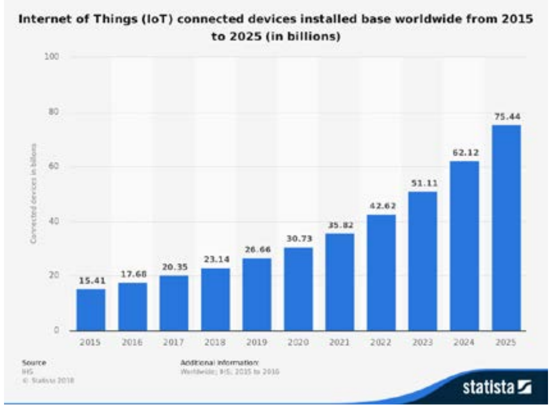


Fig. 1 Projected prominence of connected IoT devices over time. Source: [3]

INTRODUCTION

The assortment of various home Internet of Things (IoT) devices connected to and controllable through a single hub has long been termed a “smart home”. These smart homes are capable of home automation and enhanced monitoring, and are generally very secure and reliable. The affordances have led to an increased use of these devices over time (Fig 1). Previous research that falls into the domain of IoT security and privacy focuses on the cyber-threats and software vulnerabilities. Perhaps because this is the case, these devices are missing the capability to share temporary device access with others. Currently, smart homes are single-user entities with no secure access-control method built into them. This prevents users from collaborative access and monitoring of the house that was once a robust method of making sure your house or pet is safe while you are away.

We believe that the final missing piece of the truly “smart” smart homes is a flexible access-control system that is easy and intuitive to set up, and enables collaborative access and monitoring. The system should also be able to assist in situations where the residents are otherwise occupied. Our main focus is on emergency detection and notifications, and temporary emergency access for others in case the residents are away and otherwise occupied.

RESEARCH QUESTIONS

The major problem we are dealing with is the lack of access control and sharing capabilities in smart home applications. To solve this, we have posed five research questions that will help us to design and evaluate IoT hub infrastructure and supporting tools when answered. The following section describes these questions and the rationale to include each.

Since our main focus is studying the benefits of smart devices in the context of emergency situations, we first need to clearly define the term and study some instances, leading into our first question (RQ1) What qualifies as an emergency situation in the context of a residence?

Not every smart device can help us detect or deal with every emergency situation. This calls for another question: (RQ2) What category of smart devices can help in certain emergency situations?

To deal with the emergency situations effectively, we need to introduce the “human element” in the scenario. Previous research has examined the types of people and devices that IoT users might be willing to share access with [2]. We will extend this work by studying how the relationships between certain residents (for instance spouse, friends) translate in terms of sharing of access controls to their respective smart devices in particular situations, leading us to: (RQ3) How do residents share access to their respective smart devices with others to better address particular time of threats to the home?

Emergency situations are usually unforeseen, and the residents or others with full access may be otherwise occupied, rendering them unable to take appropriate action. This leads to the most important aspect of our research: (RQ4) Who are residents willing to give access to previously inaccessible devices in case of an emergency? Implementing the study results into working solutions will surely raise some red flags, which need to be taken into consideration: (RQ5) What are the best methods to implement said access control methods that do not compromise the security and privacy of the residents?

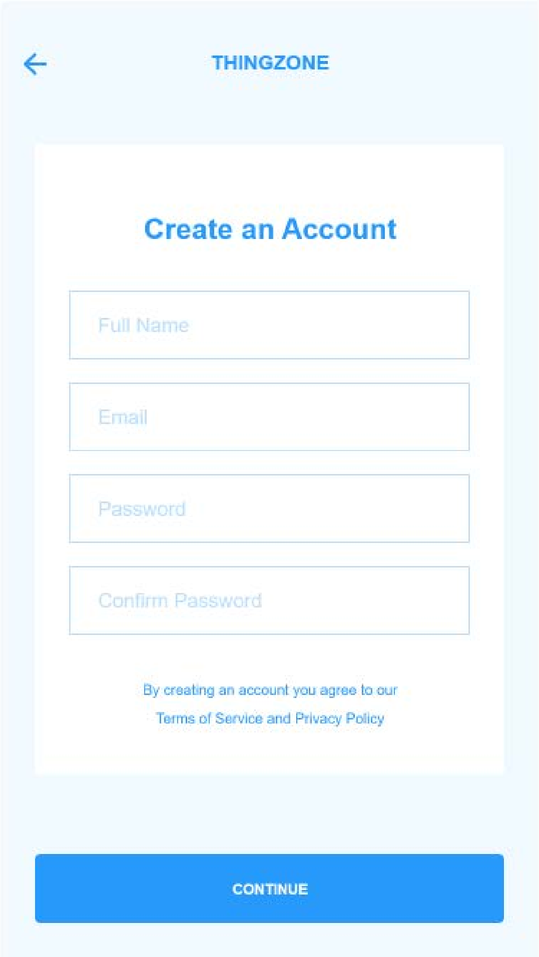
To answer these research questions we propose to design and test a prototype with potential users. The following sections will first describe the design and implementation of this prototype and the following section describes our proposed research methods.

