CDIS CENTER FOR CYBER DEFENCE AND INFORMATION SECURITY

KTH VETENSKAP OCH KONST

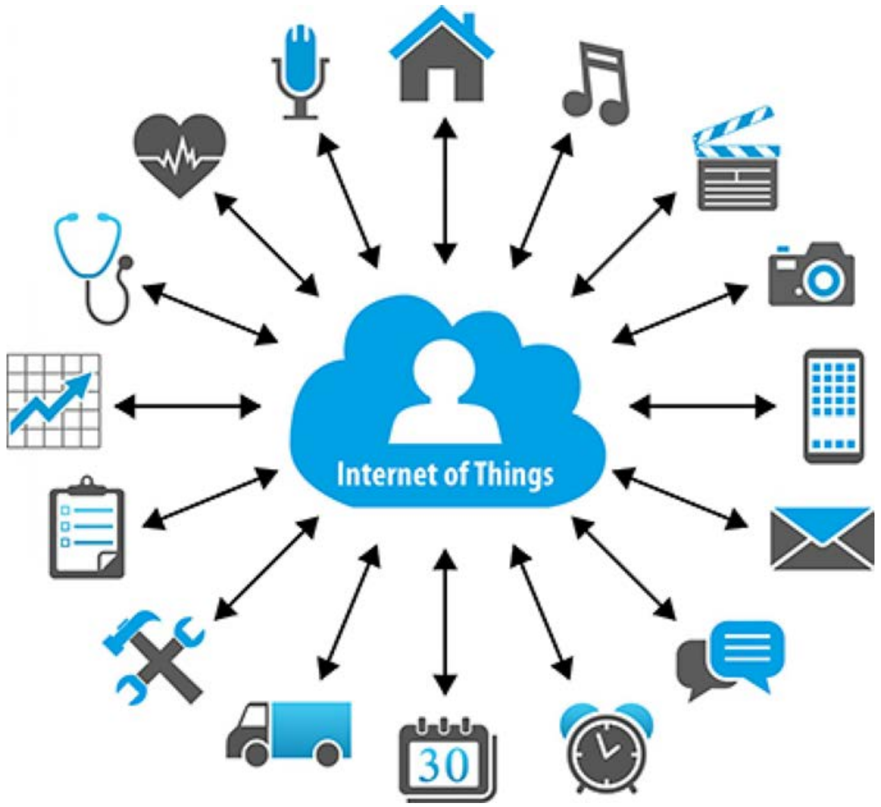
A Security-Aware Multi-User Architecture for IoT

Musard Balliu, KTH

CDIS Spring Conference 2022
KTH Royal Institute of Technology
Tuesday, May 24, 2022

Internet of Things

- Internet of Things
  - Connectivity is great, but ...
  - Incompatible standards, platforms, technologies
  - Holding back the market potential
    - Increased development cost and complexity
    - Harder to realize and monetize the value of data



Web of Things

Internet of Things (IoT)

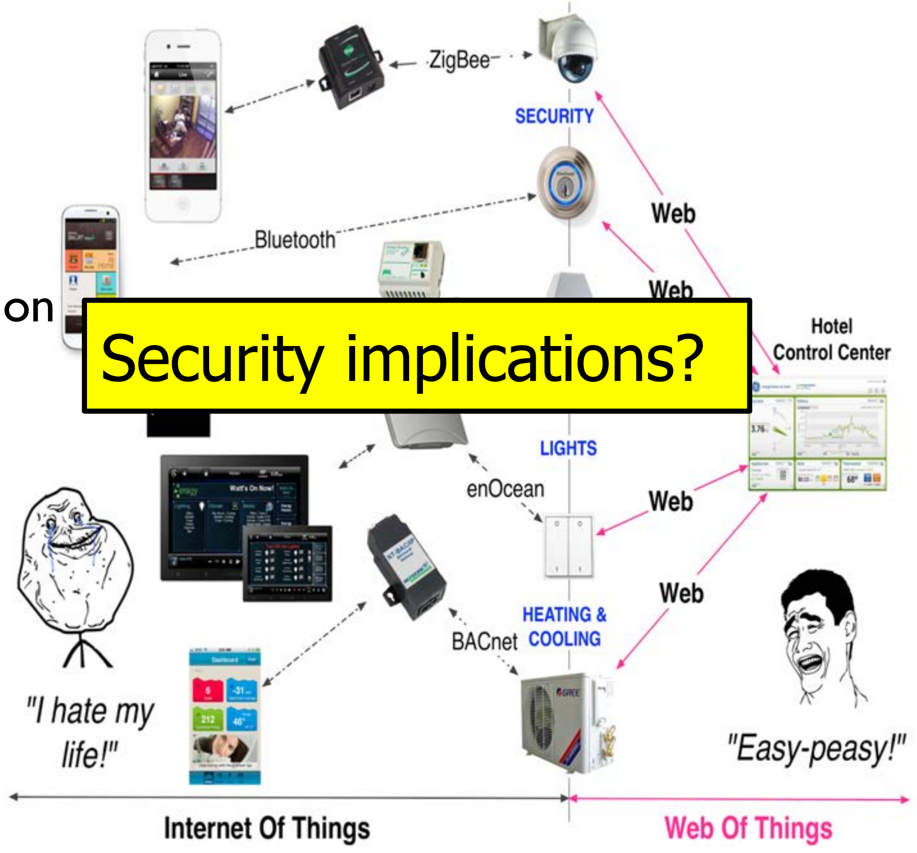
- Incompatible standards, platforms, technologies

Web of Things (WoT)

- Robust application support for IoT communication

"World Wide Web Consortium (W3C) is in a unique position to create the royalty-free and platform-independent standards needed to overcome the fragmentation of the IoT"

