



# Sharing Smart Home Devices: From the perspective of AirBnB Host

Authors: Rajib Dey, Sayma Sultana

# Introduction

- AirBnB covers more than 81,000 cities and 191 countries worldwide.
- Smart home devices to tackle security concern and maintenance.



Smart speaker



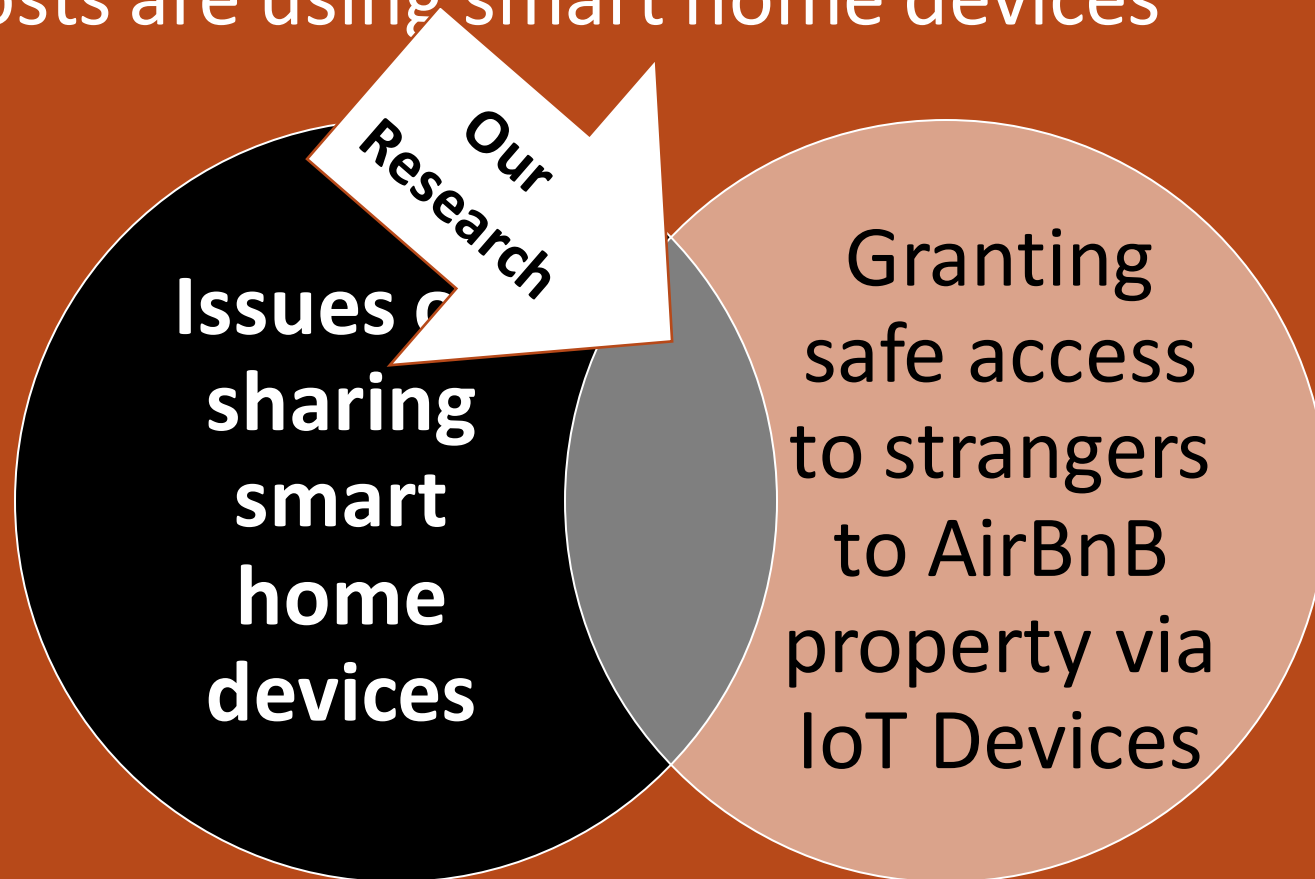
Smart lock & doorbell



Media Streamer

# Motivation

- Sharing smart home devices with differently related people imposes some issues and concerns
- AirBnB hosts are using smart home devices





# Research Questions

**RQ1 : What smart home devices are AirBNB hosts currently using on their properties and for what purpose?**

**RQ2: What are the benefits and concerns AirBNB hosts has?**

**RQ3: What unique needs do AirBNB hosts have for managing and sharing access control to their smart home devices with AirBNB guests?**



# Literature Review

**We can split our Literature Review in 2 ways**

- 1. Smart Home Access Control and Privacy**
- 2. Smart Home for AirBnB**



# Literature Review

## 1. Smart Home Access Control and Privacy

### How sharing happens within a trusted circle?

He et al. discussed how sharing of IoT devices inside a home differs based on relationships, time of the day, scenarios, location of the device, etc. [2].

