03-Sep-2018

Smart Connected Homes:

Concepts, Risks, and Challenges

Joseph Bugeja

MALMÖ UNIVERSITY
INTERNET OF THINGS AND PEOPLE RESEARCH CENTER

Licentiate Seminar

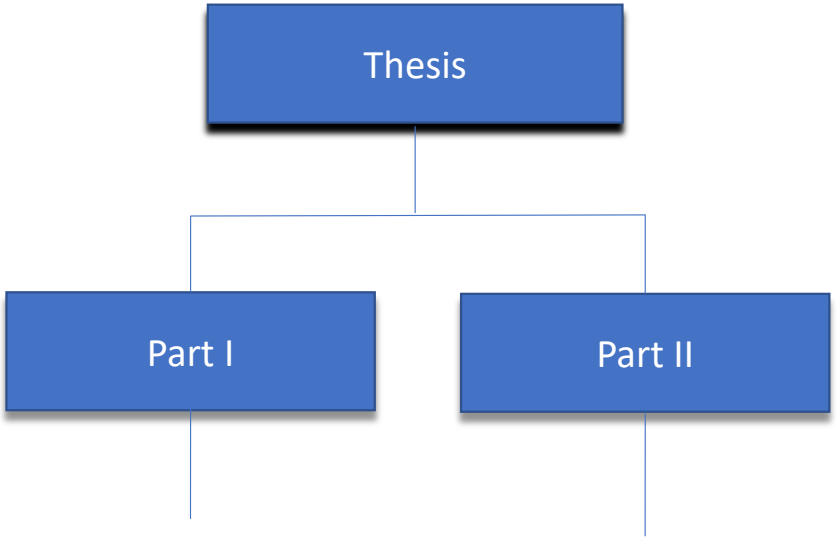
KK-stiftelsen

AGENDA

- Introduction and Research Questions
- Concepts
- Research Methodology
- Contributions
- Future Work

INTRODUCTION AND RESEARCH QUESTIONS

THESIS STRUCTURE

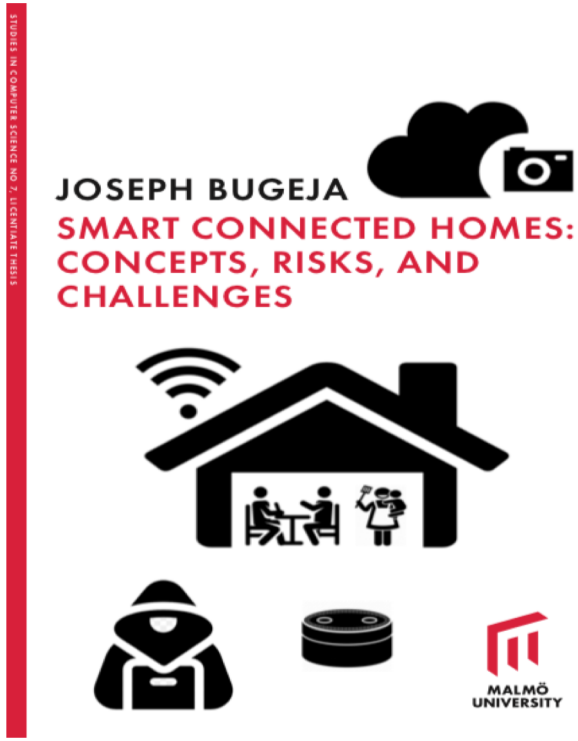


Thesis “Kappa”

pp. 18 – 62

Publications

pp. 63 – 192



INTRODUCTION

"Wireless cameras within a device such as the fridge may record the movement of suspects and owners"

-- Mark Stokes (2017)

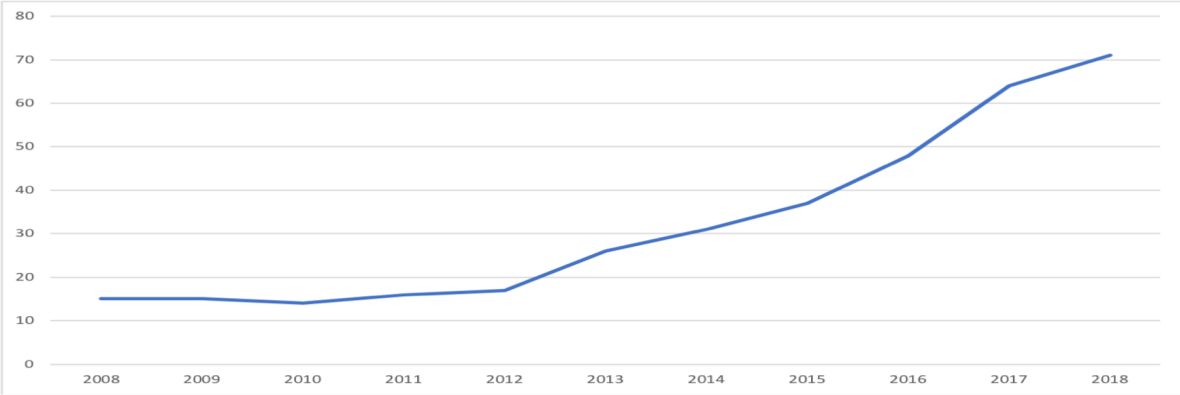
(Head of Scotland Yard's digital, forensics, and cyber communications)

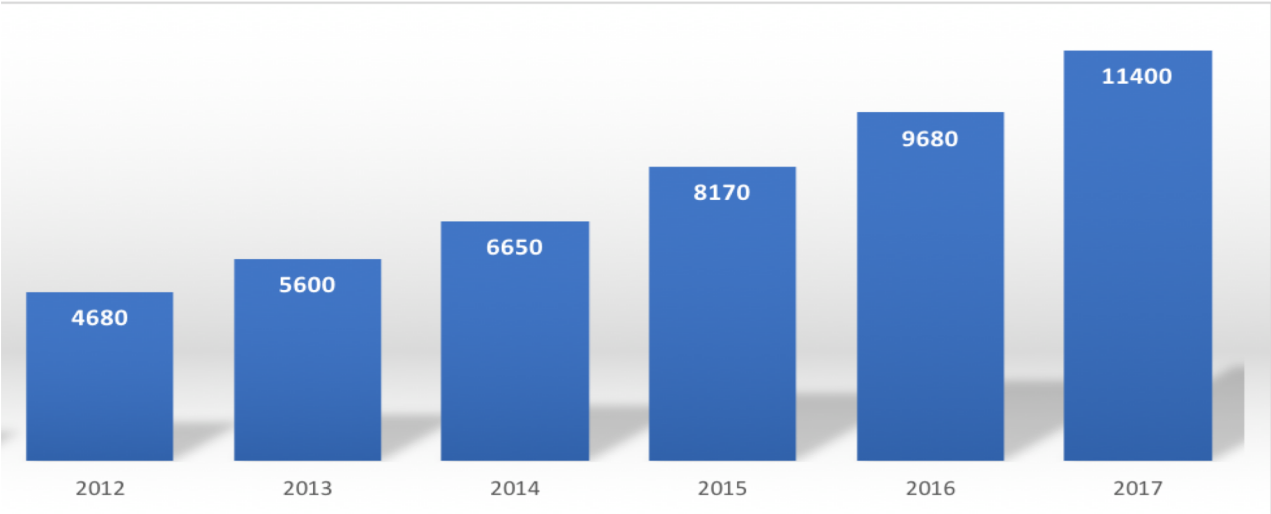
Image: Getty

INTRODUCTION

What is the motivation of this thesis?

