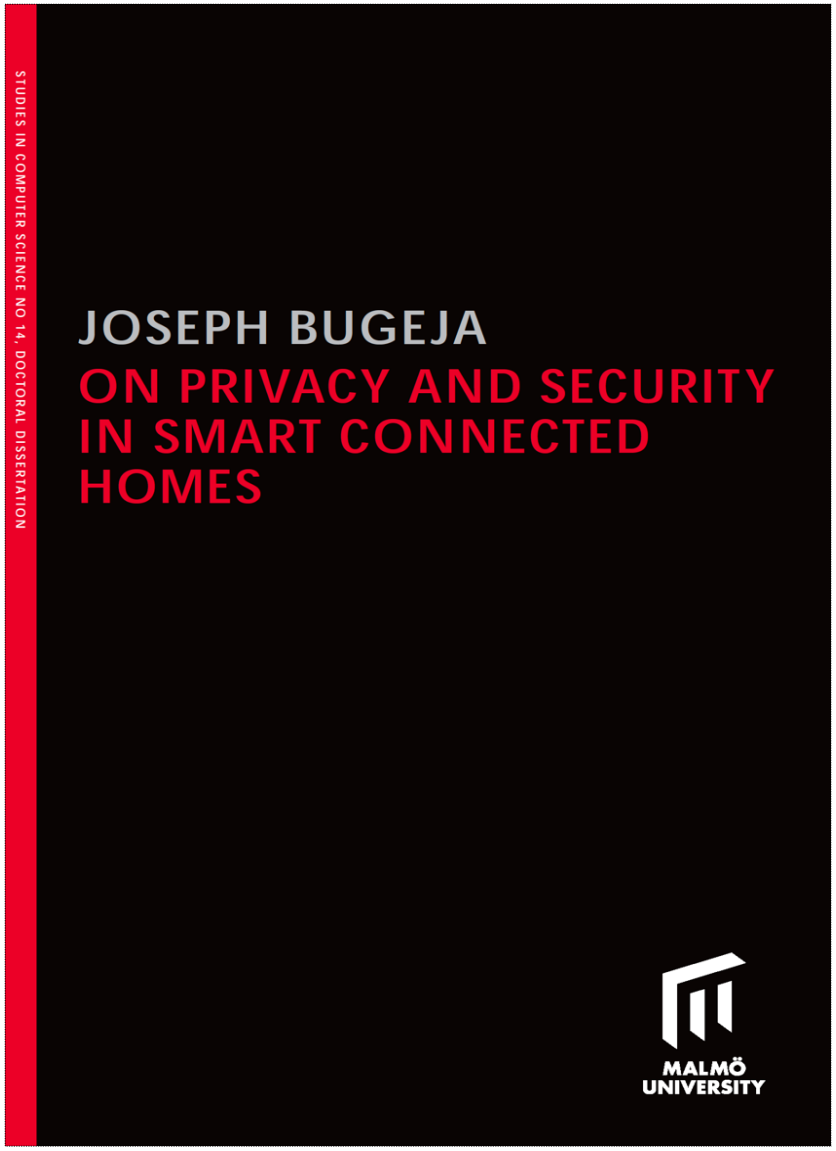
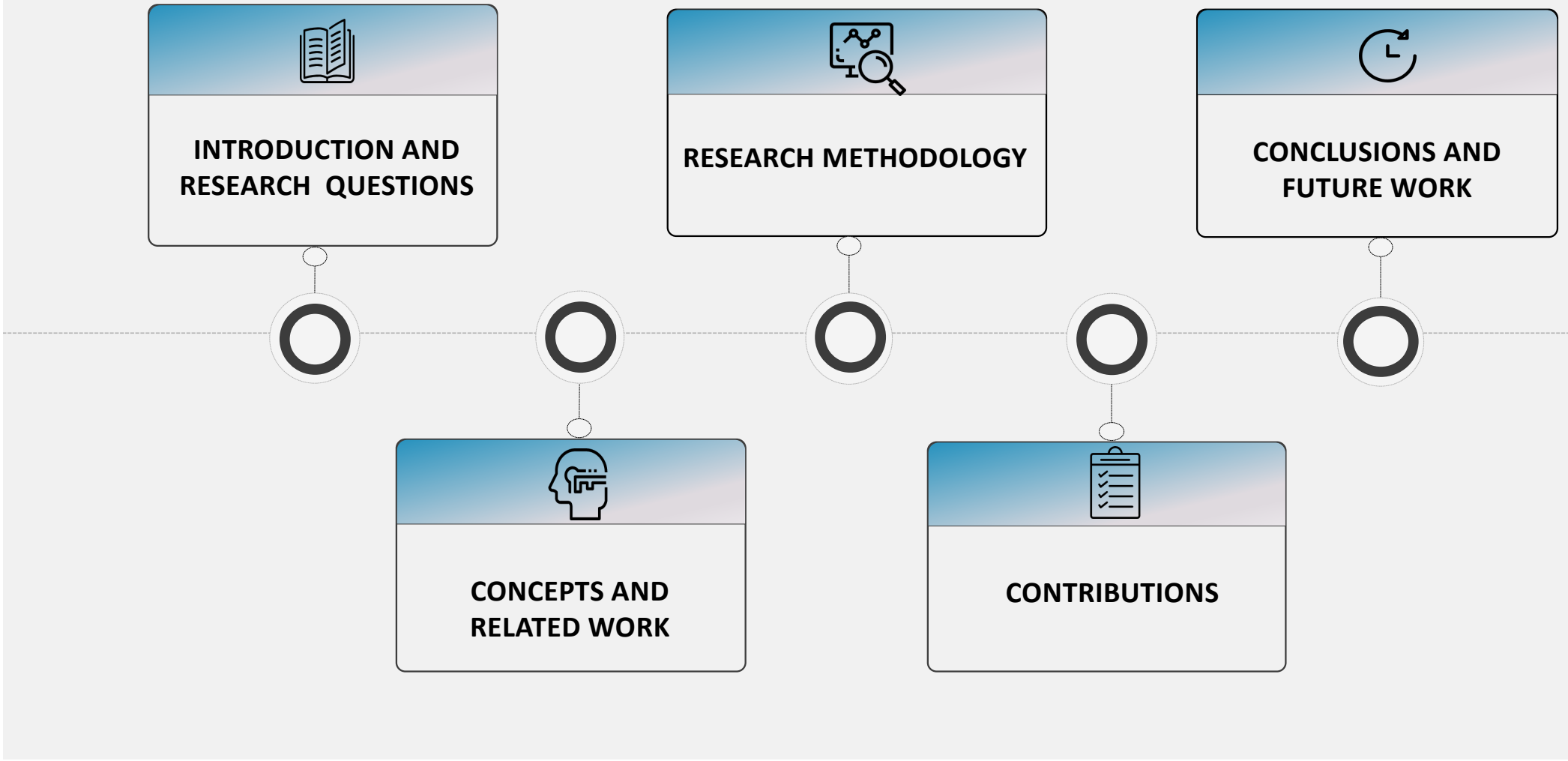

STUDIES IN COMPUTER SCIENCE NO 14, DOCTORAL DISSERTATION
JOSEPH BUGEJA
ON PRIVACY AND SECURITY IN SMART CONNECTED HOMES
MALMÖ UNIVERSITY

AGENDA


INTRODUCTION AND RESEARCH QUESTIONS
CONCEPTS AND RELATED WORK
RESEARCH METHODOLOGY
CONTRIBUTIONS
CONCLUSIONS AND FUTURE WORK