An empirical study on 15 families done by Brush et al. [3] reveals that family members trust each other while keeping separate profiles on IoT devices.

**Reason:** Block strangers with malicious intent.



# Literature Review

## 1. Smart Home Access Control and Privacy

### Sharing is complicated

Most of the smart home devices are designed just like a personal device[2].

Control systems can be so complicated that the end-user sensed that they have less control [4].

Page et al [5] discuss that consumer grade IoT devices are not user-centric and have less control over it.

Giving guests access to your IoT device in a smart home with specific with policies are important and complex task [6] [7].

It's complex, because of the varied amount of data and trust users have between themselves [8].

User concern on security & Privacy vary depending on the relationships such as guests [6], roommates [8], and children [9] [10].

Trust plays a major factor even when sharing IoT devices among neighbors can help increase the security. [11]



# Literature Review

## 1. Smart Home Access Control and Privacy

### Sharing has privacy and security issues

Sharing has privacy and security concern to users [12] [13].

Trust for the devices is also important as when the user is away from home, the access control of the home IoT devices has to be trustworthy enough to operate on their own [14].





# Literature Review

## 1. Smart Home Access Control and Privacy

### Solutions to this problems

Mazurek et al. [15] show that most of the time the user needs a complex access control policy and they try to achieve that by using makeshift methods.

Kostianinen et al. [7], tried to introduce an access control policy for smart home networks limited to family members which would pose a nominal amount of burden on the end-user by testing a few access control policies.

Another research by Dixon et al. [16] reveals, access-control policies based on time (for guests), special preventive measures for highly sensitive devices like cameras and locks, limiting of application's access to devices.

Providing users the information about the data being monitored by all the devices[17].



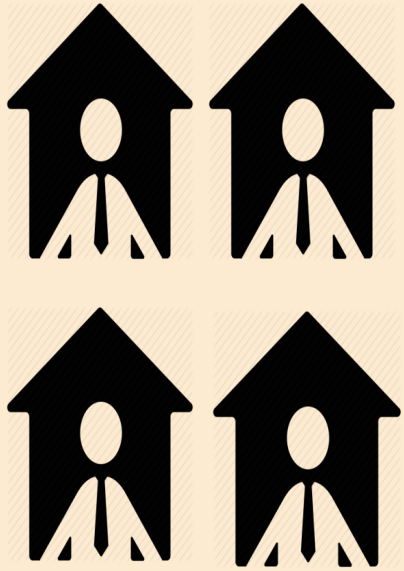
# Literature Review

## 2. Smart Home for AirBnB

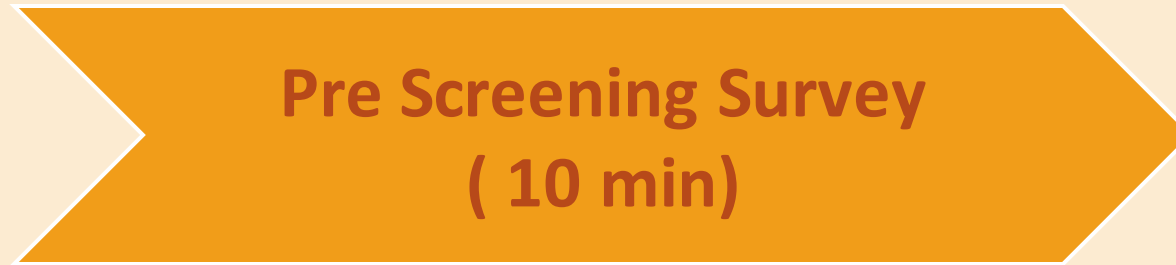
Researchers from Umass Amherst [1] proposed Preserving IoT Privacy in Sharing Economy (or AirBnB) using Blockchain technology.

We take an HCI approach to this by asking the hosts what they want.

# Methods



**50+ airBnB hosts**



- How many devices?
- Which devices ?
- Which capabilities?



**10 hosts with 2+  
smart home  
devices**

# Methods



**Follow up interview  
(30 min)**

**Data**

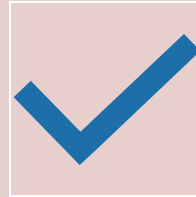
**10 hosts with 2+  
smart home  
devices**

- Do they share?
- Sharing easy or hard?
- Want more access control?
- Any security concern?
- Any incident inspired to share?