- Interest over time according to Google trends since 2008 for the term Smart Home





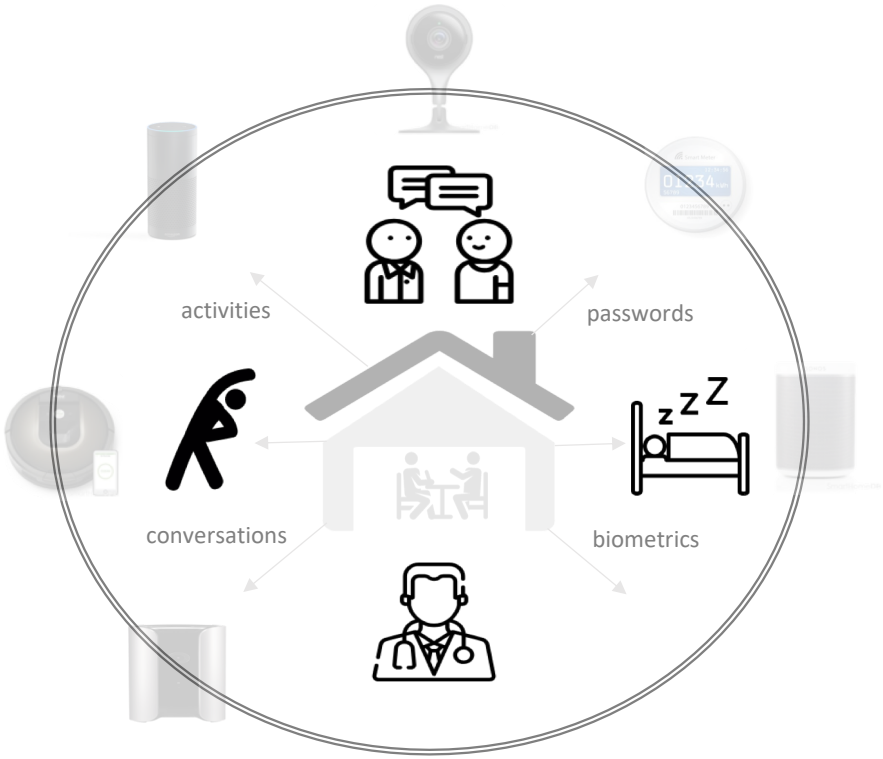
- Total number of publications appearing in Google Scholar for the term Smart Home

INTRODUCTION

What is the motivation of this thesis?

- The amount of connected devices in use is estimated to increase from 11 billion in 2018 to 20 billion by 2020 (Gartner Inc., 2017)

- The amount of data collected by networked devices is anticipated to increase from 2.5 quintillion bytes of data/day to 40 yottabytes by 2020 (Wang et al., 2015)



Smart home devices and data

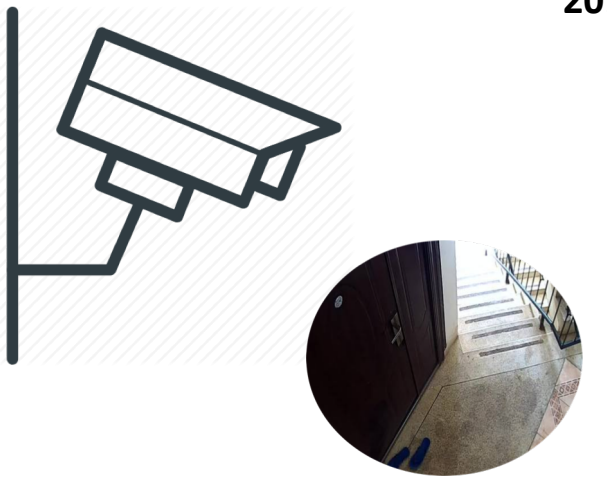
Wang, L., & Ranjan, R. (2015). Processing Distributed Internet of Things Data in Clouds. *IEEE Cloud Computing*, 1–5.

INTRODUCTION

What is the motivation of this thesis?

- Your smart home devices may jeopardize your security and privacy in multiple ways

2014



"Peeping into 73,000 unsecured security cameras thanks to default passwords"

Source: https://goo.gl/pNKEAC

2016

"A hacker could crank up the temperature of a smart thermostat to a sweltering 99 degrees"

Ransomware PoC FTW!

#Defcon24 #wargames @IoTvillage

Hackers demonstrated first ransomware for IoT thermostats at DEF CON

Source: https://goo.gl/EoxCAZ

2017

"After hearing the anchor's comment, their own devices also tried to order pricey dollhouses."

Source: Chung, H., Iorga, M., Voas, J., & Lee, S. (2017). "Alexa, Can I Trust You?." *IEEE Computer*, 1–5.

RESEARCH QUESTIONS

What are the research questions being answered in this thesis?

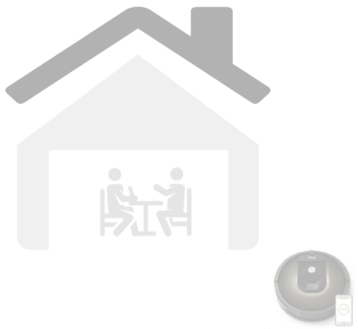
- ✓ **RQ1:** How can smart connected home devices and the data collected by them be categorized?
- ✓ **RQ2:** What security and privacy risks does the introduction of IoT technologies inside the home bring to the residents?
- ✓ **RQ3:** What are the characteristics and challenges in mitigating security and privacy risks in smart connected homes?

CONCEPTS

SMART CONNECTED HOME

What is a smart connected home?