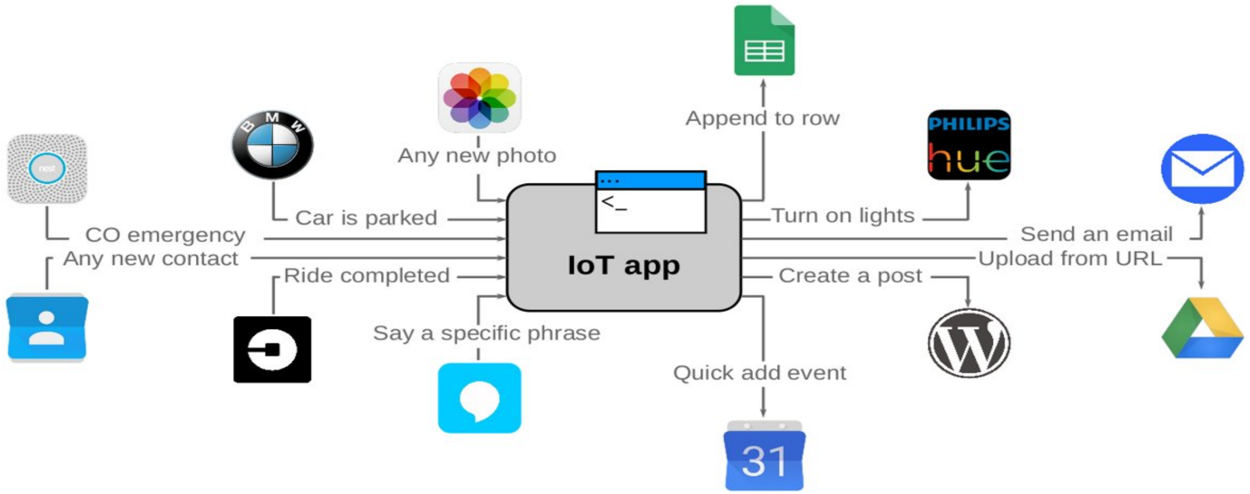
-W3C CEO Dr. Jeff Jaffe, 2017



Security implications?

IoT Platforms

- “Managing users’ digital lives”
  - Smart homes, smartphones, cars, fitness armbands
  - Online services (Google, Dropbox,…)
  - Social networks (Facebook, Twitter,…)
- Web interface + smartphone clients