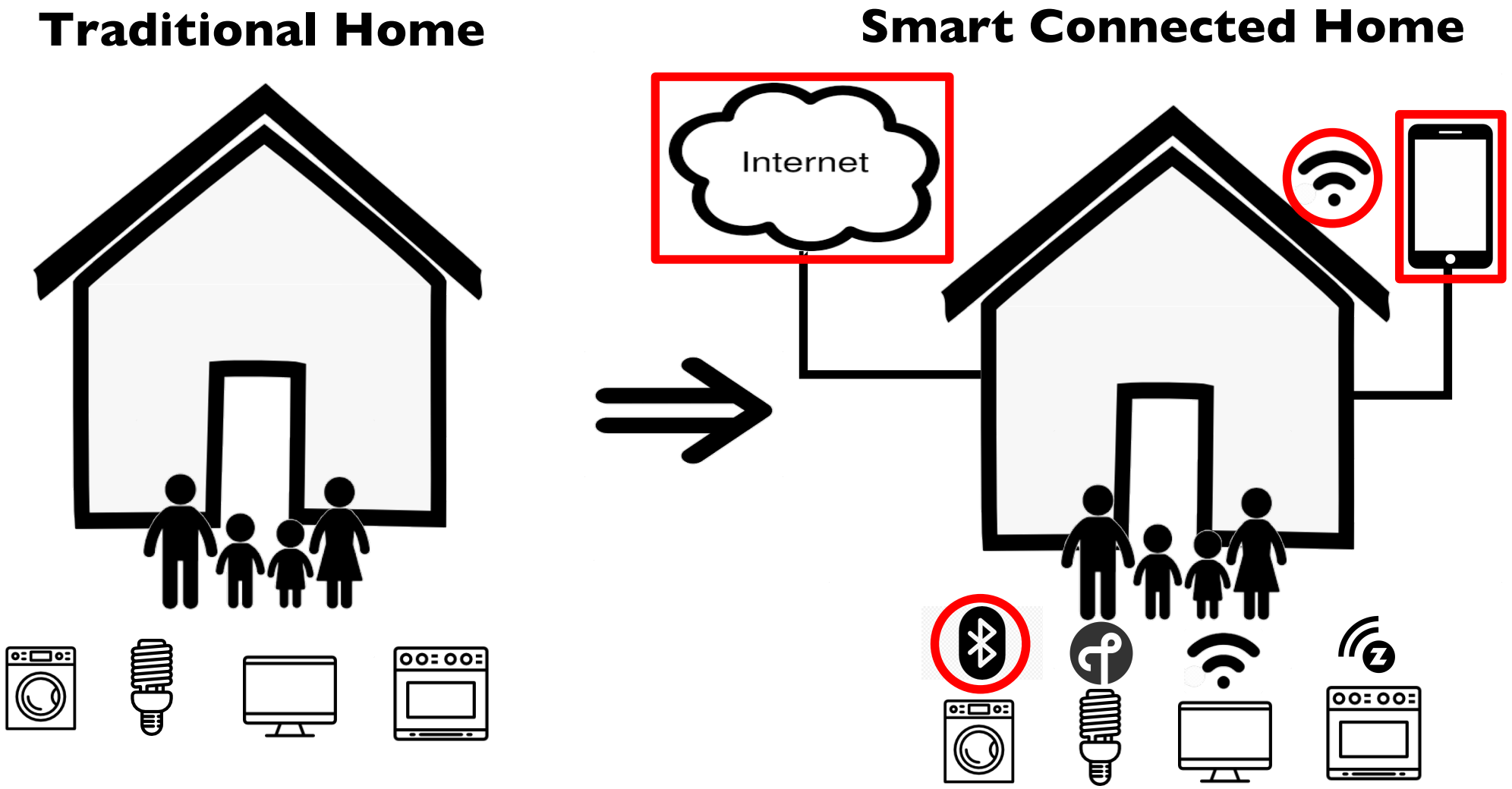
INTRODUCTION AND RESEARCH QUESTIONS

HOME IS WHERE THE HEART IS

- Our home is a deeply meaningful and human place.
- It is a place where our fundamental physical needs are (expected to be) protected.
- The home is *the most powerful sign of the self of the inhabitant who dwells within*[1].

[1] Csikszentmihalyi & Rochberg-Halton, 1981. *The Meaning of Things: Domestic Symbols and the Self.*

EVOLUTION OF THE HOME

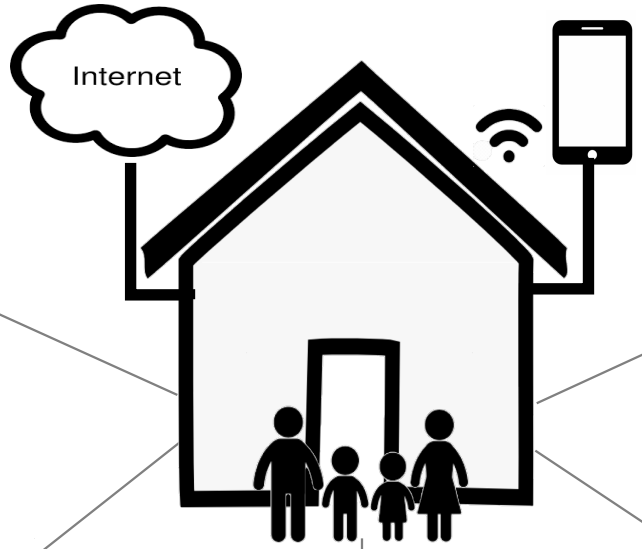


THE SMART CONNECTED HOME

August Smart lock

IFTTT

Door sensor



Google Nest

API, IFTTT

Temperature, Humidity, Proximity, Motion, Ambient light, Optical

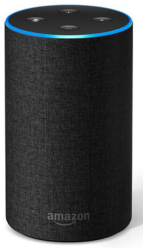
Fitbit Smart Scale

API, IFTTT

Load sensors

Amazon Echo

API, IFTTT, Alexa



Microphone

Facebook Portal

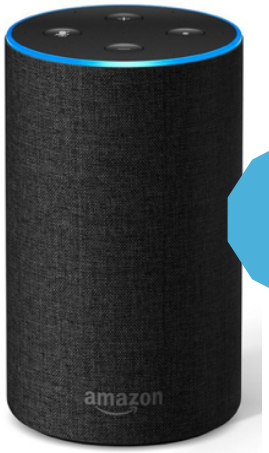
Alexa, FB services (IG, WhatsApp, Messenger)

Microphone, Camera

PRIVACY BREACHES

Amazon Workers Are Listening to What You Tell Alexa

A global team reviews audio clips in an effort to help the voice-activated assistant respond to commands.