Smart home



Connected home

Smart connected home

SMART CONNECTED HOME

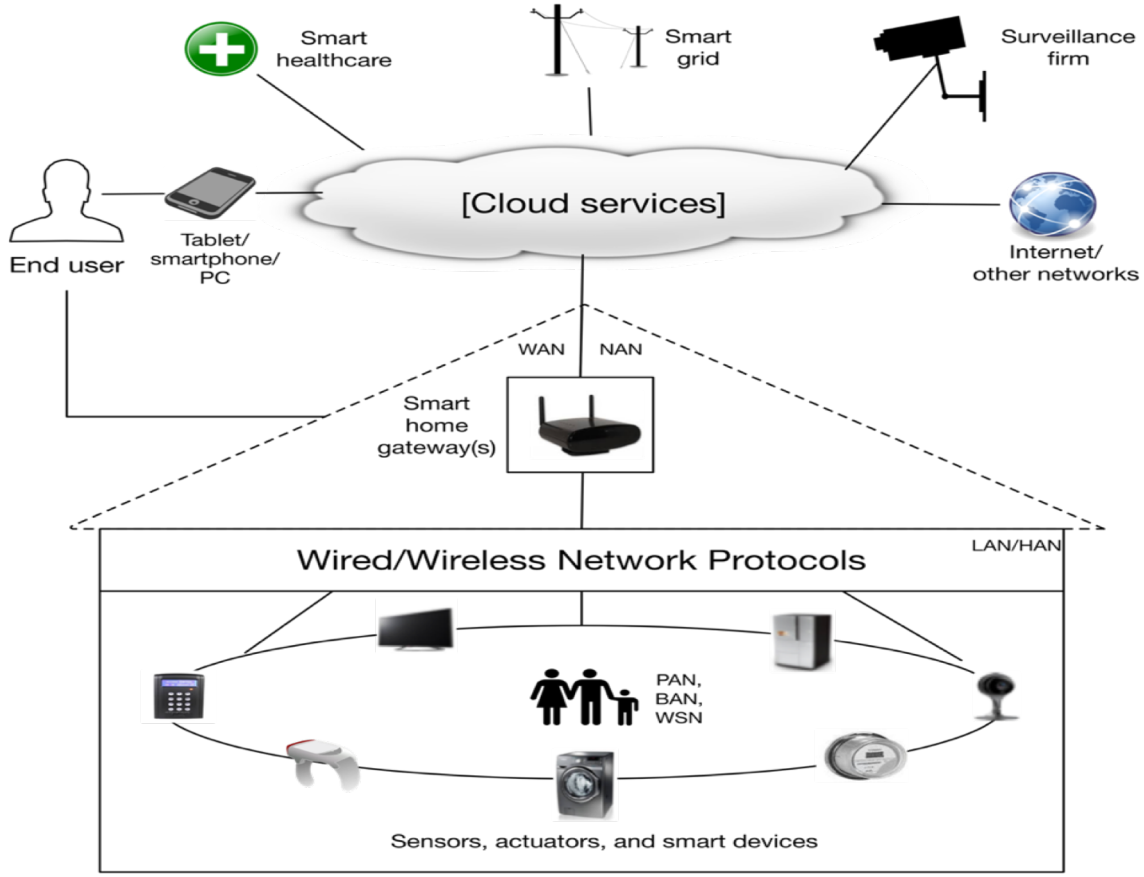
What is a smart connected home?

- Essentially, a smart connected home leverages IoT technologies to improve the quality and efficiency of life to the residents

Image: Shutterstock

SMART CONNECTED HOME

What is the generic architecture of a smart connected home?



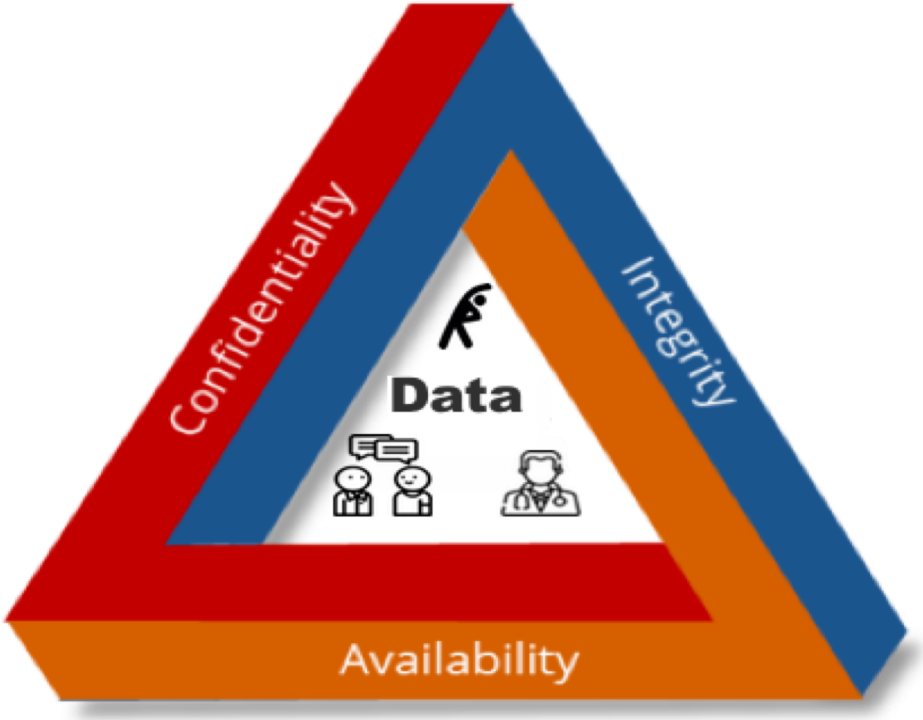
Note: WAN, LAN, NAN, HAN, PAN, BAN, and WSN correspond to wide area, local area, neighbourhood area, home area, personal area, body area, and wireless sensor networks respectively

SECURITY AND PRIVACY GOALS

What are the main objectives of security and privacy?

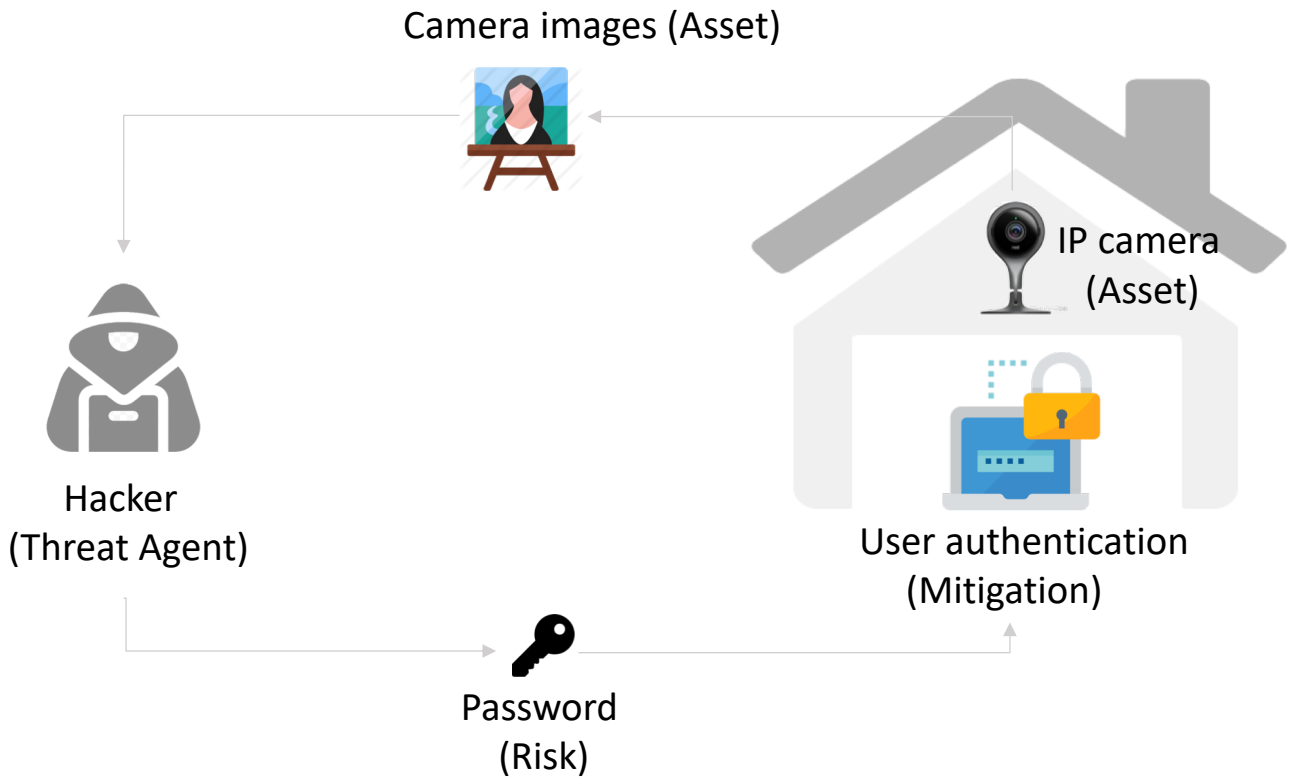
- Information security key objectives are to ensure the confidentiality, integrity, and availability of assets