IFTTT

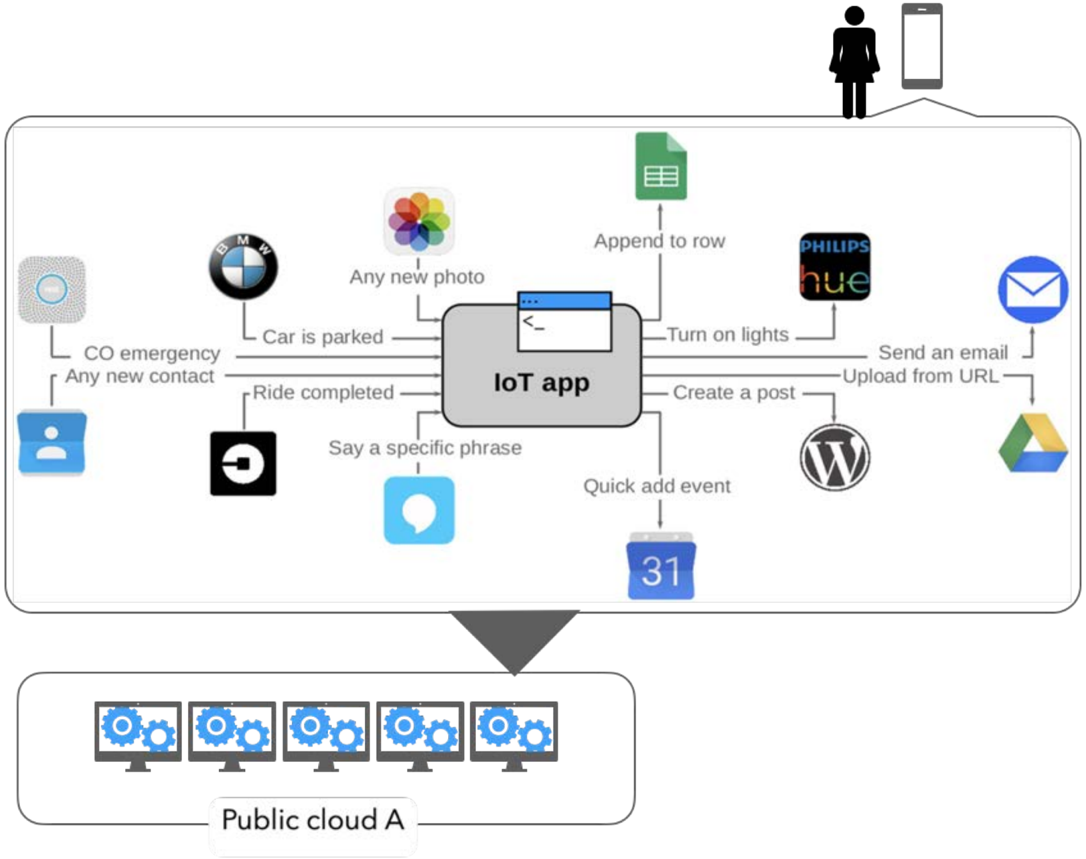
Do more with the services you love

zapier

Power Automate

Amazon AppFlow

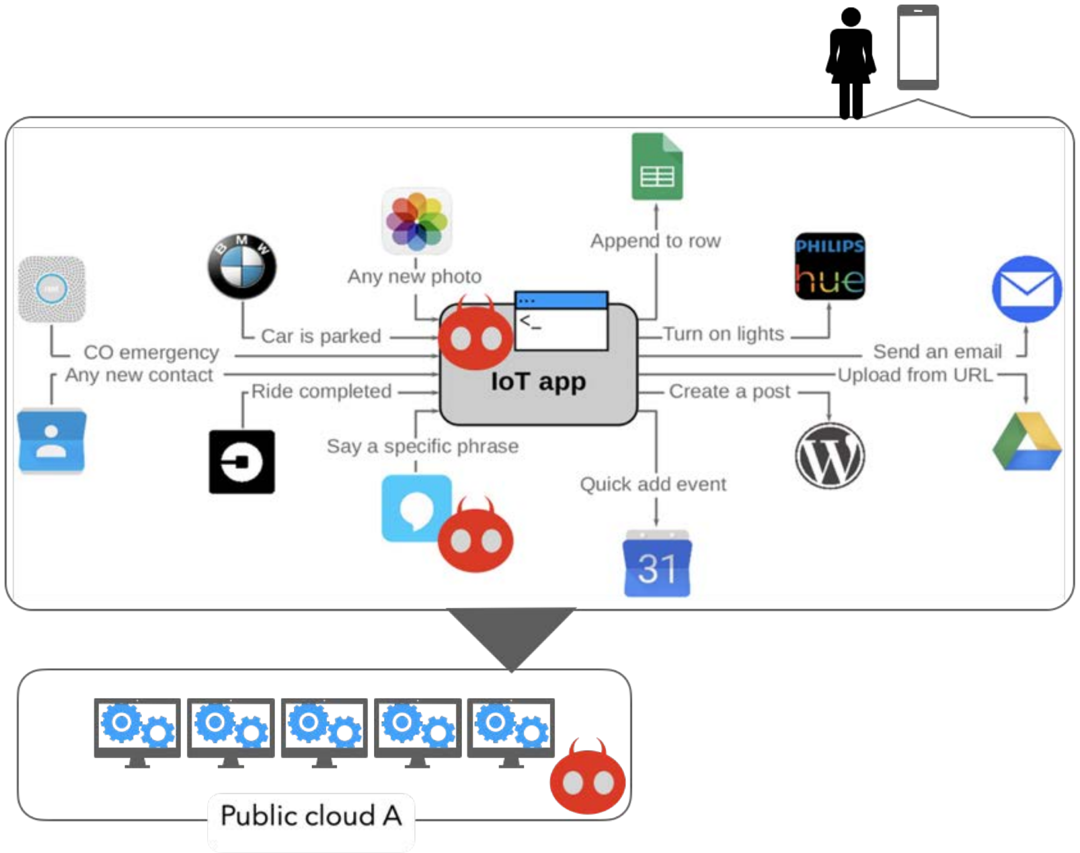
IoT platforms enable control…



From IoT to IoT platforms

- IoT platforms to the rescue
  - Cloud-based platforms
  - Managing users' digital lives by enabling powerful user automation apps
  - IoT platforms: IFTTT, Zapier, AWS AppFlow, MS Power Automate, Node-RED
  - “If heart rate exceeds a threshold, call the emergency doctor.”

...and weaponize the attackers



Third-party IoT apps

- **"Person-in-the-app" attacks [1]**
- Compromising users' security and privacy
- Major IoT platforms are vulnerable, enabling attackers to disrupt services, and steal and modify users' location, photos, voice assistants' data, video