100M

Amazon Echo

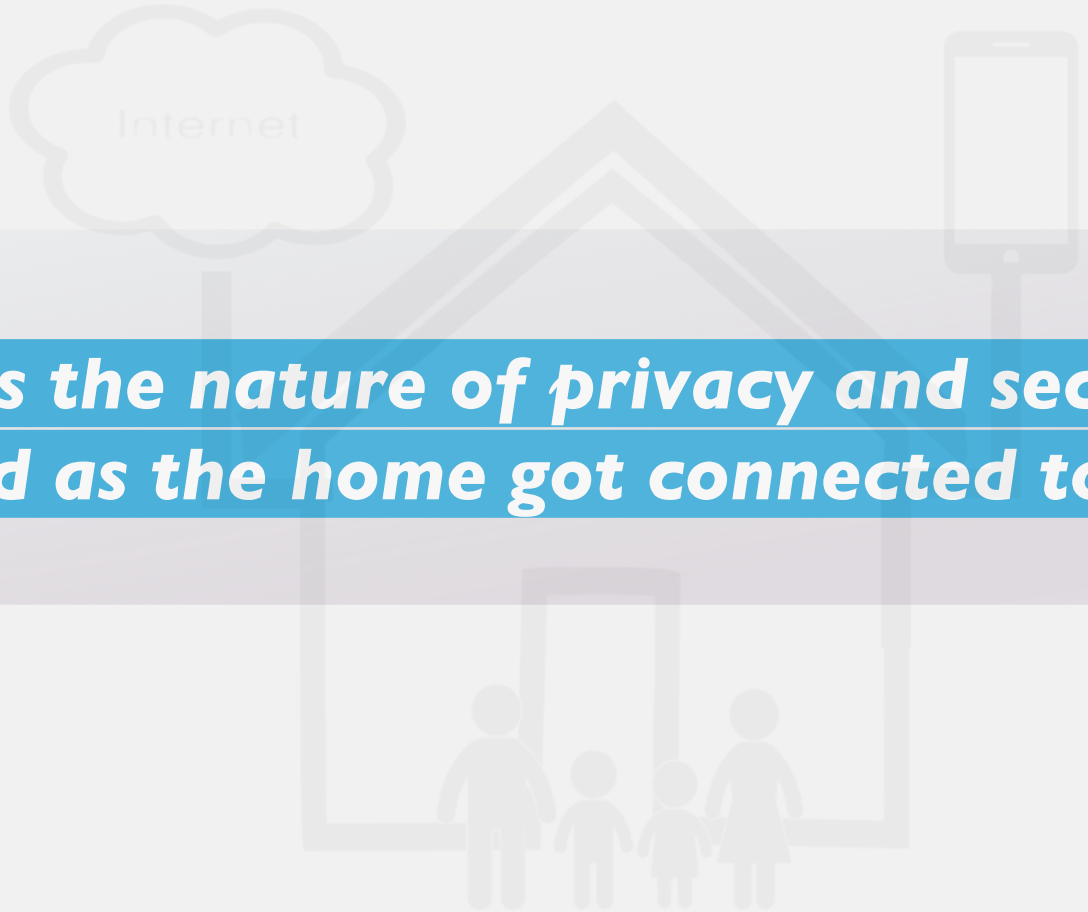
Amazon Listening To What You Tell Alexa

Bloomberg, 2019.

SECURITY BREACHES

The Mirai botnet in 2016 used thousands of hijacked IoT devices, including smart home devices, to bring down the DNS provider Dyn

OVERARCHING RESEARCH QUESTION



How has the nature of privacy and security been transformed as the home got connected to the Internet?

RESEARCH QUESTIONS

- **RQ1:** How can smart connected home devices and the data collected by them be categorized?
- **RQ2:** How can smart connected homes be modeled to support threat identification?
- **RQ3:** How can privacy and security risks affecting smart connected homes be modeled and analyzed?
- **RQ4:** What are the challenges in mitigating privacy and security risks in smart connected homes?

MOTIVATION

No reference taxonomy of smart home devices

No standard representation of the smart connected home

Shortage of methods for conducting risk analysis in IoT applications

Lack of tools for addressing privacy issues during system design

CONCEPTS AND RELATED WORK

PRIVACY

- Warren and Brandeis identified privacy as *the right to be let alone*[2].

- Westin described privacy as *the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others*[3].

- Nissenbaum defined privacy as the appropriateness of information flows in defined contexts[4].

---

[2] Samuel D Warren and Louis D Brandeis. *The Right to Privacy*. Harvard Law Review, page 193–220, 1890.
[3] Alan F Westin. *Privacy and Freedom*. Atheneum, New York, 1967.
[4] Helen Nissenbaum. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press, 2009.

SECURITY

- Security is commonly described in terms of its objectives, namely, that of confidentiality, integrity, and availability.
- Other goals are often added to it, including that of privacy.
- Security is vital to ensure the safe development of our digital world.
- The concepts of security and privacy have some overlapping goals but they are not the same.

THREATS AND RISKS

- Threats are potential occurrences that may result in an unwanted outcome.
- Risks are the potential for a threat to cause harm to an asset.
- Risk analysis is the process used to identify risks.
- Risks can be mitigated through mechanisms.

RESEARCH METHODOLOGY

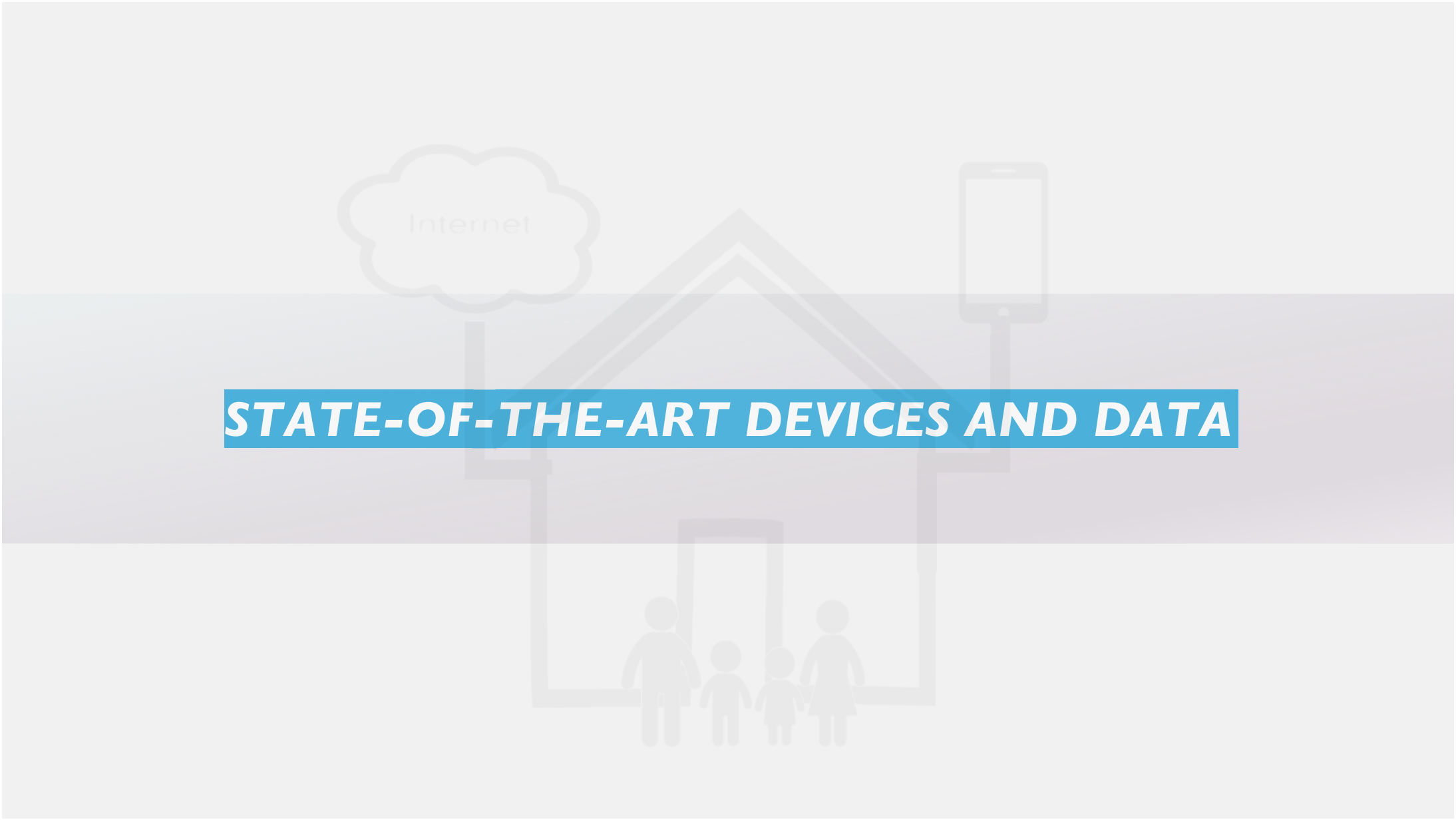
RESEARCH STRATEGIES AND DATA SOURCES

Survey	RQ1, RQ4	• Product databases and manuals • Privacy policies • Literature
Design and Creation	RQ1 – RQ4	• Product databases and manuals • Privacy policies • Simulated data • Vulnerability databases • Reports and news articles • Literature
Case Study	RQ3	• Vulnerability databases • Reports and news articles • Literature

CONSIDERATIONS

- *Ethics:* passive vulnerability scanning, data redaction, authenticated and delayed scraping.
- *Reliability and validity:* multiple product databases, triangulation of data, sample size.
- *Generalizability:* Formal models and insights.

CONTRIBUTIONS

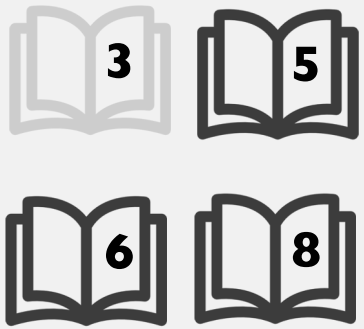


STATE-OF-THE-ART DEVICES AND DATA

STATE-OF-THE-ART DEVICES AND DATA

RQ1 How can smart connected home devices and the data collected by them be categorized?