- Privacy deals with the protection of user's personal information from unauthorized entities



PRIVACY RISK SCENARIO

- Risk that a hacker gets unauthorized access to the camera feeds through an IP camera facilitating a house break-in



MANAGING SECURITY AND PRIVACY

- Managing information security and privacy effectively requires a thorough understanding of the smart connected home

Who are the threat agents interested in the home?

What are the existing mitigations?

What are the devices?

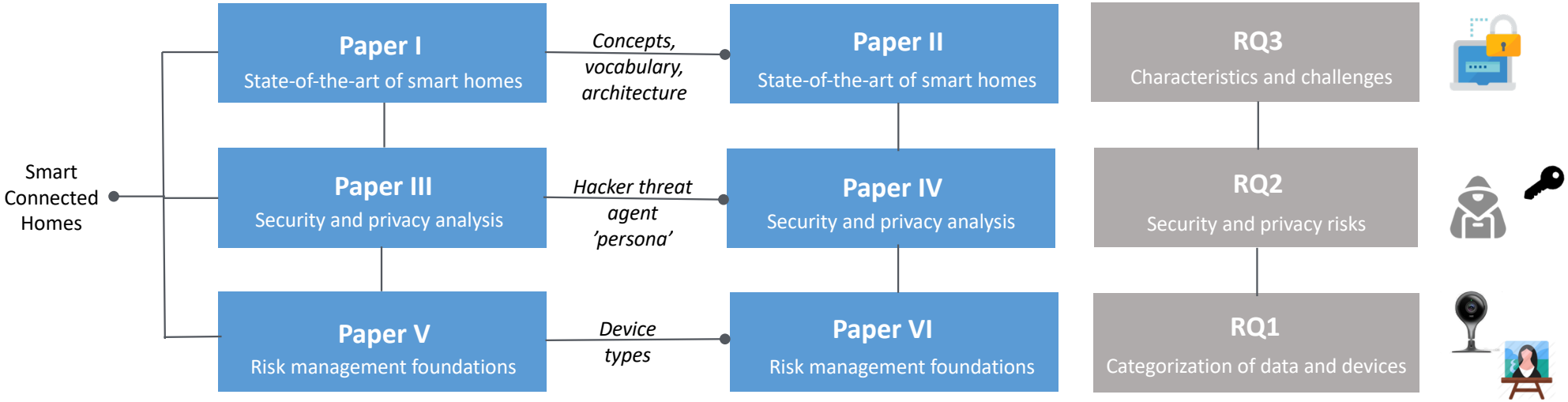
What are the risks?

What are the data?

RESEARCH METHODOLOGY

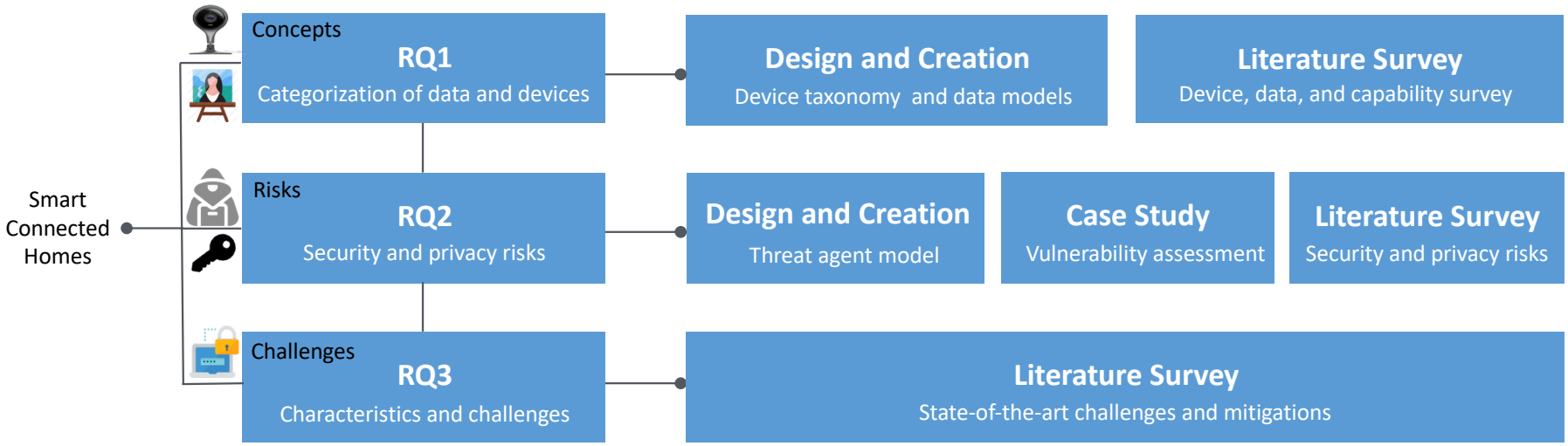
PAPER OVERVIEW

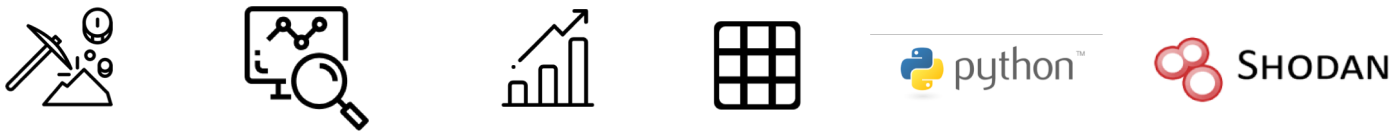
✓ Exploring the relationship between the different papers and corresponding research areas



