

# Operational Security Analysis and Challenge for IoT Solutions

**INFORMATIK2020 / WS 4: I4.0 ACS 2020**

Karlsruhe, Germany, 2020-09-28

**Author:**

Yuan Gao    Universität Magdeburg -OVGU (yuan.gao@ovgu.de)

Xinxin Lou    Bielefeld University

# Why is IoT / IIoT important?

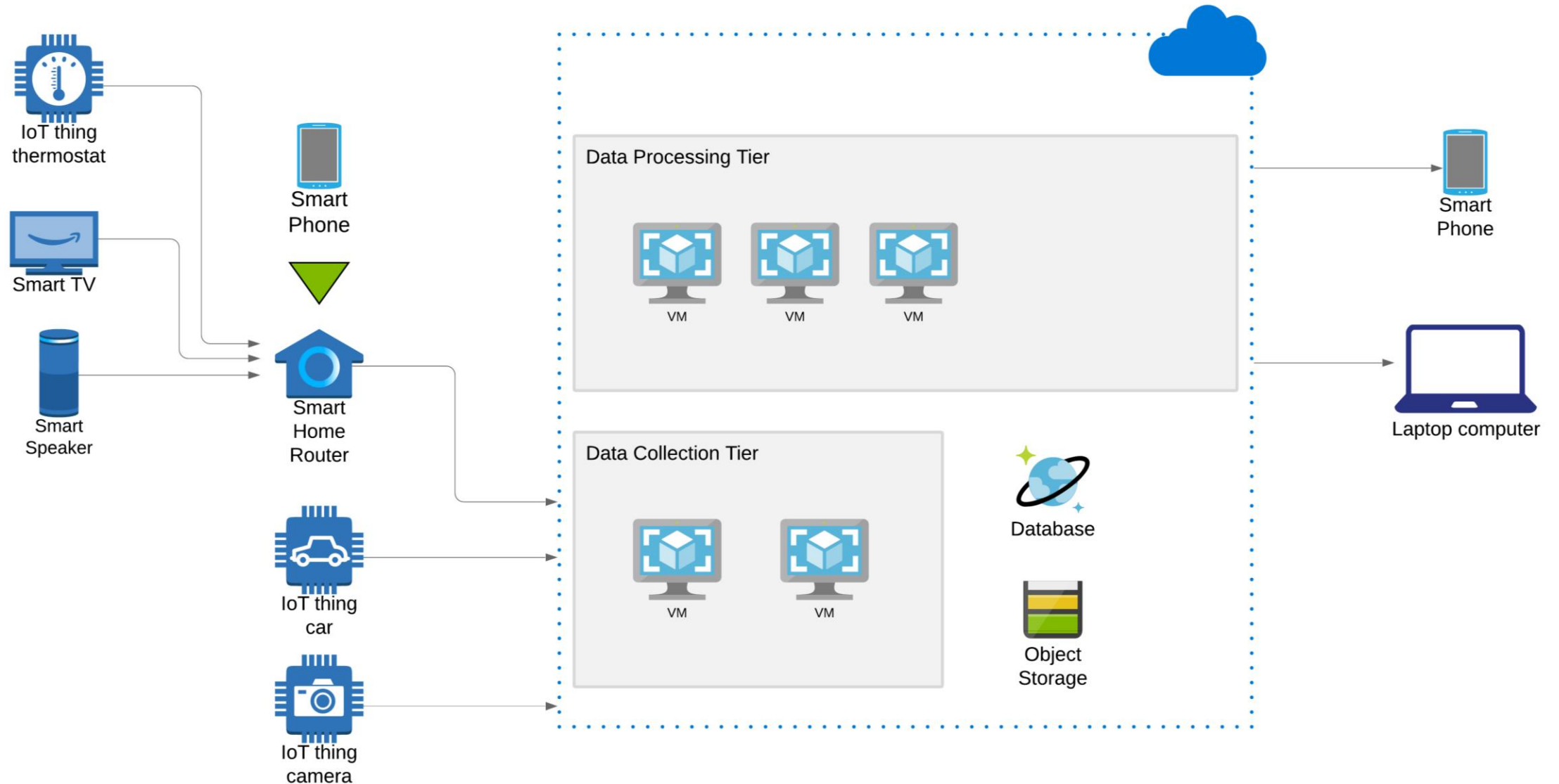
- Huge market: 1 trillion until 2025
- One foundation of Industrie 4.0
- New business models,
  - e.g. such as Drone Delivery and Smart “Everything”
- Critical Security Challenges
  - Regulations, especially regarding privacy
  - Identity Access Management (IAM)