– Papers –



– Contributions –

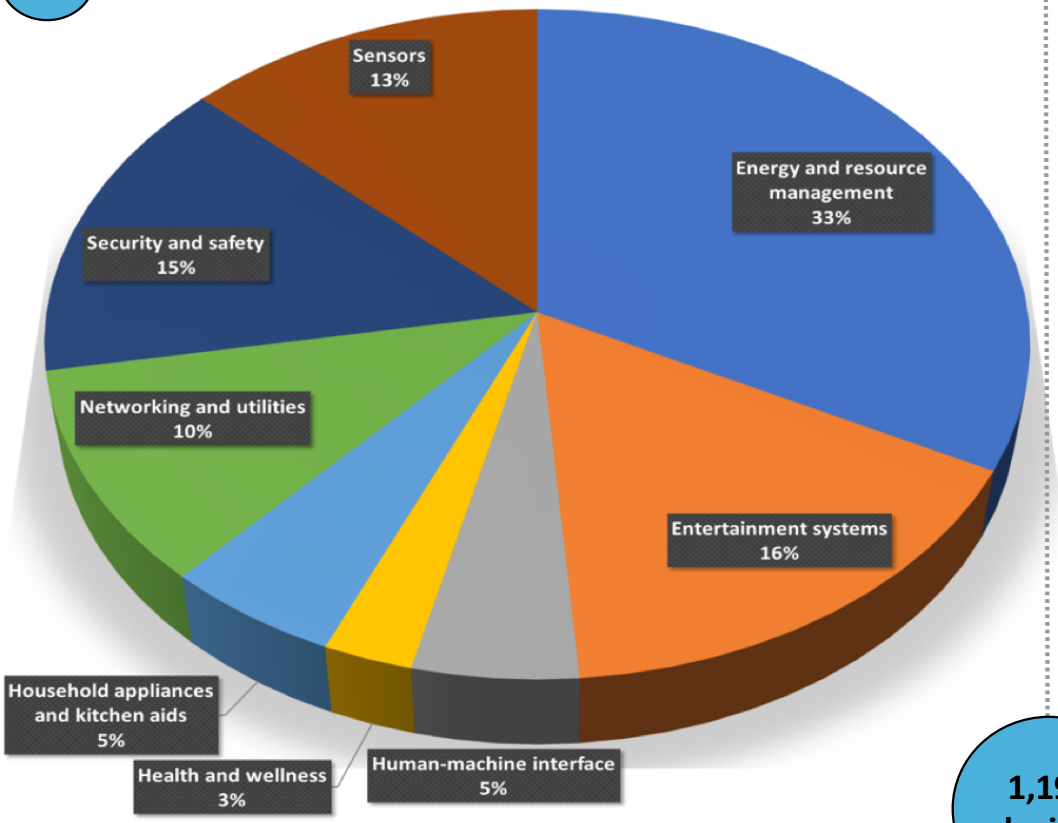
[C1] Taxonomy and analysis of connected devices

[C2] Classification and analysis of connected devices and their apps

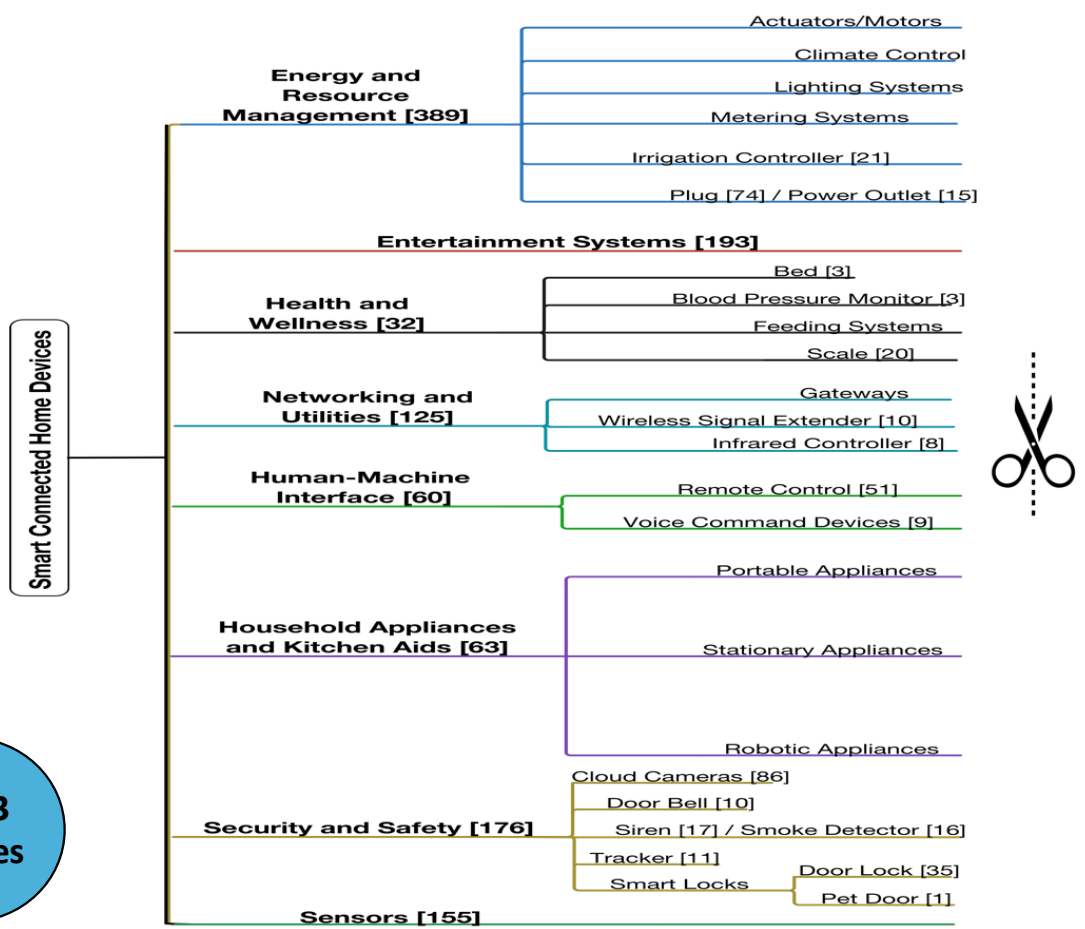
[C3] Analysis and classification of collected data

TAXONOMY AND ANALYSIS

[C1]