DESIGN AND IMPLEMENTATION

One of the major focus of the projects is implementing a robust access control method into a smart home application, and use the implementation as a high-fidelity prototype, and then as a product to run alpha testing. Our initial approach was to integrate a simplified version of Role Based Access Control (RBAC) system which the smart home resident (administrator) can use to create roles and set permissions for them. But because an RBAC does not take temporary emergency access into consideration, the model was modified to integrate unpredictable circumstances into access control. We call the new model a Role and Situation Based Access Control (RSBAC).

Our initial approach also involved using a development version of the Mozilla Web of Things Gateway project, which is an open source smart home hub application that can be run on a Raspberry Pi. However, making changes to the code requires a complete understanding of the complex source code that Mozilla has built over more than a year, and is still receiving frequent updates from the team that might interfere with our changes. So we took a different approach - building a third party application that uses OAuth to authorize a user and provide access to the devices connected to the gateway. This way we are able to implement the RSBAC model in the most optimized way possible.

Understanding these technical specifications has helped us to envision the front end interactions of a potential user. Based on these specifications we have designed an initial interactive prototype using Adobe XD [4] called Thingzone. We have proposed a login screen (Fig. 2), device list (Fig. 3), user options (Fig. 4), and new user settings (Fig. 5) among other screens.



By creating an account you agree to our Terms of Service and Privacy Policy

Fig. 2 Thingzone login screen.

RESEARCH METHODS

To answer our five research questions we propose 2 concatenated user studies. The first will employ Scenario-Based Design [1] that will present users with the Adobe XD prototype in order to test and refine the overall information flows, notification texts, and possible use cases. The insights gathered in this study will be used to finalize our design of a high fidelity prototype that will be shared with potential users to test in their homes on a trial basis in our second user study.

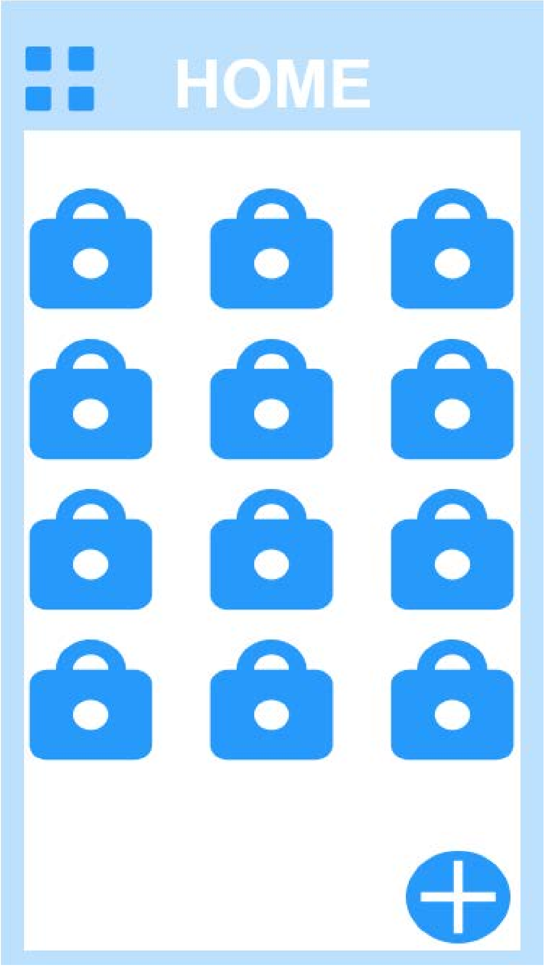


Fig. 3 Thingzone device list.