# Outline



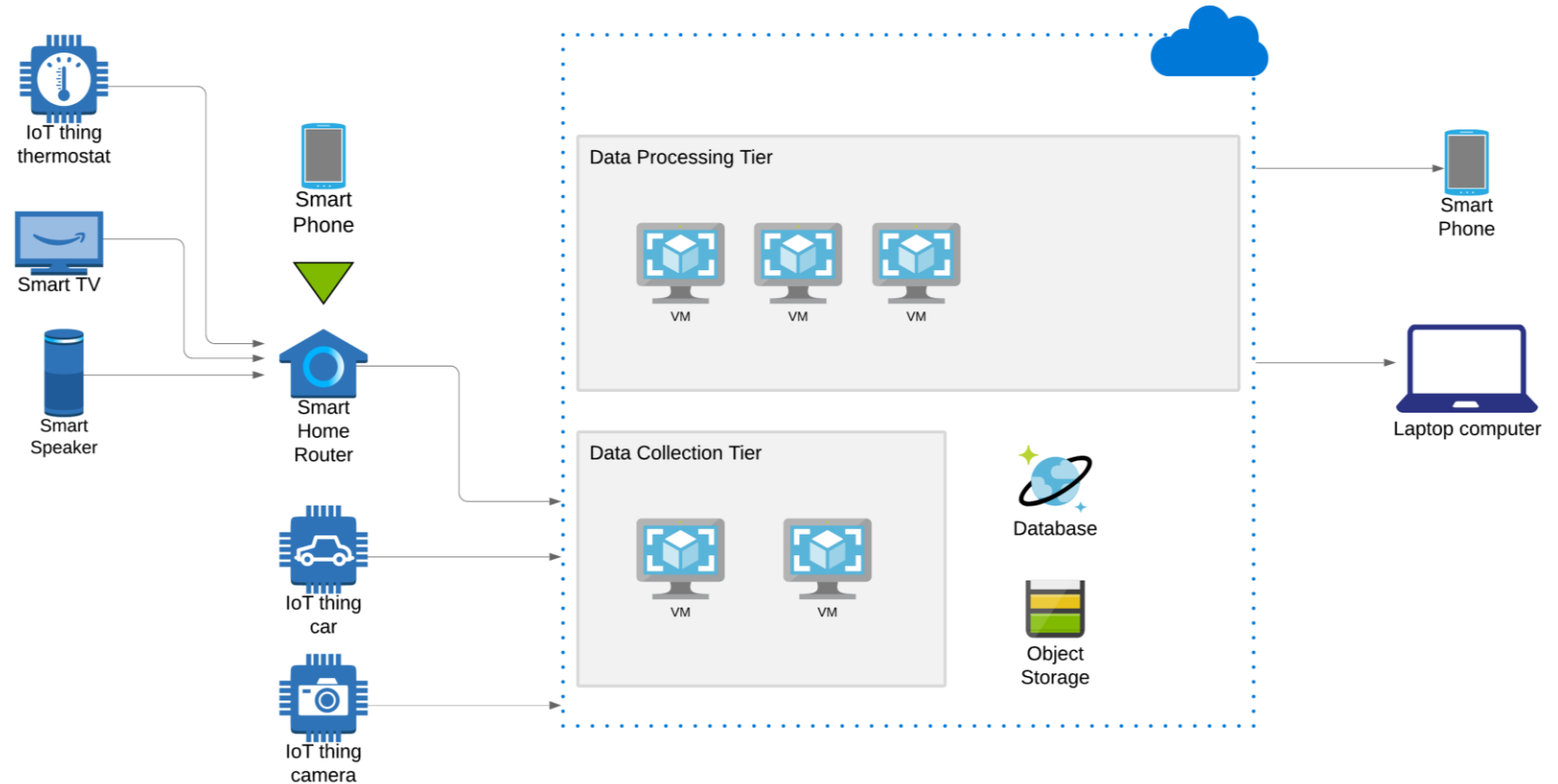
- A general IoT Solution Architecture
- Challenges of Perimeter Model
- Zero Trust Model (3 Rules)
- IoT vs. IIoT (optional)