RESEARCH DESIGN

✓ We adopted primarily an exploratory research approach but leverage also positivist strategies



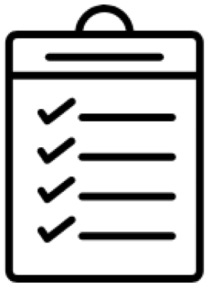


SOME TECHNICAL CHALLENGES

- ✗ Shortage of IoT open vulnerability databases allowing for quantitative analysis

- ✗ Lack of dedicated datasets that identify the full technical specification of devices

- ✗ Existing models are not aligned well to actual smart home setups



CONTRIBUTIONS

MAIN CONTRIBUTIONS

i. A taxonomy and quantitative analysis of devices in smart connected homes

ii. An analysis and classification of data collected by smart connected homes

iii. A threat agent model for the smart connected home

iv. Identification of state-of-the-art security challenges and their mitigations in smart connected homes

RQ1
Categorization of data and devices

RQ1
Categorization of data and devices

RQ2
Security and privacy risks

RQ3
Characteristics and challenges

MAIN CONTRIBUTIONS

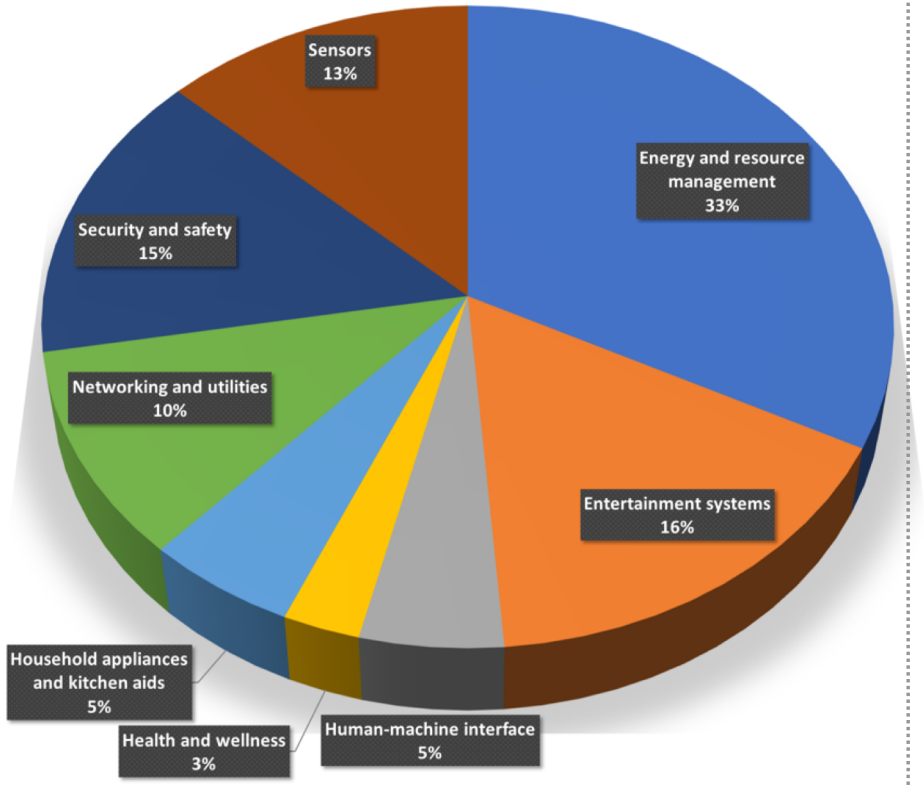
- Taxonomy and quantitative analysis of smart home devices