1,193 devices

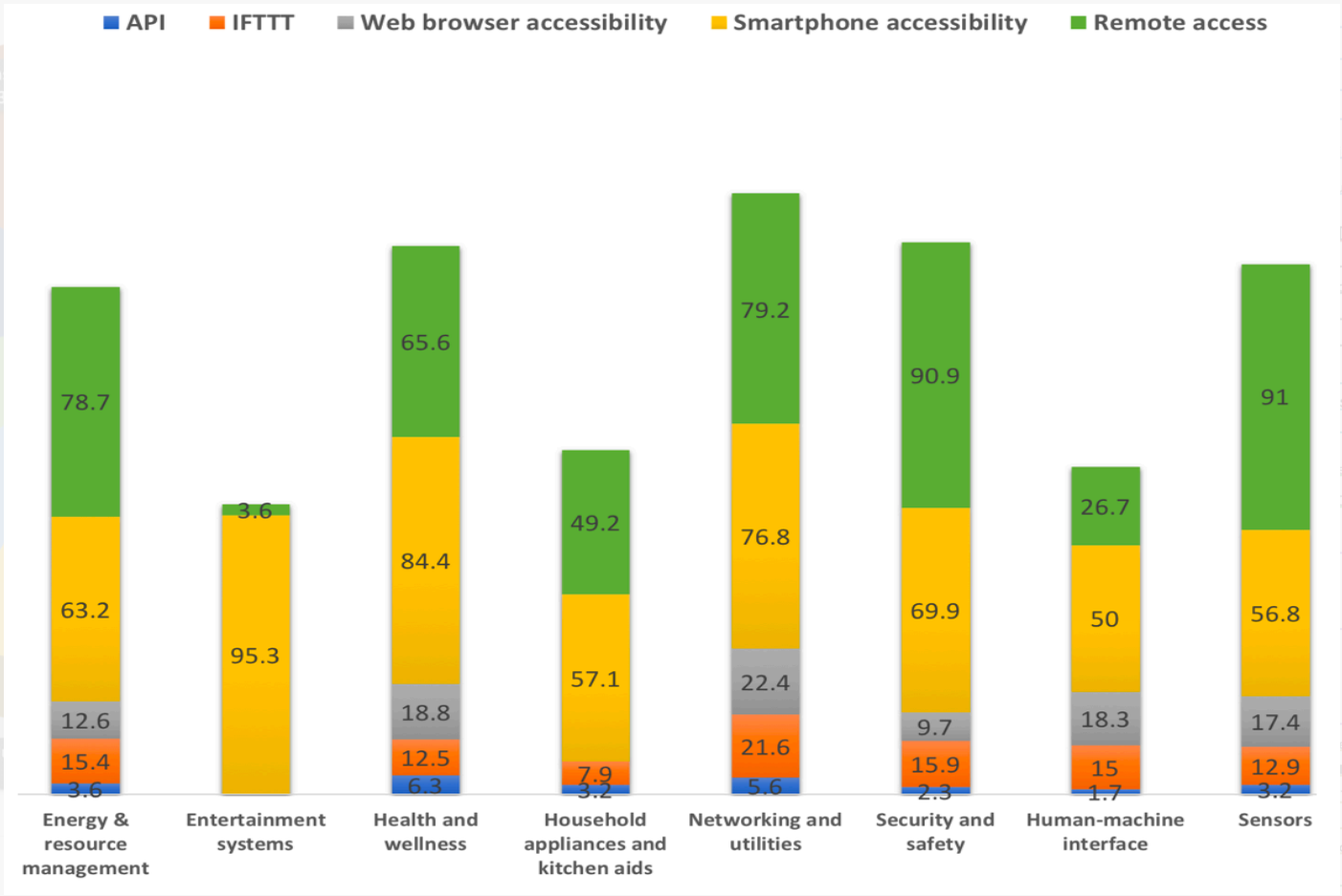


Bugeja, J., Davidsson, P., Jacobsson, A. (2018). Functional Classification and Quantitative Analysis of Smart Connected Home Devices (pp. 1–6). In: *Proceedings of the Global IoT Summit (GIoTS 2018)*. IEEE.

RQ1

TAXONOMY AND ANALYSIS

[C1]



Bugeja, J., Davidsson, P., Jacobsson, A. (2018). Functional Classification and Quantitative Analysis of Smart Connected Home Devices (pp. 1–6). In: *Proceedings of the Global IoT Summit (GIoTS 2018)*. IEEE.

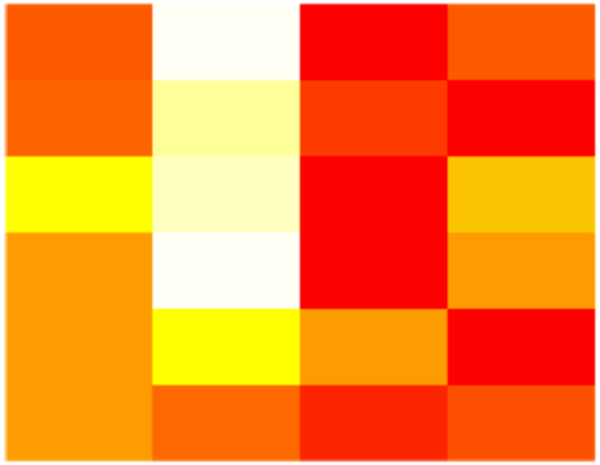
5

RQ1

CLASSIFICATION OF SYSTEMS

[C2]