# IoT Architecture



# Components

- IoT Devices
  - normal ones
  - Edge Devices
- Terminals
- IoT Applications
  - on cloud
  - on devices
  - on terminals

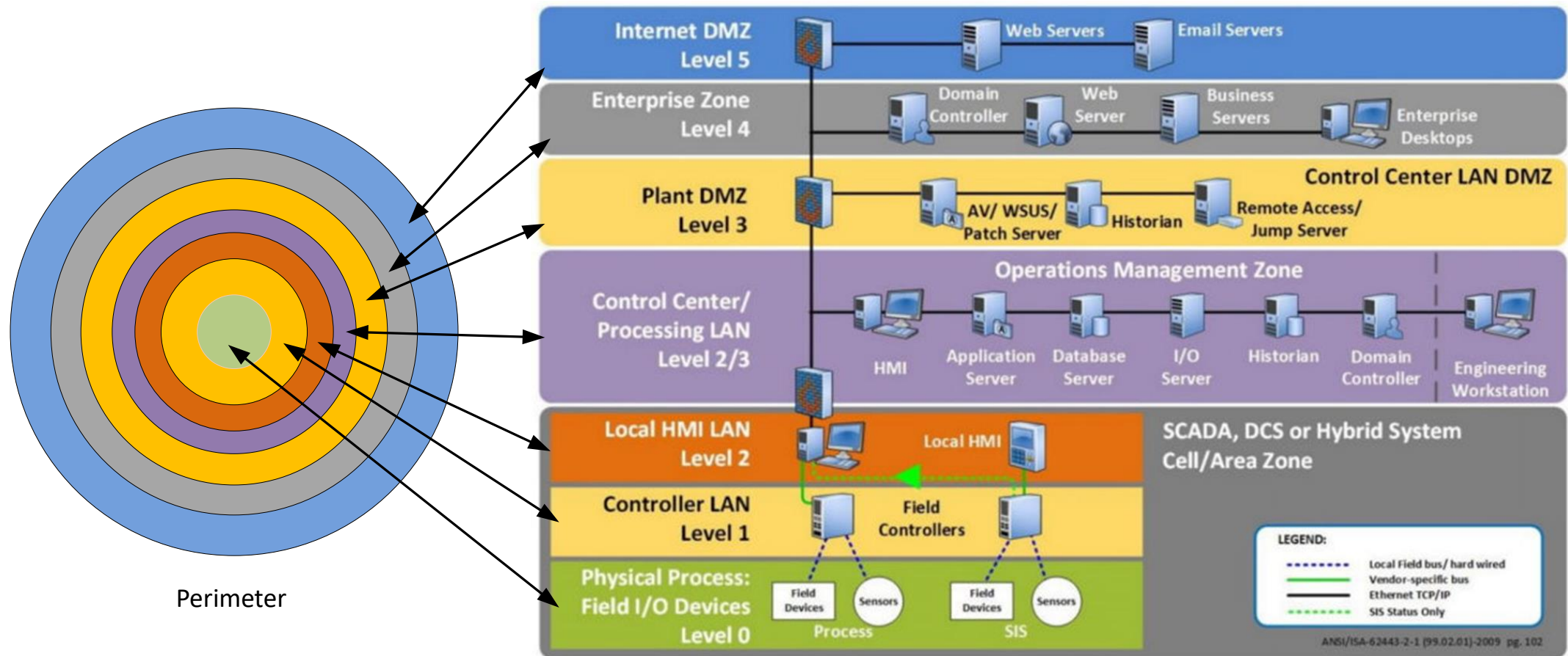


# Outline



- A general IoT Solution Architecture
- **Challenges of Perimeter Model**
- Zero Trust Model (3 Rules)
- IoT vs. IIoT (optional)