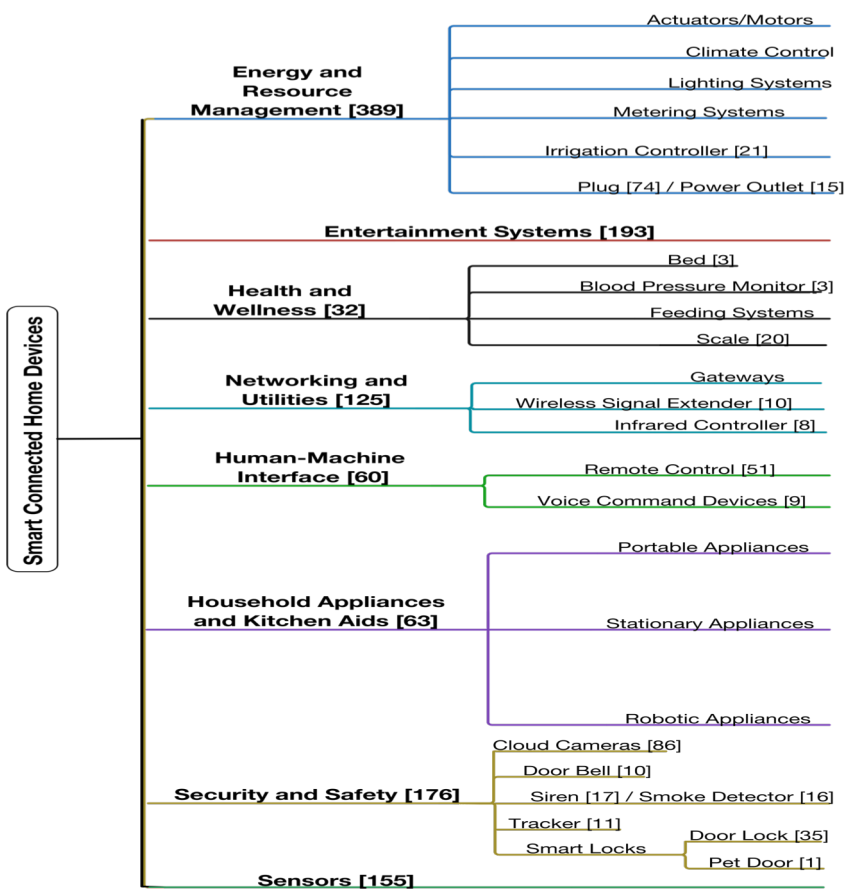
Paper V
Risk management foundations

RQ1
Categorization of data and devices

RQ2
Security and privacy risks

RQ3
Characteristics and challenges





MAIN CONTRIBUTIONS

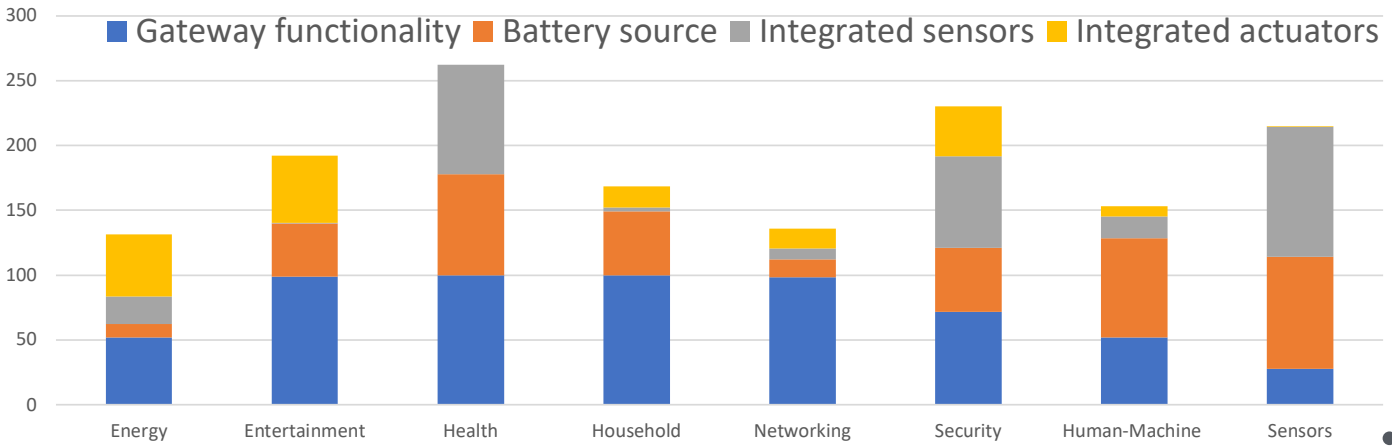
Paper V
Risk management foundations

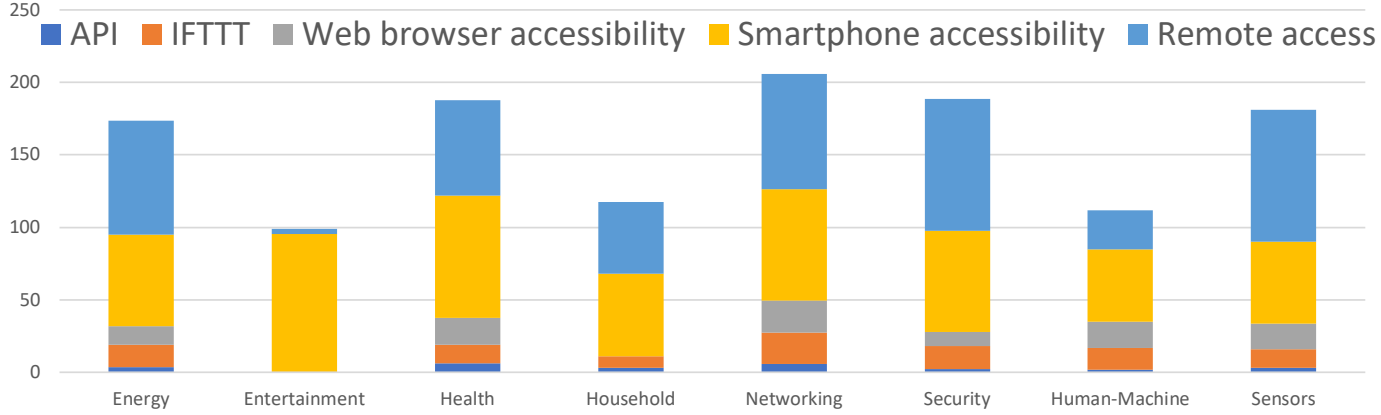
- Generic capabilities of smart home devices