The main objective of the first user study is to determine people's preferences when it comes to shared access of their devices in the Internet of Things (IoT) and usability testing of a prototype of our app. To do this we will be inviting people in groups of 3-4 and walk them through a set of role-playing activities with specific roles for each person in the group. These activities will involve performing tasks to maintain the security of a home with IoT devices with shared access. These people will be students in the school of IT or roommates that know each other, these people will be offered extra credit in a class in return as an incentive.

These groups will be invited together in a conference room, where after a small introduction of IoT devices and our app, they will be asked to distribute any 2-3 available roles within themselves among their group where one person will be the admin and the other two will either be "medium duration" or "short duration" guests. Their responses on why they chose which role for whom will be recorded and then they will be given two scenarios to play out:-

Scenario 1: Fire (physical threat to a home)

The premise of the first scenario is that there is a fire in the house which needs to be taken care of. In this case the app would systematically notify users which could have two outcomes. The first user (first set of users) to be notified respond(s) to the emergency and handles the situation. The first user does not respond due to which the next user (set of users) is notified and so on until the emergency is taken care of.

Scenario 2: Cyber (cyber threats to the security of the home)

This scenario would follow the same flow of notifications as the first scenario with the difference being in the way the notification is responded to and handled.

Task 1: The group of users will be given a form to fill out where they will all be asked to consensually select one person in their group to have the role of an administrator who would then decide what permissions and what devices he wanted people in his group to access in what situations and why.

These users would then be sent links to their respective versions of the prototype depending on what permissions they have after which they would be told to familiarize themselves with it all while noting down any design flaws/ improvements they think could be implemented for a better user experience.

Task 2 (fire scenario case 1): A prototyped notification will be triggered onto the administrators' phone which he will be told to read and appropriately respond to. The notification will be that a fire has been detected in his living room and on clicking on it he would be taken to a live feed of

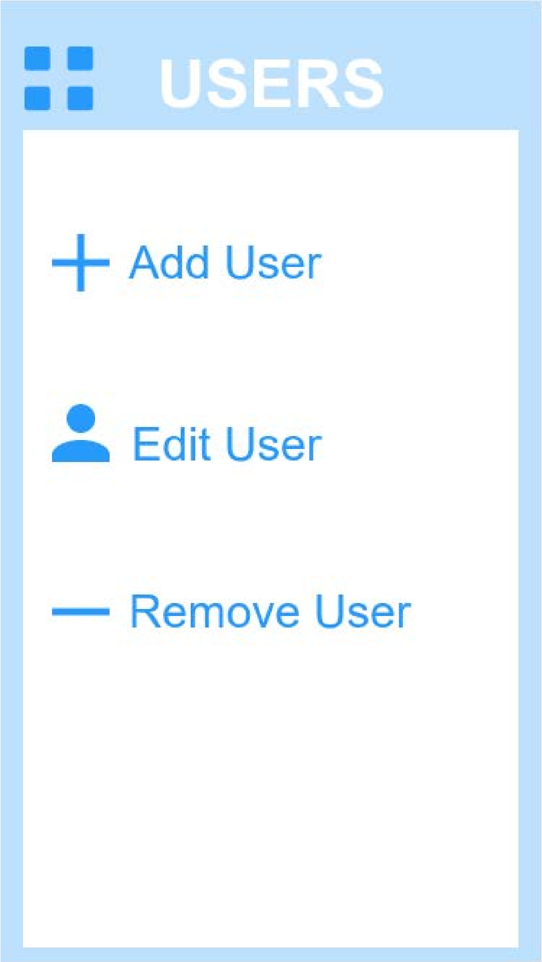


Fig. 4 Thingzone user options.

his living room (where he can see that there is a fire). The appropriate response to this would be to click on the call 911 button on the prototype.