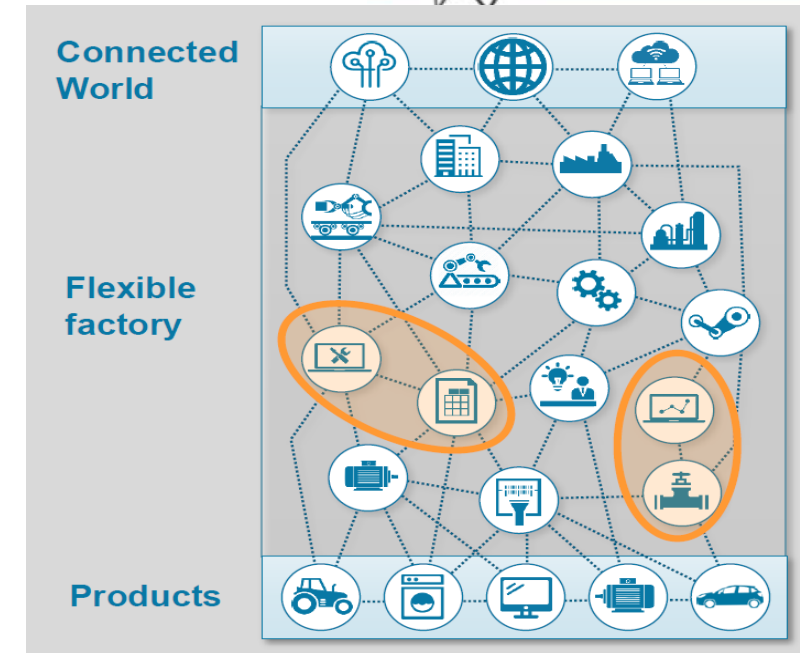
# ISA Purdue Model



Structure [source: <https://dale-peterson.com/2019/02/11/is-the-purdue-model-dead/>]

# Challenges P-Model

- Challenges:
  - Shared Infrastructure on the Cloud
  - SDN rather than Network Segmentation
  - No static Assets Inventory, especially in I4.0



- Problem: no static structure for security evaluation
- Solution: evaluate access explicitly each time – Zero Trust Model

Picture source: [https://www.plattform-i40.de/PI40/Redaktion/EN/Downloads/Publikation/rami40-an-introduction.pdf?\\_\\_blob=publicationFile&v=4](https://www.plattform-i40.de/PI40/Redaktion/EN/Downloads/Publikation/rami40-an-introduction.pdf?__blob=publicationFile&v=4)



# Outline



- A general IoT Solution Architecture
- Challenges of Perimeter Model
- **Zero Trust Model (3 Rules)**
- IoT vs. IIoT (optional)