RQ1
Categorization of data and devices

RQ2
Security and privacy risks

RQ3
Characteristics and challenges





- Device
- Communication
- Software
- Accessibility

MAIN CONTRIBUTIONS

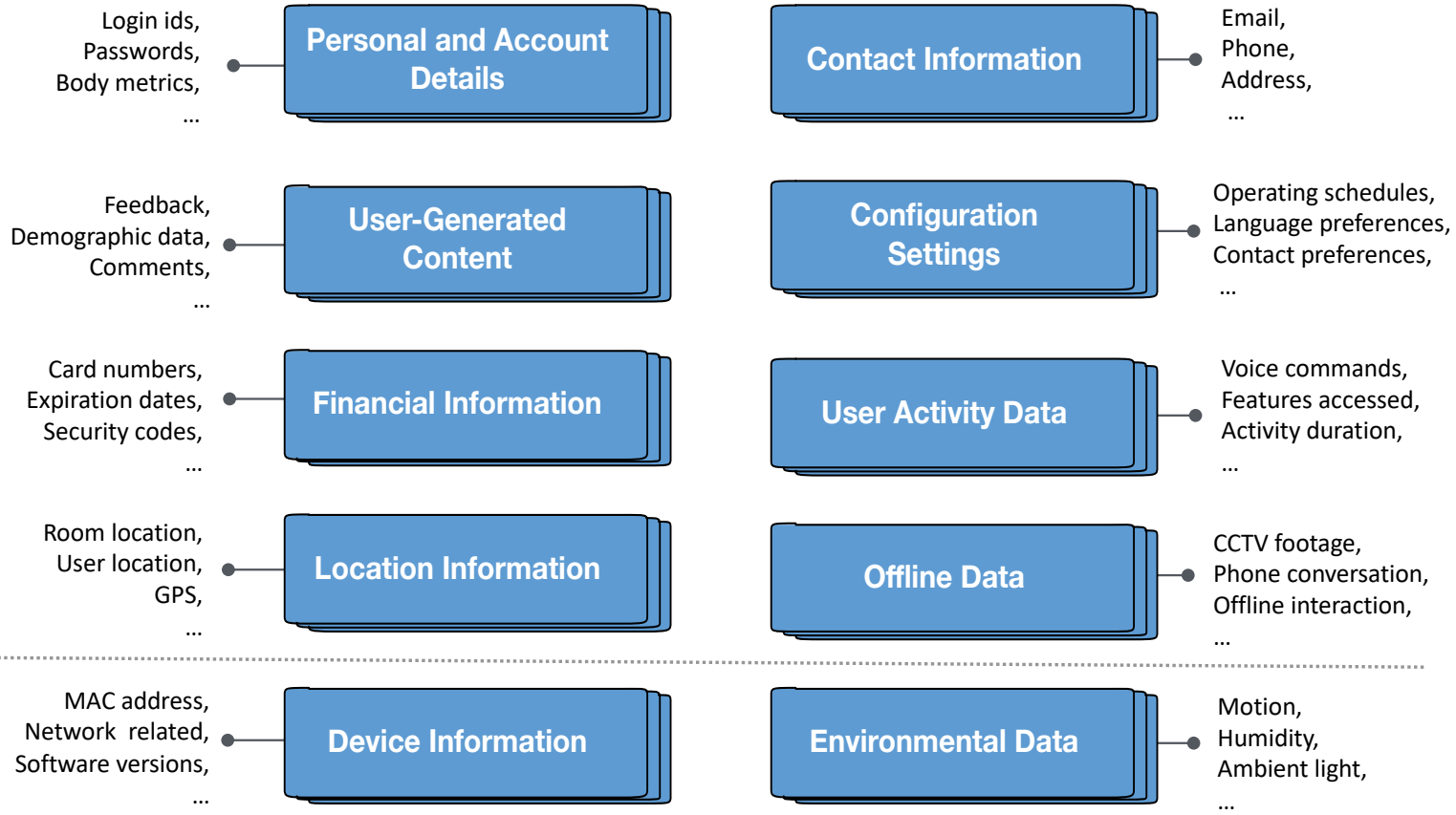
Paper VI
Risk management foundations

- Data types for the smart connected home

RQ1
Categorization of data and devices

RQ2
Security and privacy risks

RQ3
Characteristics and challenges



MAIN CONTRIBUTIONS

Paper VI
Risk management foundations

- Data collection model for the smart connected home

RQ1
Categorization of data and devices

RQ2
Security and privacy risks

RQ3
Characteristics and challenges

Data category	Collection mode	Collection method	Collection phase
Contact information	Explicit	Website form, service	System setup
Device information	Implicit, explicit	Smart home device, end-user device	System operation, sync process
Personal and account details	Explicit	Website form, service	System setup
User activity data	Implicit, explicit	Sensors, service	System operation, sync process
Configuration settings	Explicit	Website form, cookies, service	System setup
Location information	Implicit, explicit	Smart home device, end-user device	System operation
Financial information	Explicit	Website form, service	Purchase process
Environmental data	Implicit	Sensors	System operation
User-generated content	Explicit	Surveys, feedback form, support ticket	System operation, troubleshooting process
Offline data	Implicit, explicit	Paper, digital	Offline

MAIN CONTRIBUTIONS

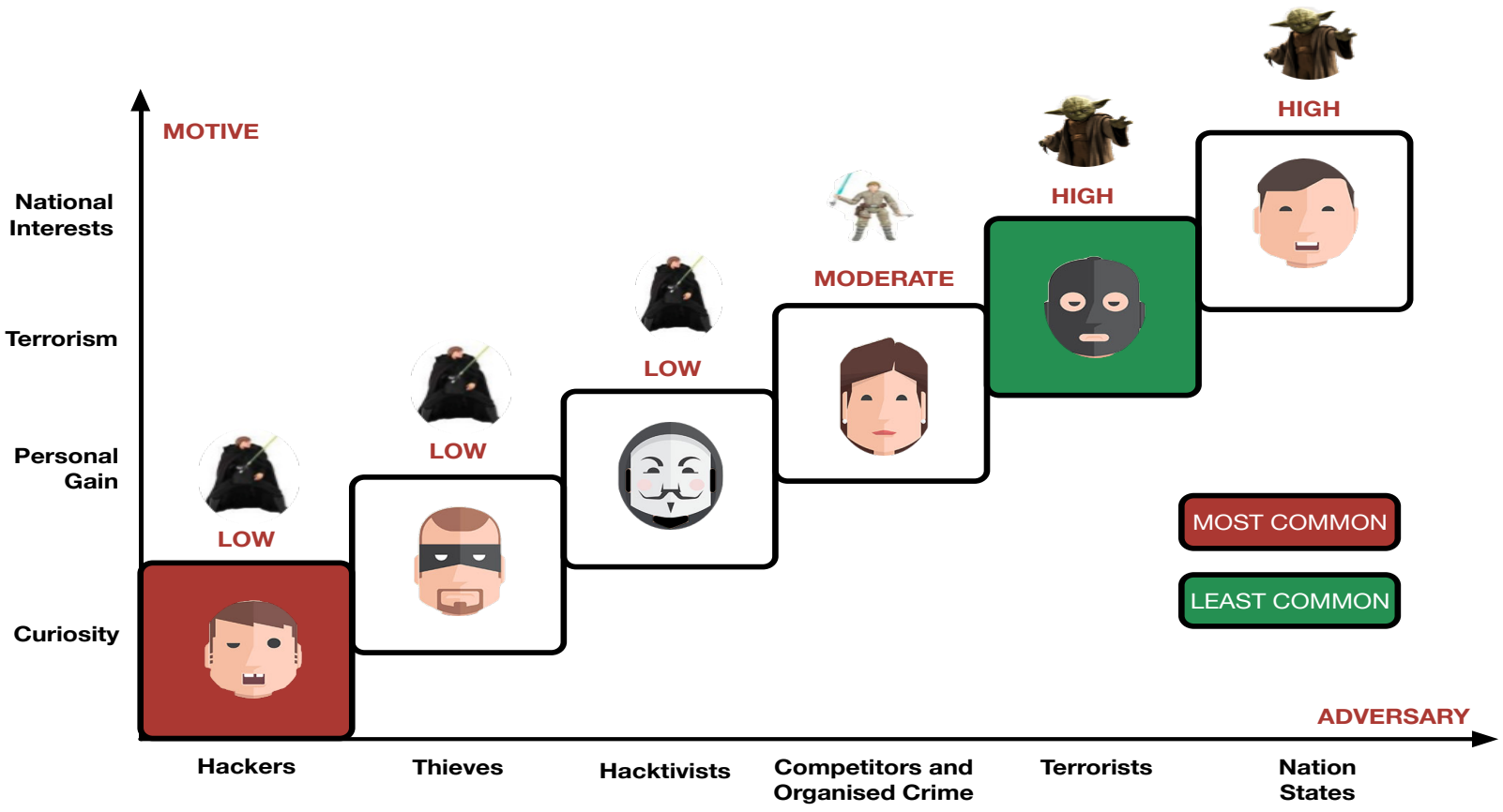
Paper III
Security and privacy analysis

- Threat agent model for the smart connected home

RQ1
Categorization of data and devices

RQ2
Security and privacy risks

RQ3
Characteristics and challenges



MAIN CONTRIBUTIONS

Paper III
Security and privacy analysis

- Threat agent model for the smart connected home

RQ1
Categorization of data and devices

RQ2
Security and privacy risks

RQ3
Characteristics and challenges

Threat Agent	Typical Compromise Methods	
	Security	Privacy
Nation states	Attack a communication device, e.g. home router, to disrupt or corrupt smart home services (availability)	Attack on sensors, e.g. cameras, to eavesdrop communication of adversaries
Terrorists	Attack an actuator, e.g. insulin pump, to inject medication, possibly overdosing a patient (integrity)	N/A
Competitors and Organized Crime	Attack a smart appliance, e.g. refrigerator, to help grow a criminally-funded botnet (integrity) Attack a device firmware to get a competitor's software (confidentiality)	Attack on sensors, e.g. microphones, to snoop on private conversations
Hacktivists	Attack a smart home network to disrupt its services (availability)	Attack the smart home network resources to intercept sensitive communication
Thieves	Attack a smart home alarm system to rob a house (availability)	Attack a smart home hub to detect when the residents are away
Hackers	Attack a smart home network to gather information, e.g. credentials, about the user (confidentiality)	Attack a smart home device, e.g. a baby monitor, to cause chaos