Public cloud

- **"Person-in-the-cloud" attacks [2]**
- Cloud has full access to users' data
- Data over-sharing with 3rd parties
- Lack of support for information sharing and aggregation
- No migration between clouds

[1] Balliu et al. "Securing IoT Apps ", Security & Privacy Magazine 2019

[2] Paladi et al. "Providing user security guarantees in public infrastructure clouds." *IEEE Transactions on Cloud Computing* (2017).

Solution overview

A Secure and Usable IoT platform

Goals:

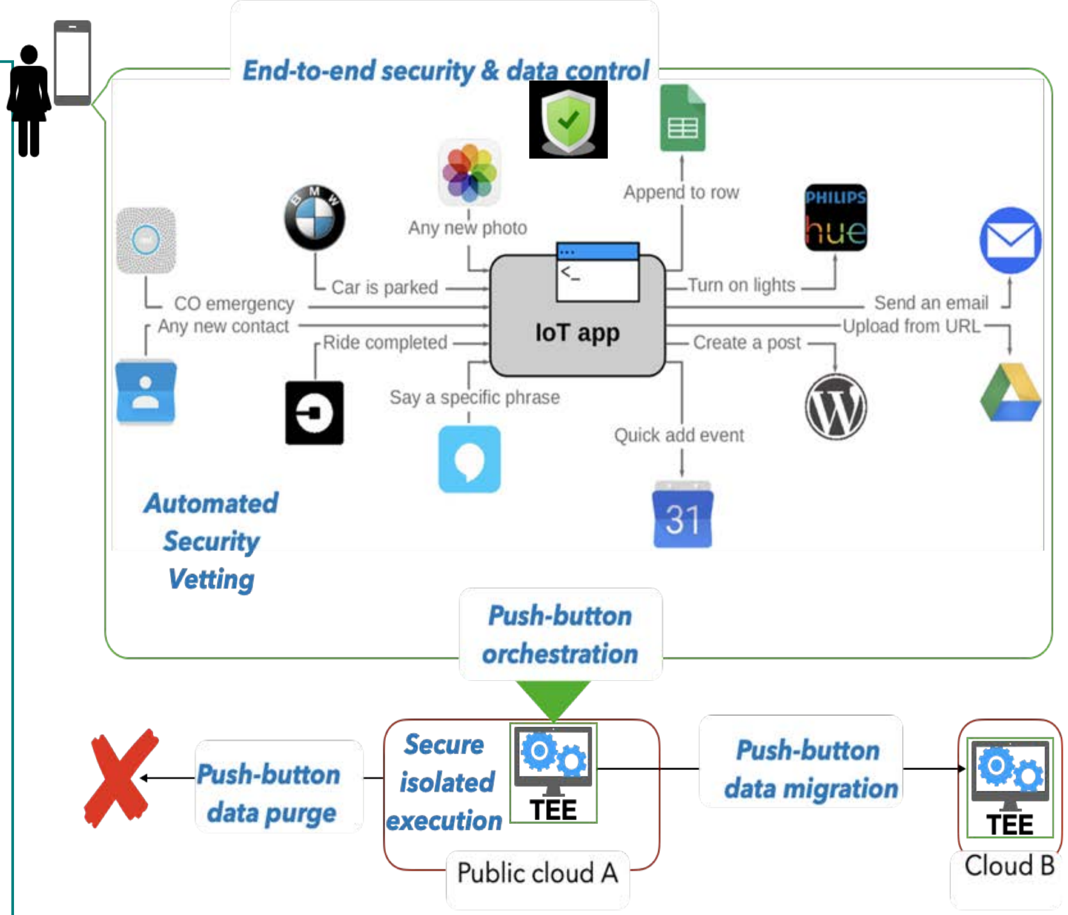
- Security **vetting and execution** of IoT apps by breaking and tracking the insecure flows.
- Support for multiple users and secure sharing
- User-friendly and **push-button orchestration** of secure IoT platforms in Trusted Execution Environments (TEEs)