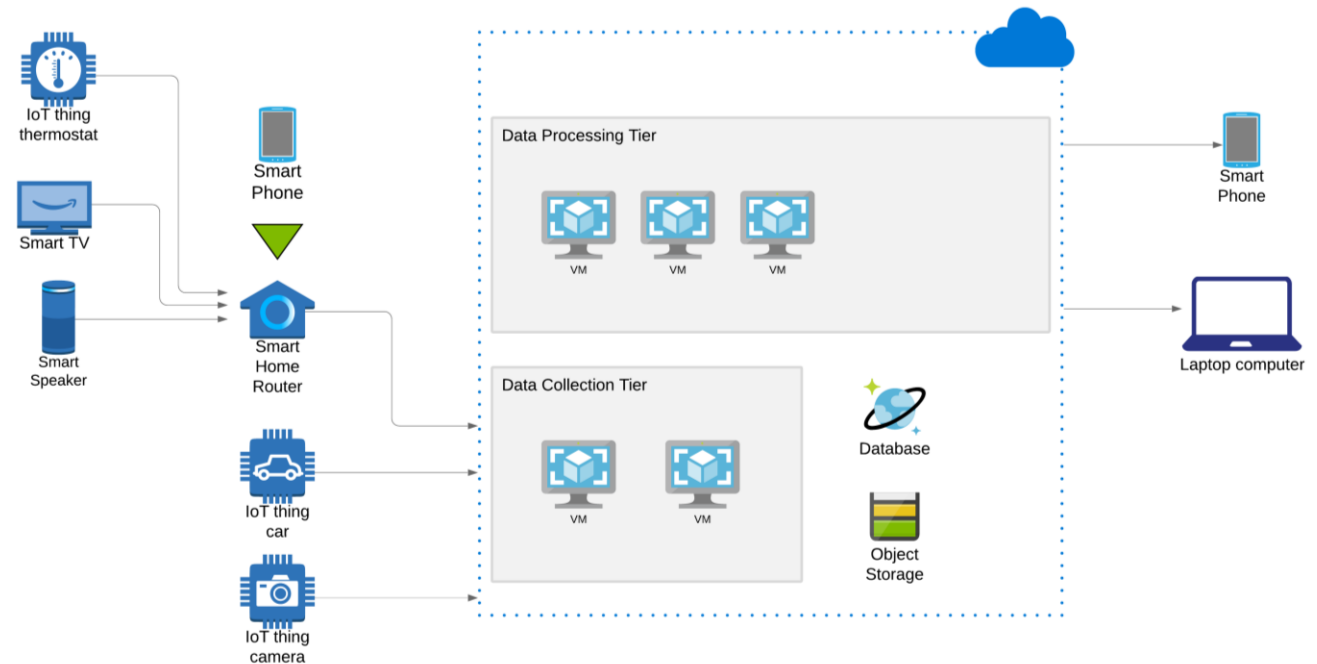
# Zero Trust Model



- Rule 1 – Traced Access: all data access must be traced and stored in logs.
- Rule 2 – Explicit Evaluation: access authorization must be evaluated explicitly before deciding Allow or Deny.
- Rule 3 – Automatic Revocation: under certain conditions, the system is capable of revoking data access authorization automatically.

# Examples

- Edge Location
  - Put a rogue device in the smart home
    - eavesdropping , DDoS
- Cloud Location
  - Insufficient logging



# Mitigations

- Edge Location
  - threat:
    - put a rogue device in the smart home
  - mitigation:
    - Rule 2 and 3
- Cloud Location
  - threat:
    - Insufficient logging
  - mitigation:
    - Rule 1

**Table1: Rules of Zero-Trust model**

Rule	Description
Rule 1	Traced Access
Rule 2	Explicit Evaluation
Rule 3	Automatic Revocation

# Outline



- A general IoT Solution Architecture
- Challenges of Perimeter Model
- Zero Trust Model (3 Rules)
- **IoT vs. IIoT(optional)**

# Differences: IoT vs. IIoT



- Availability vs. Confidentiality
  - For IACS (Industrial Automation and Control Systems), the system availability has higher priority
  - The Rule 2 (Explicit Evaluation) might not be feasible
- Safety vs. Privacy
  - Functional Safety is strictly regulated while regulation on privacy is being progressed.

# Trade-Offs



- Implementations of Rule 2 and 3 can be flexible.
- Zero Trust Model and Perimeter Model can be applied to different sub-systems
  - Control system – perimeter security model
  - Additional IoT sensor system – zero trust model

# Summary



- A general IoT Solution Architecture
- Zero Trust Model with 3 Rules
- How to Build the Security Architect of IoT Systems?



# Operational Security Analysis and Challenge for IoT Solutions

**INFORMATIK2020 / WS 4: I4.0 ACS 2020**  
Karlsruhe, Germany, 2020-09-28

- **Author:**
- Yuan Gao    Universität Magdeburg -OVGU (yuan.gao@ovgu.de)
- Xinxin Lou    Bielefeld University

Thanks!

Questions?