MAIN CONTRIBUTIONS

- Vulnerability assessment of smart connected cameras

Paper IV
Security and privacy analysis

RQ1
Categorization of data and devices

RQ2
Security and privacy risks

RQ3
Characteristics and challenges

SHODAN

62.[redacted]

Property Name	Value
area_code	null
asn	AS6830
city	Gelsenkirchen
country_code	DE
country_code3	DEU
country_name	Germany
data.0._shodan.crawler	264b5a9d15a64f96a4768e9d8081b
data.0._shodan.id	null
data.0._shodan.module	rtsp-tcp
data.0.data	RTSP/1.0 200 OK CSeq: 1 Server: Hipcam RealServer/V1.0 Public: OPTIONS,DESCRIBE,SETUP,TEARDOWN,PLAY,SET_PARAMETER,GET_PARAMETER
data.0.domains	['unitymediagroup.de']

ip	1049610876
ip_str	62.143.202.124
isp	Unitymedia
last_update	2018-03-20T19:29:37.676273
latitude	51.5221
longitude	7.0575
org	Unitymedia
os	null
ports	[554]
postal_code	45883
region_code	07

MAIN CONTRIBUTIONS

Paper IV
Security and privacy analysis

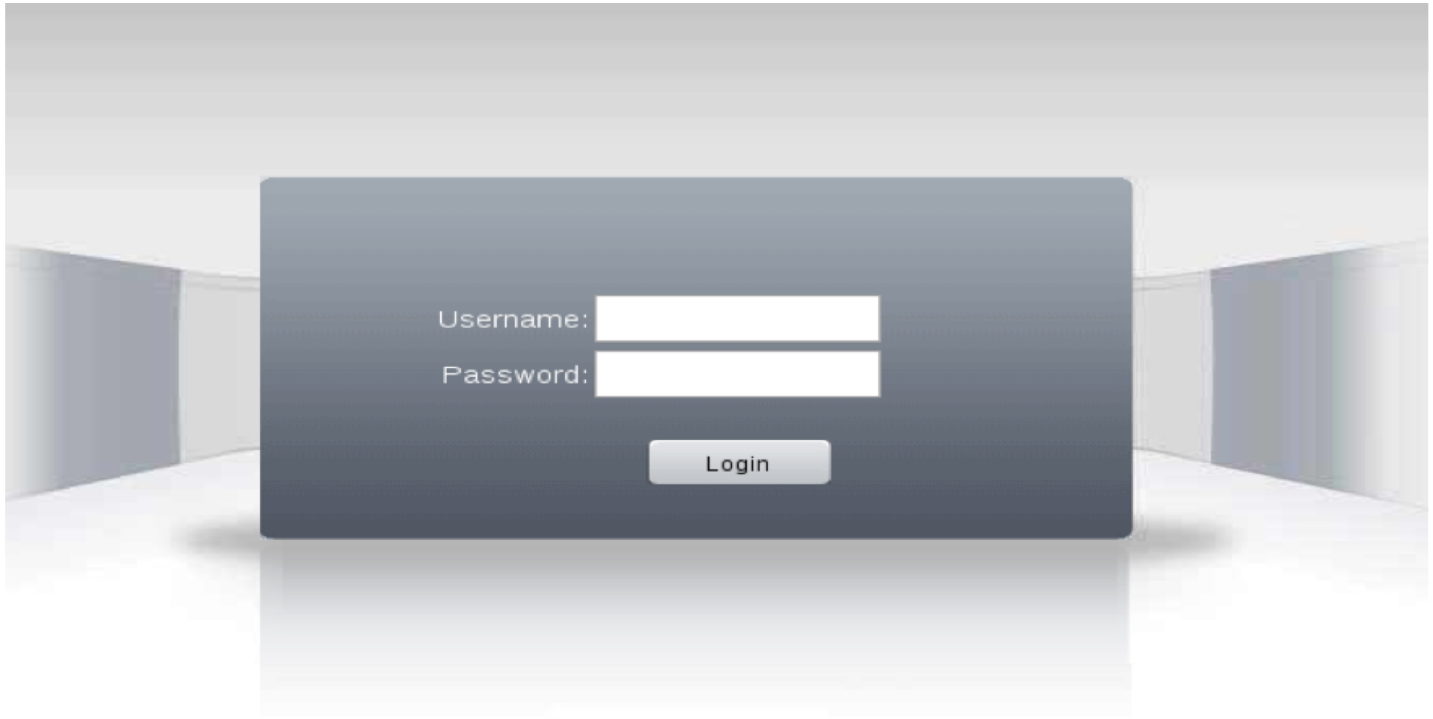
- Vulnerability assessment of smart connected cameras

RQ1
Categorization of data and devices

RQ2
Security and privacy risks

RQ3
Characteristics and challenges

542,270 devices, mostly IoT security cameras, were running “uc-httpd” (*Nov 2017*)



SHODAN

MAIN CONTRIBUTIONS

Paper IV
Security and privacy analysis

- Vulnerability assessment of smart connected cameras

RQ1
Categorization of data and devices

RQ2
Security and privacy risks

RQ3
Characteristics and challenges

SHODAN

Critical

CVE-2015-2887

- Video baby monitor
- Complete compromise of security and privacy

High

CVE-2007-5213

- Home camera
- Perform tasks with full privileges

Medium

CVE-2011-5261

- Small business camera
- Unauthorized modification of data

MAIN CONTRIBUTIONS

Paper II
State-of-the-art of smart homes

- Security and privacy mitigations

RQ1
Categorization of data and devices

RQ2
Security and privacy risks

RQ3
Characteristics and challenges

DEVICE	COMMUNICATION	SERVICE
H/W encryption	VPN	Security testing
Fail-secure design	Firewalls	Secure design
Device authorization	IDS/IPS	Data masking
Enhanced algorithms	TOR-based systems	Cryptographic schemes
Secure platforms	Dedicated devices	Security organizations
CC and EMVCo IC SE	Guidelines	Open guidelines

MAIN CONTRIBUTIONS

Paper II
State-of-the-art of smart homes

- Security and privacy challenges

RQ1
Categorization of data and devices

RQ2
Security and privacy risks

RQ3
Characteristics and challenges

FUTURE WORK

FUTURE WORK

- ✓ **User controllable privacy artifact:** Designing a component (e.g., similar to a light dimmer) that allows residents the option to tune their privacy preferences

- ✓ **Proactive networking security approaches:** Network-based solution, working similar to an Intrusion Detection System, that complements existing security mechanisms

- ✓ **Smart connected home formal model:** Capturing the description of a generic and more secure and privacy-preserving smart connected home in a formal model

Thank you

for *your*

Attention !