Methods:

➢ Decentralized label model (DLM), Static and dynamic code analysis, fine-grained access control via sandboxing, TEEs

Current results:

- Discovered major vulnerabilities in IoT platforms, IFTTT, Zapier, and Node-RED
- Built defenses based on fine-grained sandboxing for JavaScript
- **Multi-user architecture based on DLM**

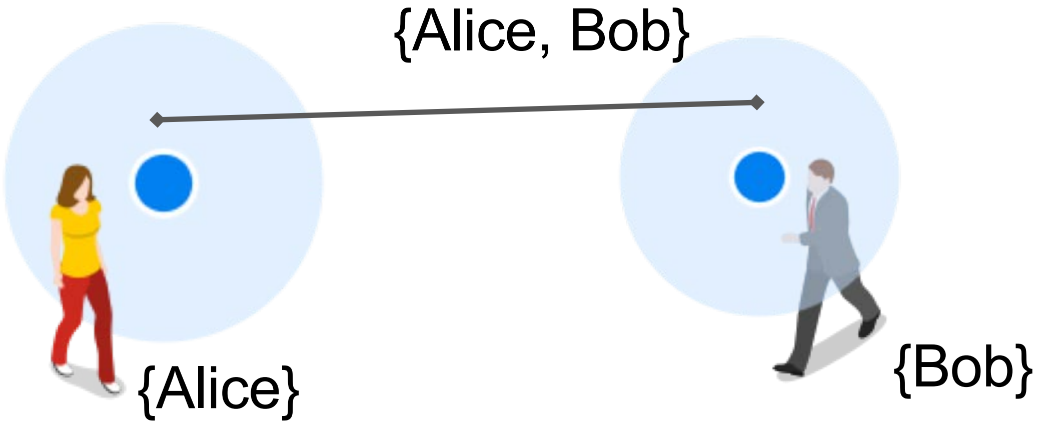