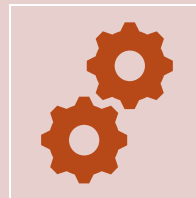
# Data Analysis



**Transcribe interview**



**Coding to common  
theme**



**Code aggregation**

# Project Timeline





# Contribution

- Better understanding of the status quo of smart home devices in AirBnB.



# References

- [1] M. N. Islam and S. Kundu. Poster abstract: Preserving iot privacy in sharing economy via smart contract. In 2018 IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation (IoTDI), pages 296–297, April 2018.
- [2] Weijia He, Maximilian Golla, Roshni Padhi, Jordan Ofek, Markus Dürmuth, Earlene Fernandes, and Blasé Ur. Rethinking access control and authentication for the home internet of things (iot). In 27th USENIX Security Symposium (USENIX Security 18), pages 255–272, 2018.
- [3] A.J. Brush and Kori Inkpen. Yours, mine and ours? sharing and use of technology in domestic environments. In Ubicomp 2007. Springer, September 2007.
- [4] Dave Randall. Living Inside a Smart Home: A Case Study, pages 227–246. Springer London, London, 2003.
- [5] Xinru Page, Paritosh Bahirat, Muhammad I. Safi, Bart P. Knijnenburg, and Pamela J. Wisniewski. The internet of what?: Understanding differences in perceptions and adoption for the internet of things. IMWUT, 2:183:1–183:22, 2018.
- [6] Matthew Johnson. Usability of security management: Defining the permissions of guests. In Bruce Christianson, Bruno Crispo, James A. Malcolm, and Michael Roe, editors, Security Protocols, pages 284–285, Berlin, Heidelberg, 2009. Springer Berlin Heidelberg.
- [7] K. Kostinen, O. Rantapuska, S. Moloney, V. Roto, U. Holmstrom, and K. Karvonen. Usable access control inside home networks. In 2007 IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks, pages 1–6, June 2007.
- [8] Vassilios Lekakis, Yunus Basagalar, and Pete Keleher. Don't trust your roommate or access control and replication protocols in "home" environments. In Proceedings of the 4th USENIX Conference on Hot Topics in Storage and File Systems, HotStorage'12, pages 12–12, Berkeley, CA, USA, 2012. USENIX Association.





# References

- [9] Tamara Denning, Tadayoshi Kohno, and Henry M. Levy. Computer security and the modern home. *Commun. ACM*, 56(1):94–103, January 2013.
- [10] Stuart Schechter. The user is the enemy, and (s)he keeps reaching for that bright shiny power button! In *Proceedings of the Workshop on Home Usable Privacy and Security (HUPS)*, July 2013.
- [11] A.J. Brush, Jaeyeon Jung, Ratul Mahajan, and Frank Martinez. Digital neighborhood watch: Investigating the sharing of camera data amongst neighbors. In *CSCW 2013*. ACM, February 2013.
- [12] Pardis Emami-Naeini, Sruti Bhagavatula, Hana Habib, Martin Degeling, Lujo Bauer, Lorrie Faith Cranor, and Norman Sadeh. Privacy expectations and preferences in an iot world. In *Proceedings of the Thirteenth USENIX Conference on Usable Privacy and Security, SOUPS '17*, pages 399–412, Berkeley, CA, USA, 2017. USENIX Association.
- [13] Eric Zeng, Shrirang Mare, and Franziska Roesner. End user security and privacy concerns with smart homes. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, pages 65–80, 2017.
- [14] W. Keith Edwards and Rebecca E. Grinter. At home with ubiquitous computing: Seven challenges. In *Proceedings of the 3rd International Conference on Ubiquitous Computing, UbiComp '01*, pages 256–272, Berlin, Heidelberg, 2001. Springer-Verlag.
- [15] 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. Access control for home data sharing: Attitudes, needs and practices. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, CHI '10*, pages 645–654, New York, NY, USA, 2010. ACM.



# References

- [16] Colin Dixon, Ratul Mahajan, Sharad Agarwal, A.J. Brush, Bongshin Lee, Stefan Saroiu, and Paramvir Bahl. An operating system for the home. In Presented as part of the 9th USENIX Symposium on Networked Systems Design and Implementation (NSDI 12), pages 337–352, San Jose, CA, 2012. USENIX.
- [17] Simon Moncrieff, Svetha Venkatesh, and Geoff West. Privacy and the access of information in a smart house environment. In Proceedings of the 15th ACM International Conference on Multimedia, MM '07, pages 671–680, New York, NY, USA, 2007. ACM.

Questions ?