81 systems



Energy and resource management

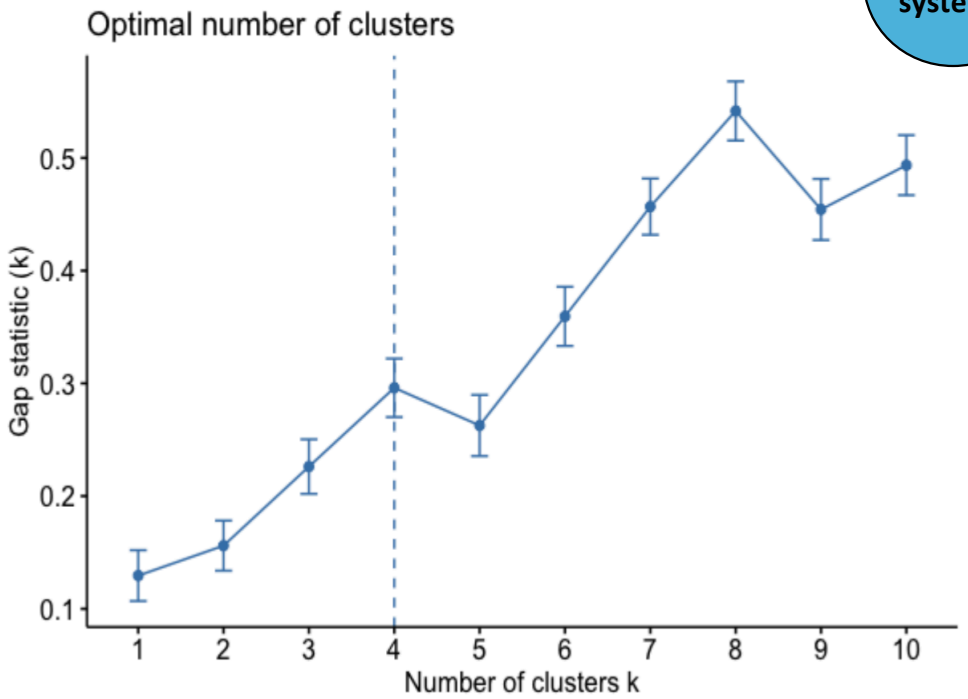
Entertainment systems

Health and wellness

House appliances and kitchen aids

Human-machine interface

Security and safety



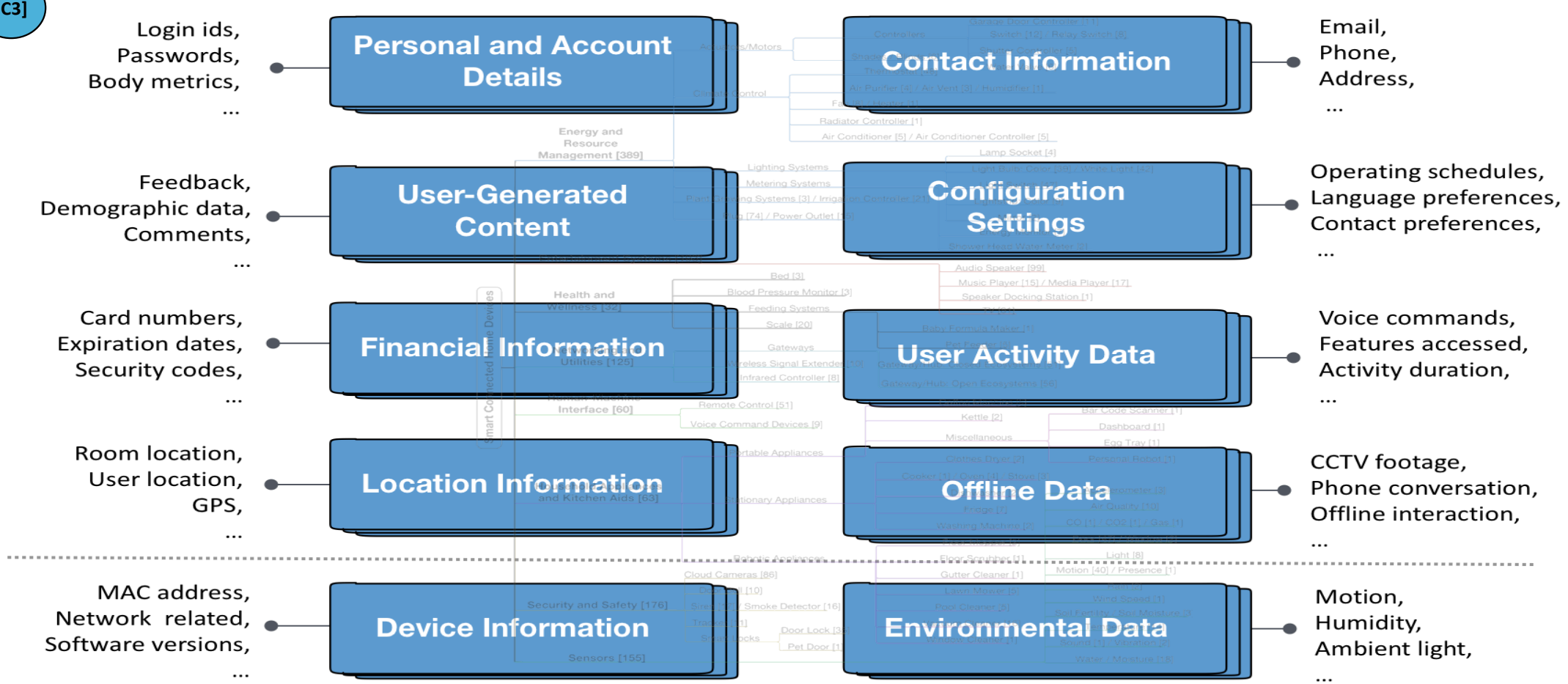
Bugeja, J., Jacobsson, A., Davidsson, P. (2020). Is Your Home Becoming a Spy? A Data-Centered Analysis and Classification of Smart Connected Home Systems. In: *Proceedings of the 10th International Conference on the Internet of Things (IOT 2020).* ACM.

8

RQ1

DATA CATEGORIZATION

[C3]



Bugeja, J., Jacobsson, A., Davidsson, P. (2018). An Empirical Analysis of Smart Connected Home Data (pp. 134–149). In: *Proceedings of the Internet of Things (ICIOT 2018). Lecture Notes in Computer Science,* vol 10972. Springer.

6

RQ1

THREAT IDENTIFICATION AND ANALYSIS

THREAT IDENTIFICATION AND ANALYSIS

RQ2

How can smart connected homes be modeled to support threat identification?

– Papers –

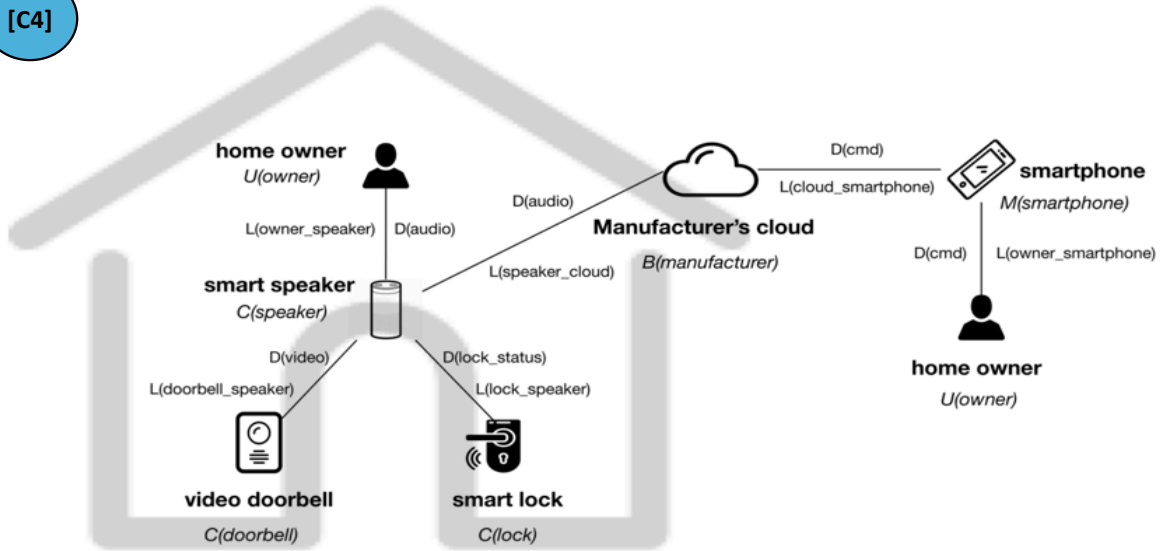
– Contributions –

[C4] Privacy-centered system model

[C5] Privacy-centered data lifecycle

PRIVACY-CENTERED SYSTEM MODEL

[C4]



Nodes, $N = \{doorbell, lock, speaker, manufacturer, smartphone\}$
$C(speaker).capabilities = \{gateway, storage, processing, interaction\}$
$B(manufacturer) = cloud$

Policy, $P =$
$\{(doorbell\_speaker, \{(video, \{read\})\}, doorbell, speaker, \emptyset),$
$(lock\_speaker, \{(lock\_status, \{read\})\}, lock, speaker, \emptyset),$
$(speaker\_cloud, \{(audio, \{read\})\}, speaker, manufacturer,$
$Time = \{8:00 - 24:00\} \wedge Location = \{house\}),$
$(cloud\_smartphone, \{(cmd, \{read\})\}, smartphone,$
$manufacturer, \emptyset),$
$(owner\_smartphone, \{(cmd, \{read\})\}, owner, smartphone, \emptyset),$
$(owner\_speaker, \{(audio, \{read\})\}, owner, speaker, \emptyset)\}$

Identification

Localization and Tracking

Profiling

○ **Threat does not exist**

◐ **Threat is a potential future threat**

● **Threat is present**

Bugeja, J., Jacobsson, A., Davidsson, P. (2020). A Privacy-Centered System Model for Smart Connected Homes (pp. 1–4). In: *Proceedings of the International Conference on Pervasive Computing and Communications Conference (PerCom Workshops 2020).* IEEE.

PRIVACY-CENTERED DATA LIFECYCLE

[C5]

Information privacy threats	Protection goals	Data generation	Data collection	Data processing	Data disclosure
Identification	Unlinkability	◐	◐	●	○
Localization and tracking	Unlinkability	◐	◐	●	○
Profiling	Unlinkability	○	◐	◐	●
Linkage	Unlinkability	○	◐	◐	●
Privacy-violating interaction and presentation	Confidentiality	●	○	○	●
Inventory attacks	Detectability	○	●	○	○
Lifecycle transitions	Transparency	○	●	○	○

Bugeja, J., Jacobsson A. (2020). On the Design of a Privacy-Centered Data Lifecycle for Smart Living Spaces (pp. 126-141). In: *Friedewald M., Önen M., Lievens E., Krenn S., Fricker S. (eds) Privacy and Identity Management. Data for Better Living: AI and Privacy. Privacy and Identity 2019. IFIP Advances in Information and Communication Technology*, vol 576. Springer.

7

RQ2

RISK MODELING

RISK MODELING

RQ3

How can privacy and security risks affecting smart connected homes be modeled and analyzed?