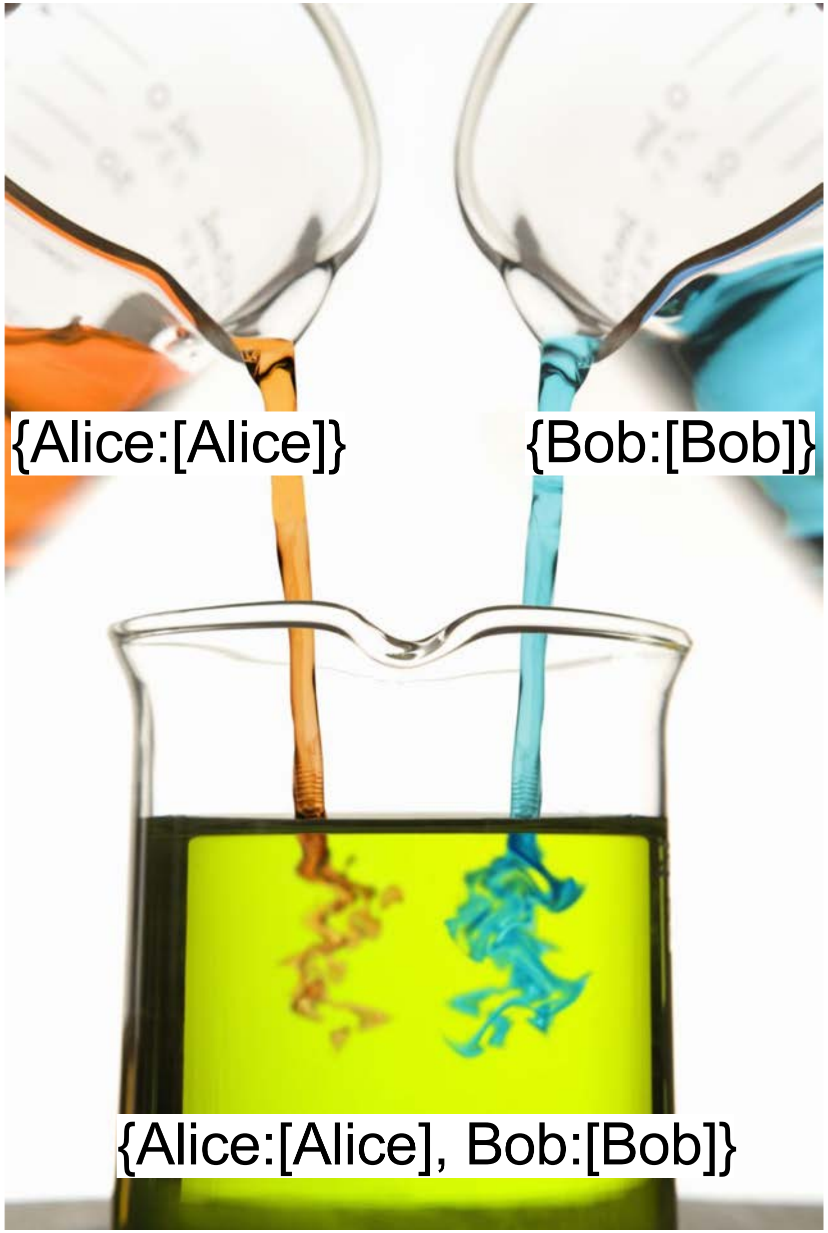
Decentralized Label Model

1. Data owners define access policies as labels

2. Track labels when computing over data

3. Stop data release unless the owners agree

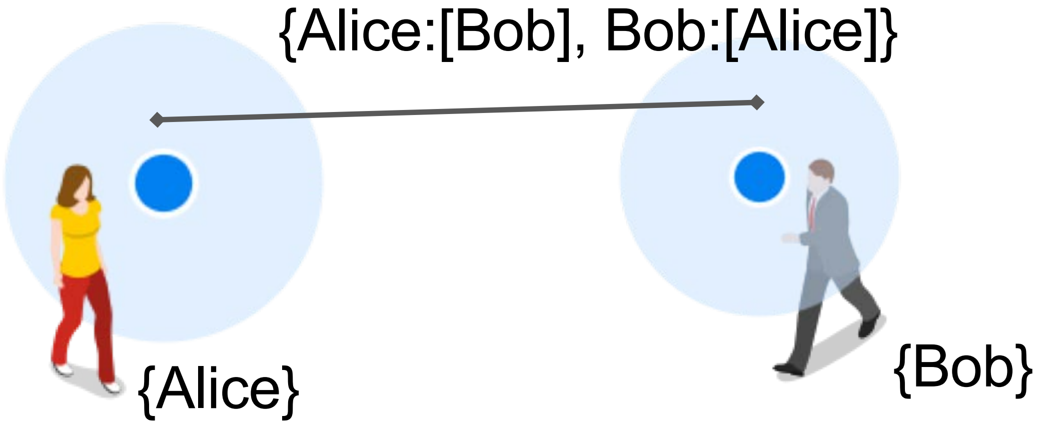


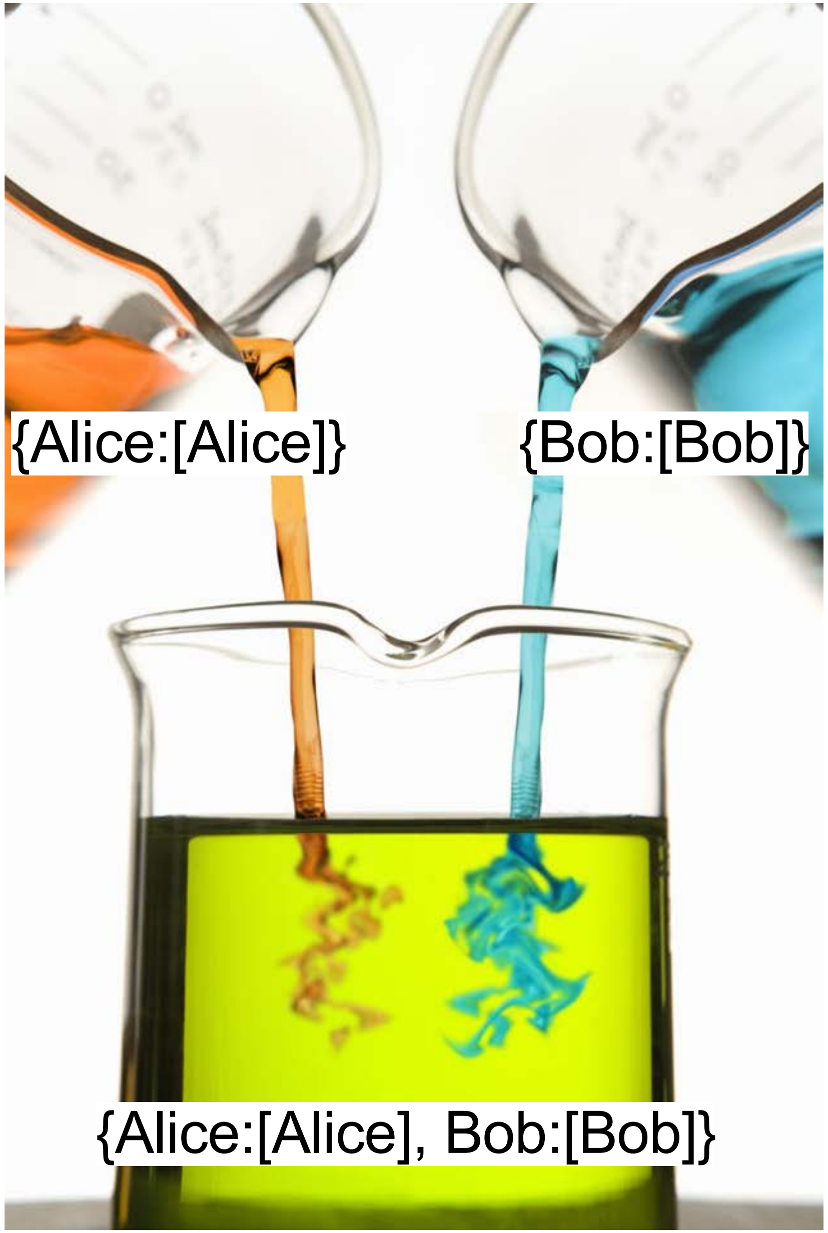


Declassification

Declassification – controlled information release:

1. Data owners explicitly agree on a declassification function
2. The underlying defensive mechanism ensures security



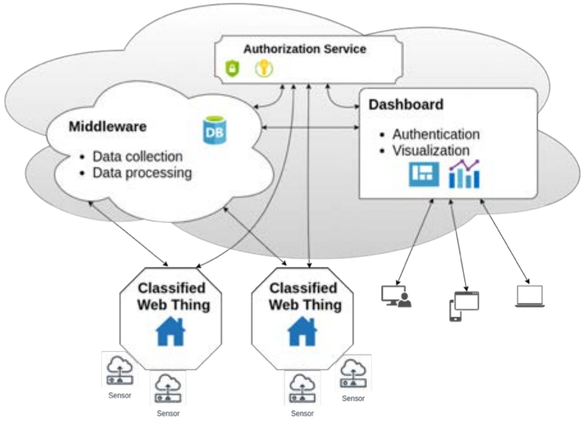


Marcus' results

WEB THINGS OF

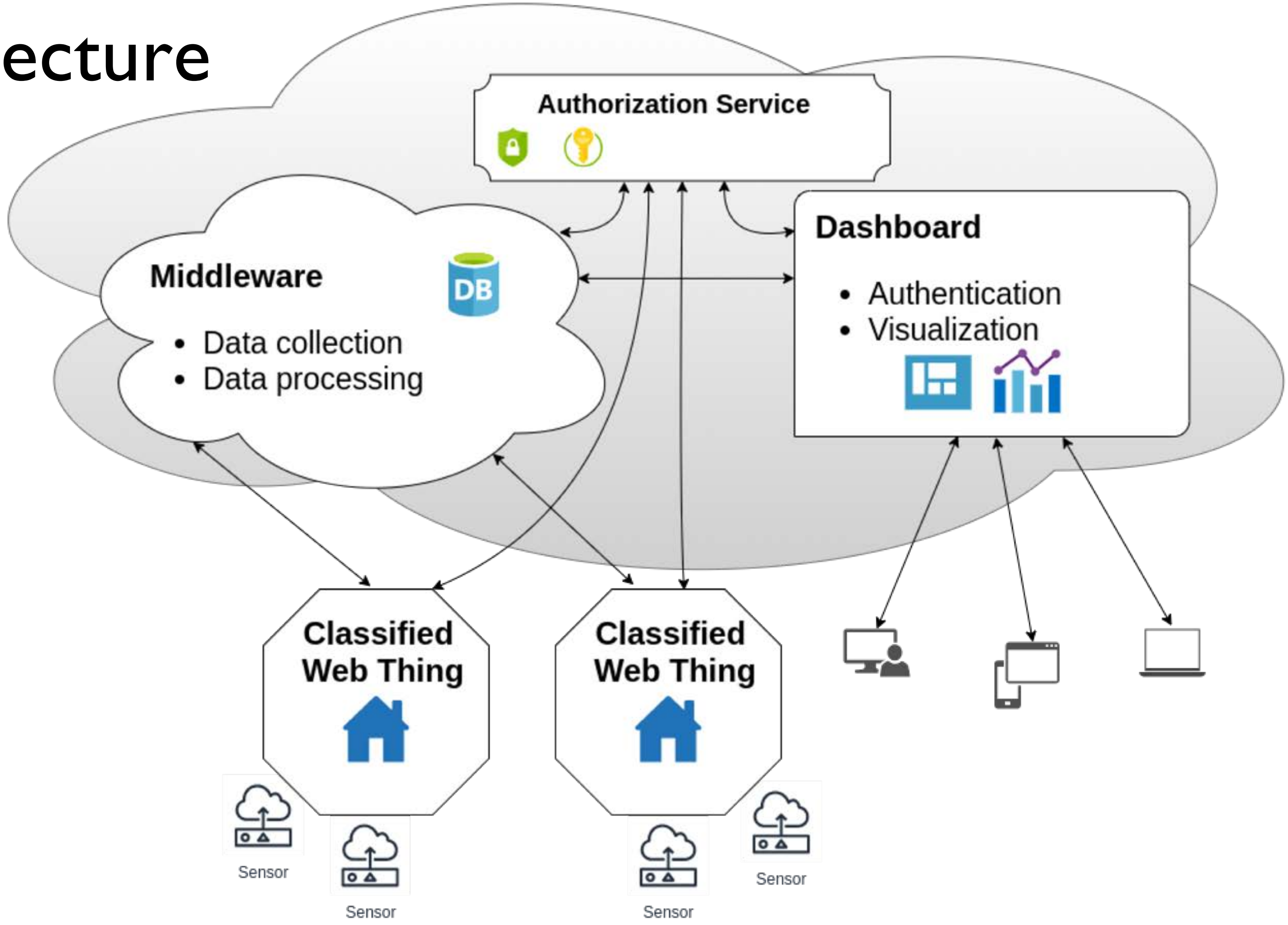
Node-RED

Grafana

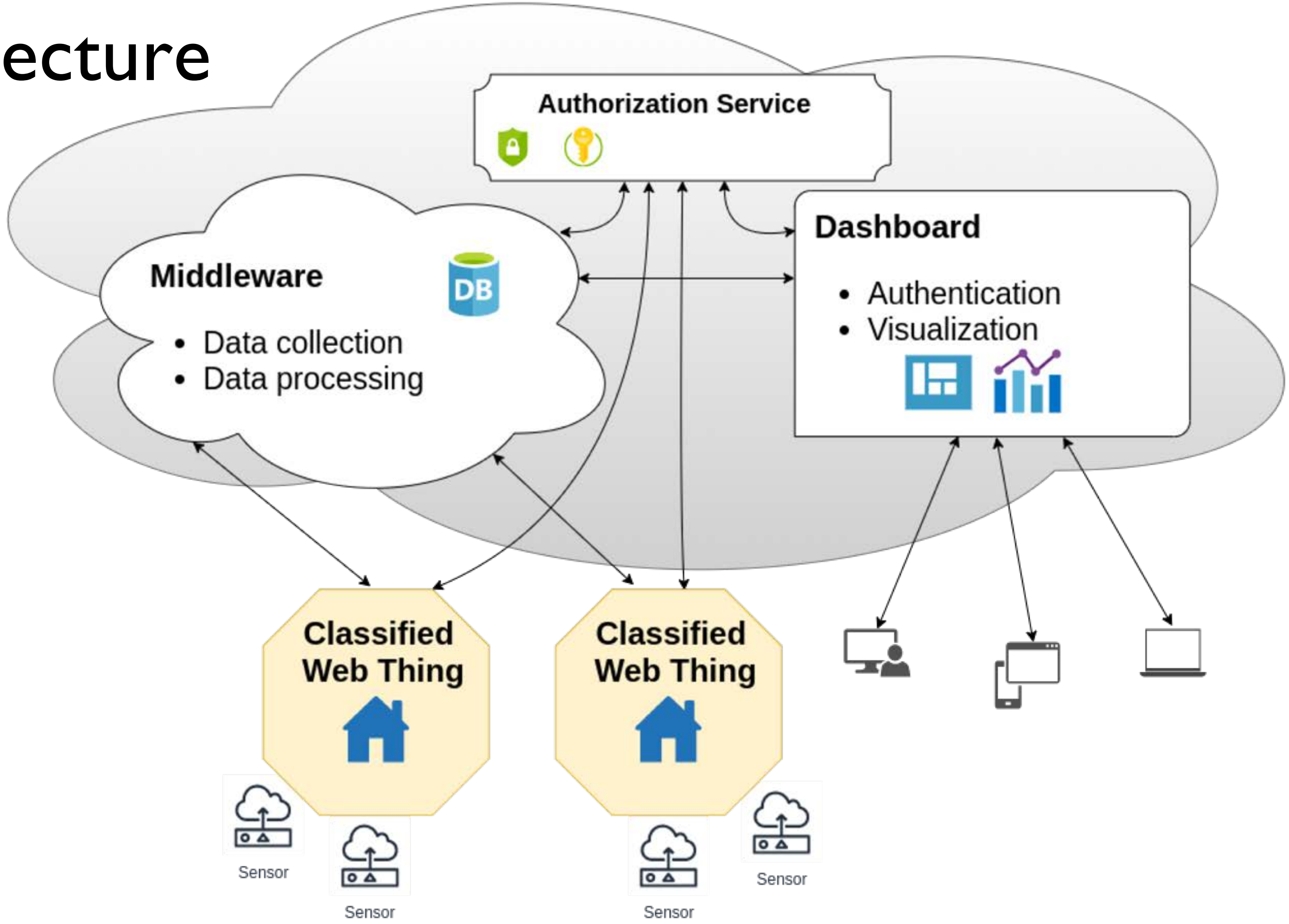


[1] M. Birgersson, C. Artho, and M. Balliu, ‘Security-Aware Multi-User Architecture for IoT’, presented at the 21st IEEE International Conference on Software Quality, Reliability, and Security (QRS’21), 2021.