Task 3: This will begin exactly as task two with the difference being that the administrator would now ignore the notification after which it will be triggered (by us) on another user's phone where he would have a unique way of accessing the camera/devices depending on the type of access he has. At the end of these tasks the groups will have a better understanding of the pros and cons of sharing different kinds of access with different people post which we can go on to ask them questions such as: In a real life situation, how would you share access with your friends and family if such an application was to be implemented? How was their experience through all the tasks and any advice they have on improving the user experience for faster response times to emergencies. If they would be willing to "crowdsource" access in the sense that if no one in their circle responds, anyone with the app could respond to this emergency (all while prioritizing privacy and anonymity)

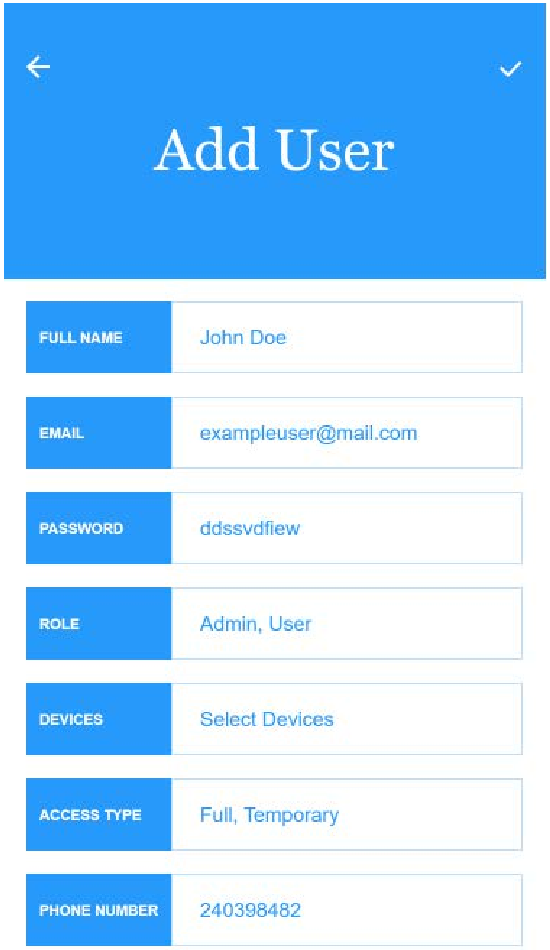
Task 4: This will begin similar to task 2 and 3 where the users would get notifications they could respond to with the difference being that the notification this time would be for unusual network activity, too much device activity in any of their smart devices, etc. This notification would lead them to a page where they could either: (1) Shut-down their network, (2) Shut-down the device, or (3) Dismiss.

These users will then be asked why they chose what they did and if they could think of any other cyber scenarios or any added functionality (e.g. viewing their network logs, etc.).

This will conclude the first user study. The insights will be used to refine notifications, options, and logic for implementation in our tool. Afterward, we will invite users to take the device home. We propose the use of "fire drills" or "cyber drills" to test notifications and logic further when users are invited to respond to notifications in their daily lives (as opposed to a lab environment).

CONTRIBUTIONS AND SIGNIFICANCE

The usage IoT devices has increased significantly in the last few years, and it has been predicted to grow even more in the coming decade. Most of this usage comes from smart homes, and they still lack an access control system. As previously mentioned, a system like RSBAC can open a new perspective of smart home accessibility. Once the testing is complete and the implementation is out for public to use, the model can be implemented in more popular smart home vendors like Amazon Home, Google Nest, Philips Hue etc. Not only will this make detecting and dealing with emergency situations that might otherwise cause damage to lives and property much easier, but it also opens up many possibilities like analytics and machine learning to study access patterns and detect anomalies, blockchain ledger based architecture, or an "IoT centric social device network".



Add User

FULL NAME	John Doe
EMAIL	exampleuser@mail.com
PASSWORD	ddssvdfiew
ROLE	Admin, User
DEVICES	Select Devices
ACCESS TYPE	Full, Temporary
PHONE NUMBER	240398482

Fig. 5 Thingzone new user settings.

ACKNOWLEDGMENTS

This work was partially supported by the National Science Foundation (Award # 1814110) and Mozilla.

REFERENCES

1. J M Carroll. 2006. Scenario-Based Design. In *International Encyclopedia of Ergonomics and Human Factors (2nd Edition)*. CRC Press of Taylor and Francis, 198–202.
2. Weijia He, Roshni Padhi, Jordan Ofek, et al. *Rethinking Access Control and Authentication for the Home Internet of Things (IoT)*. .
3. IoT: number of connected devices worldwide 2012-2025 | Statista. Retrieved March 23, 2019 from https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/.
4. Adobe XD | UX/UI design and collaboration tool. Retrieved March 27, 2019 from https://www.adobe.com/products/xd.html?scid=social52541916.