– Papers –

– Contributions –

[C6] Threat agent model

[C7] Framework for modeling and analyzing privacy risks

VULNERABILITIES IN CONNECTED CAMERAS

[C6]

SHODAN

{Threat Agent :: Hacker}

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	104[redacted]
ip_str	62.[redacted]
isp	Unitymedia
last_update	2018-03-20T19:29:37.676273
latitude	51.5221
longitude	7.0575
org	Unitymedia
os	null
ports	[554]
postal_code	[redacted]
region_code	07

National Interests

Terrorism

Personal Gain

Curiosity

High
CVE-2007-5213

Medium
CVE-2011-5261

Critical
CVE-2015-2887

Hackers Thieves Hacktivists Competitors and Organized Crime Terrorists Nation States

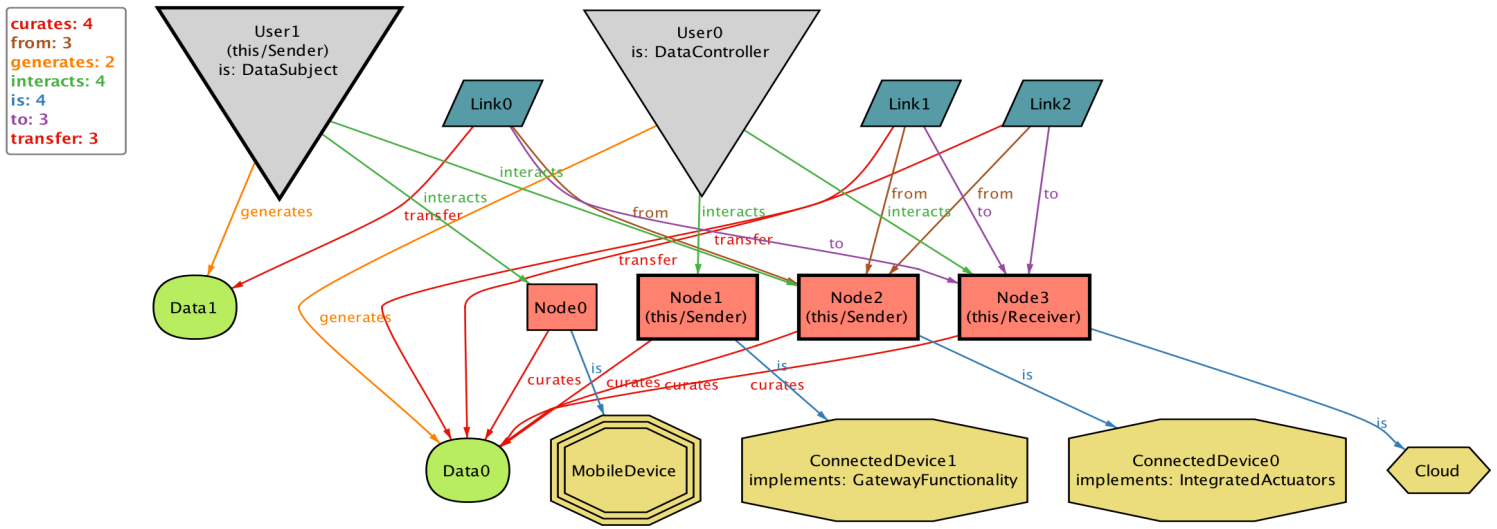
An Investigation of Vulnerabilities in Smart Connected Cameras (pp. 537–542). In: *Proceedings of the International Conference on Pervasive Computing and Communications Conference (PerCom Workshops 2018)*. IEEE.

4

RQ3

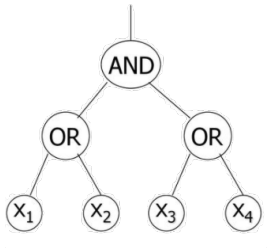
PRIVACY RISK ANALYSIS OF SMART HOMES

[C7]



$$\alpha_l = \begin{cases} \prod_{i=1}^{n} \alpha_{l.i}, & \text{if } AND \text{ node} \\ max(\alpha_{l.i}), i = 1...n, & \text{if } OR \text{ node} \end{cases}$$

$$\alpha_i = max(\alpha_{i.i}), i = 1...n, \text{for both } AND \text{ or } OR \text{ node}$$



$$\begin{aligned} \alpha_l &= max((\alpha_{l.v_1} \times \alpha_{l.v_2}), \alpha_{l.v_3}, (\alpha_{l.v_4} \times \alpha_{l.v_5}), \alpha_{l.v_6}, \alpha_{l.v_7}, \alpha_{l.v_8}) \\ &= max((0.2 \times 0.4), 0.8, (0.1 \times 0.3), 0.3, 0.2, 0.2) \\ &= max(0.08, 0.8, 0.03, 0.3, 0.2, 0.2) \\ &= 0.8 \end{aligned}$$

Bugeja, J., Jacobsson, A., Davidsson, P. (2020). PRASH: A Framework for Privacy Risk Analysis of Smart Homes. Submitted to *ACM Digital Threats: Research and Practice (DTRAP)*.

CHALLENGES AND MITIGATIONS

CHALLENGES AND MITIGATIONS

RQ4

What are the challenges in mitigating privacy and security risks in smart connected homes?

– Papers –

– Contributions –

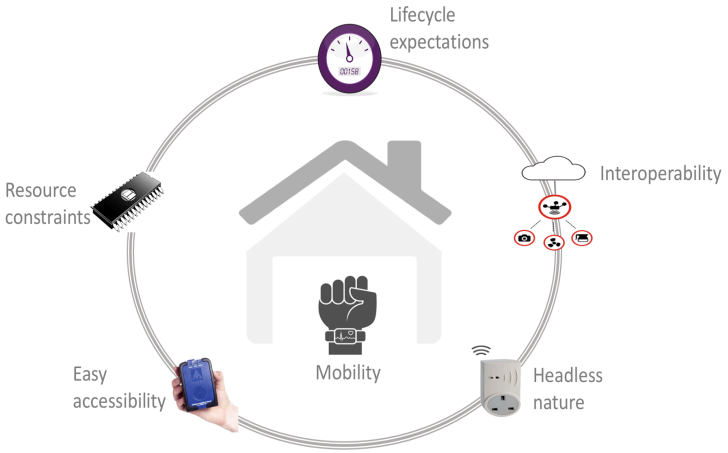
[C8] Identification of security challenges and their mitigations

CHALLENGES AND MITIGATIONS

[C8]

- Mitigations :: Architecture level

DEVICE	COMMUNICATION	SERVICE
• H/W enc, fail-secure design, and device authZ • Enhanced algorithms, e.g. DTLS and ECSDA • Platforms such as RERUM • CC and EMVCo IC SE	• VPNs, firewalls, IDS, and IPS • TOR-based systems • Devices such as Cujo, Dojo, and Keezel • ENISA, CSA, etc.	• Security testing, secure design, and data masking • Cryptographic schemes • OWASP, Builditsecure.ly, I Am the Cavalry • Sites such as BugCrowd

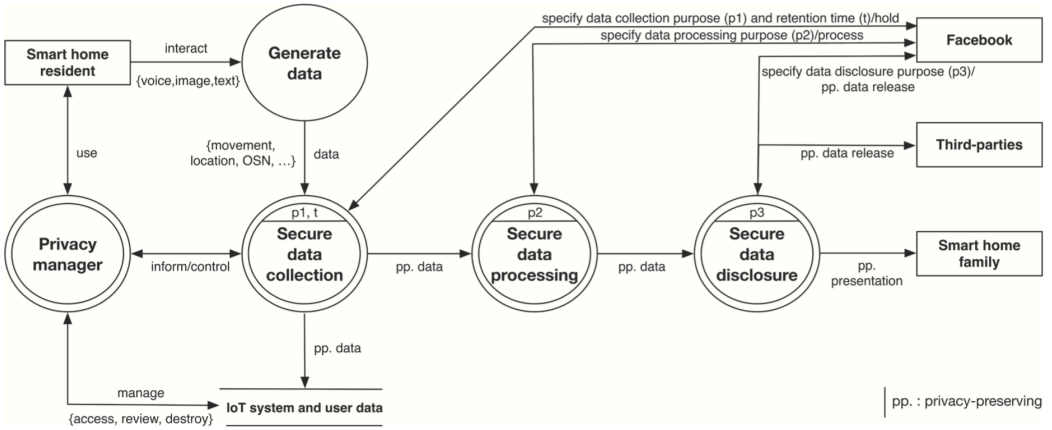


Challenges

Bugeja, J., Jacobsson, A., Davidsson, P. (2016). On Privacy and Security Challenges in Smart Connected Homes (pp. 172–175). In: *Proceedings of the 2016 Intelligence and Security Informatics Conference (EISIC 2016).* IEEE.

1 RQ4

- Mitigations :: Development lifecycle



Bugeja, J., Jacobsson A. (2020). On the Design of a Privacy-Centered Data Lifecycle for Smart Living Spaces (pp. 126-141). In: *Friedewald M., Önen M., Lievens E., Krenn S., Fricker S. (eds) Privacy and Identity Management. Data for Better Living: AI and Privacy. Privacy and Identity 2019. IFIP Advances in Information and Communication Technology*, vol 576. Springer.

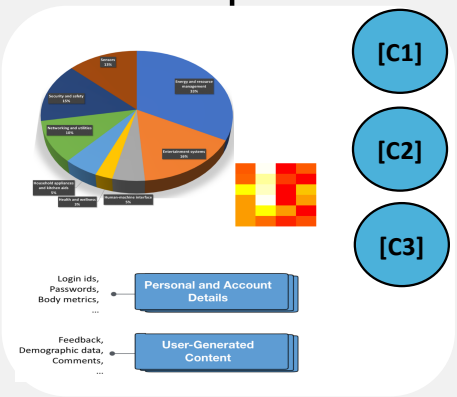
7 RQ4

SUMMARY OF CONTRIBUTIONS

{assets}

RQ1

Papers: 3,5,6,8



[C1]

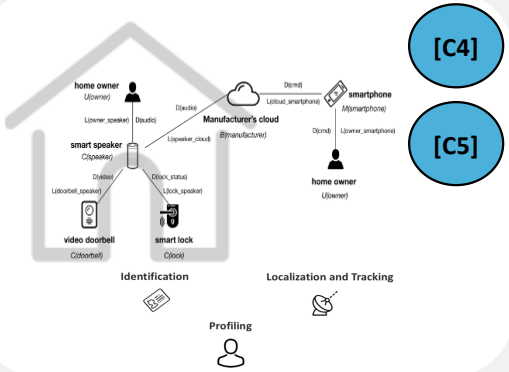
[C2]

[C3]

{threats}

RQ2

Papers: 7,9



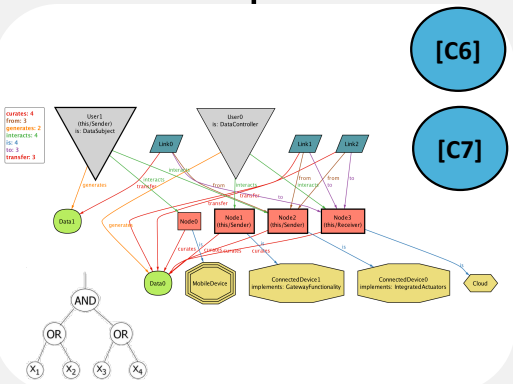
[C4]

[C5]

{risks}

RQ3

Papers: 2,4,10



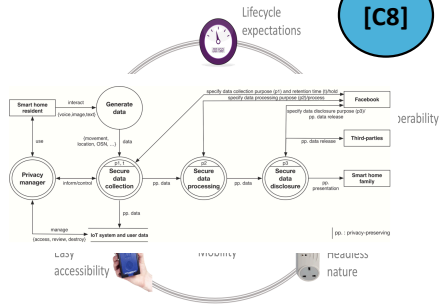
[C6]

[C7]

{mitigations}

RQ4

Papers: 1,3,7



[C8]

CONCLUSIONS AND FUTURE WORK

CONCLUSIONS

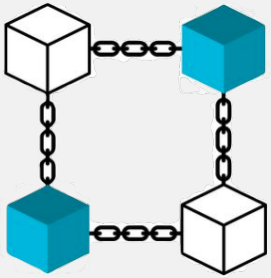
- Threat agents are finding ways to learn how to tap into the smart connected home and looking for new ways to attack in-home technologies.

- In the dissertation, we presented contributions that enable early identification of threats, better planning for risks, and enable informed decisions about mitigations of potential impacts.

- The presented contributions provide a foundation that helps deepen the understanding of privacy and security in smart connected homes.

FUTURE WORK

Embedding privacy- and security-enhancing mechanisms into connected devices

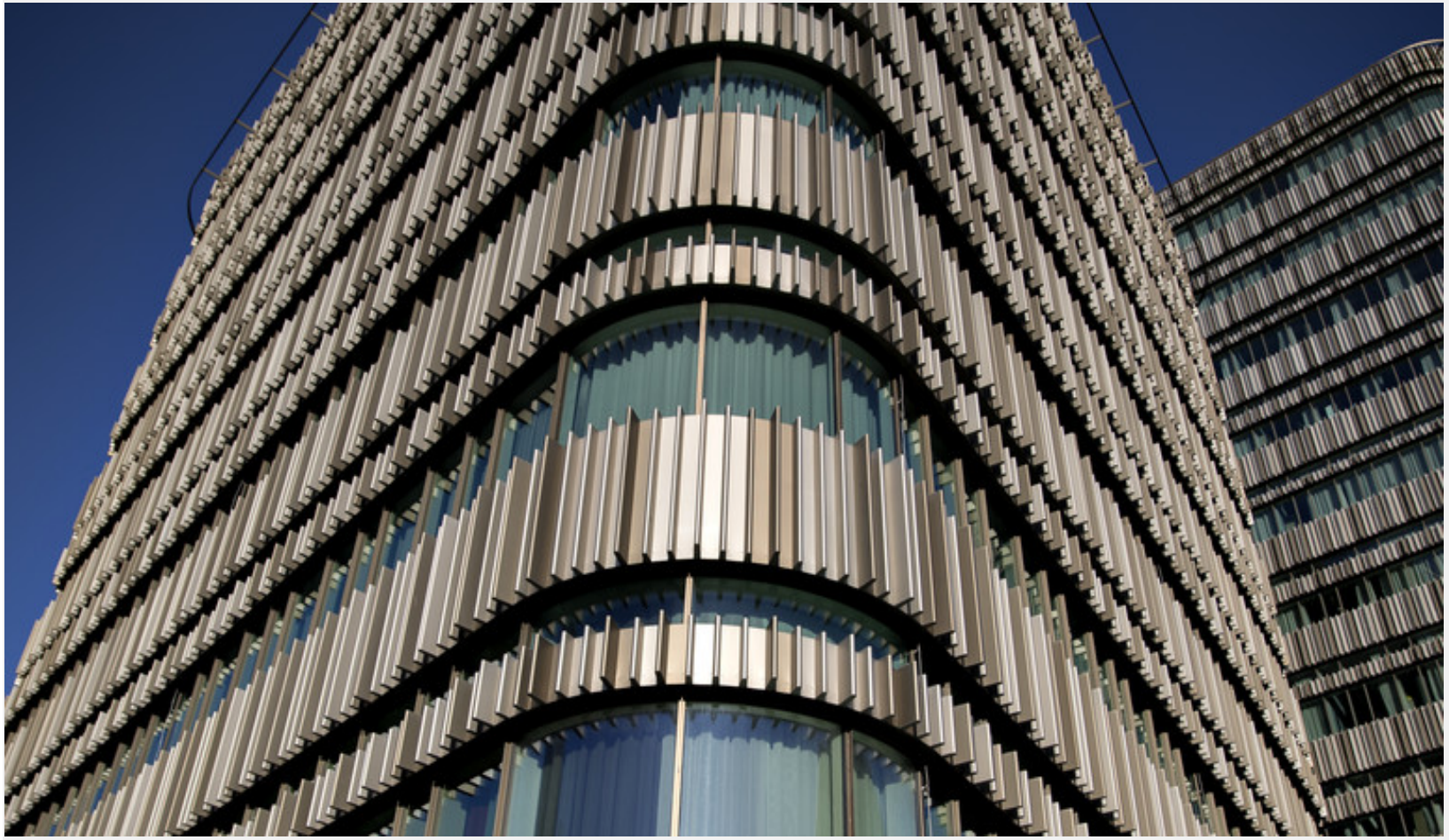


Blockchain as a privacy- and security-enhancing mechanism

AI

AI as a mechanism for automatically responding to threats

Thank you for your attention!



Source: mau.se

Joseph Bugeja

joseph.bugeja@mau.se