Architecture



Architecture



Authorization Service

Middleware

- Data collection
- Data processing

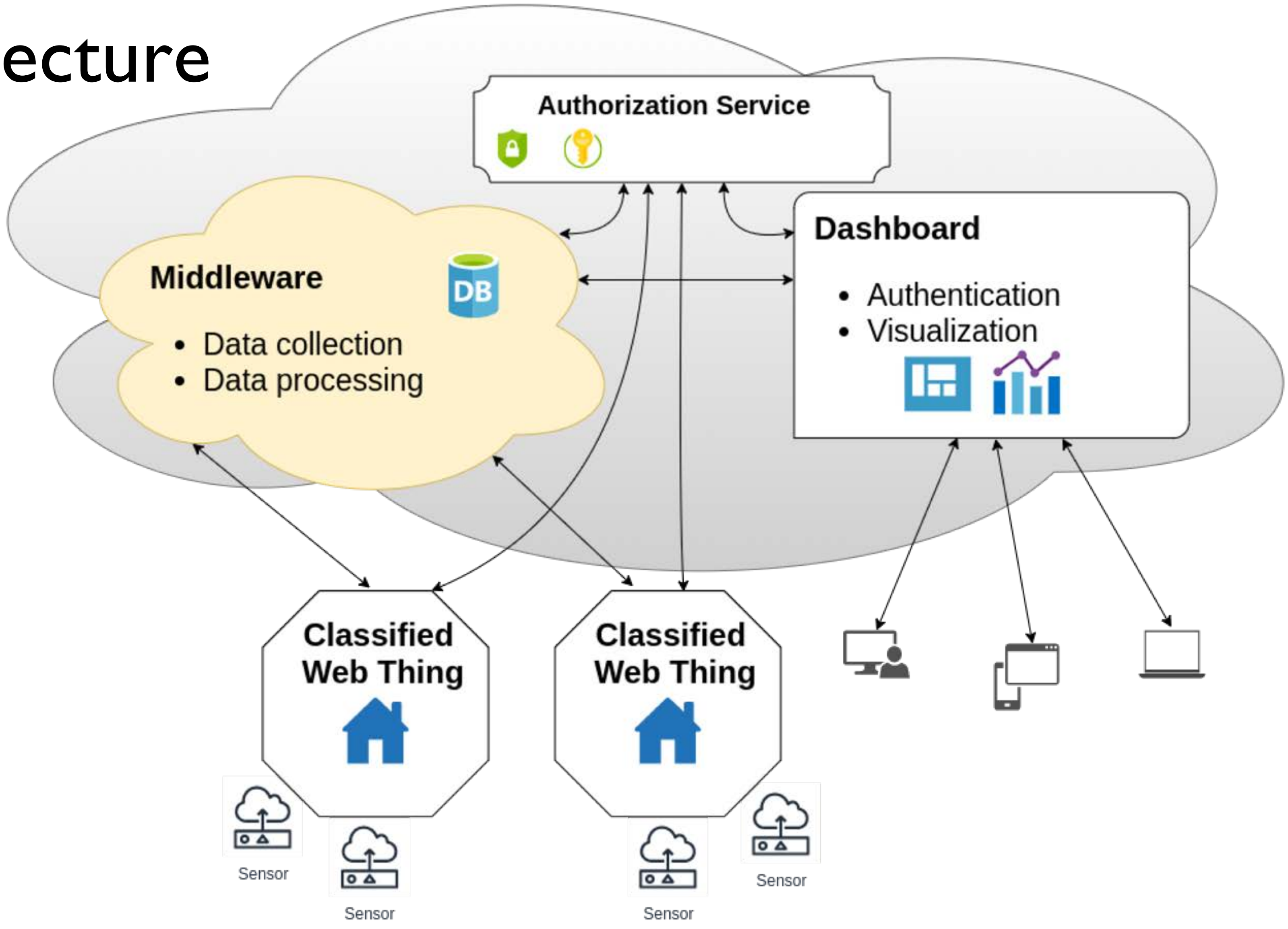
Dashboard

- Authentication
- Visualization

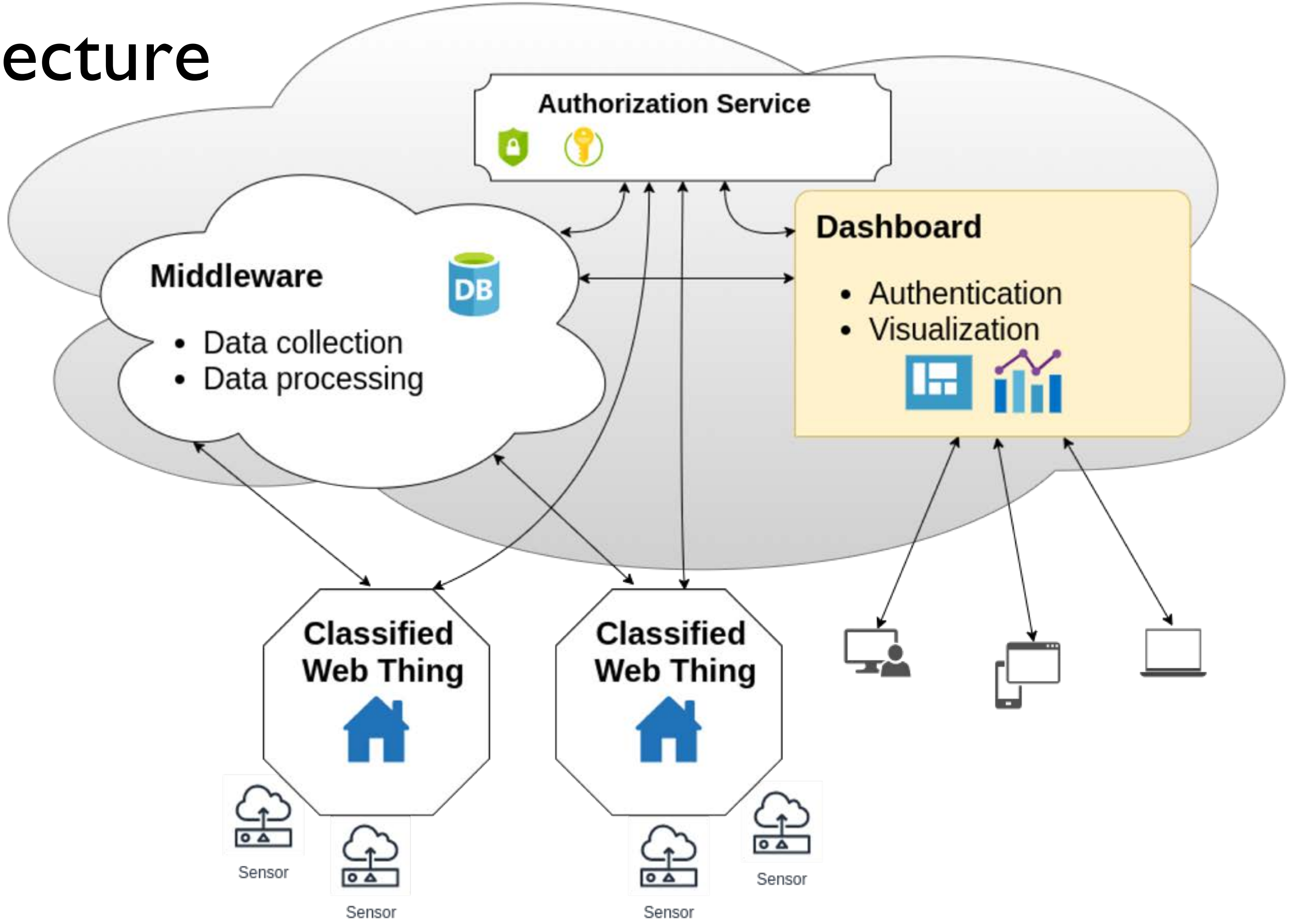
Classified Web Thing

Classified Web Thing

Architecture



Architecture



Authorization Service

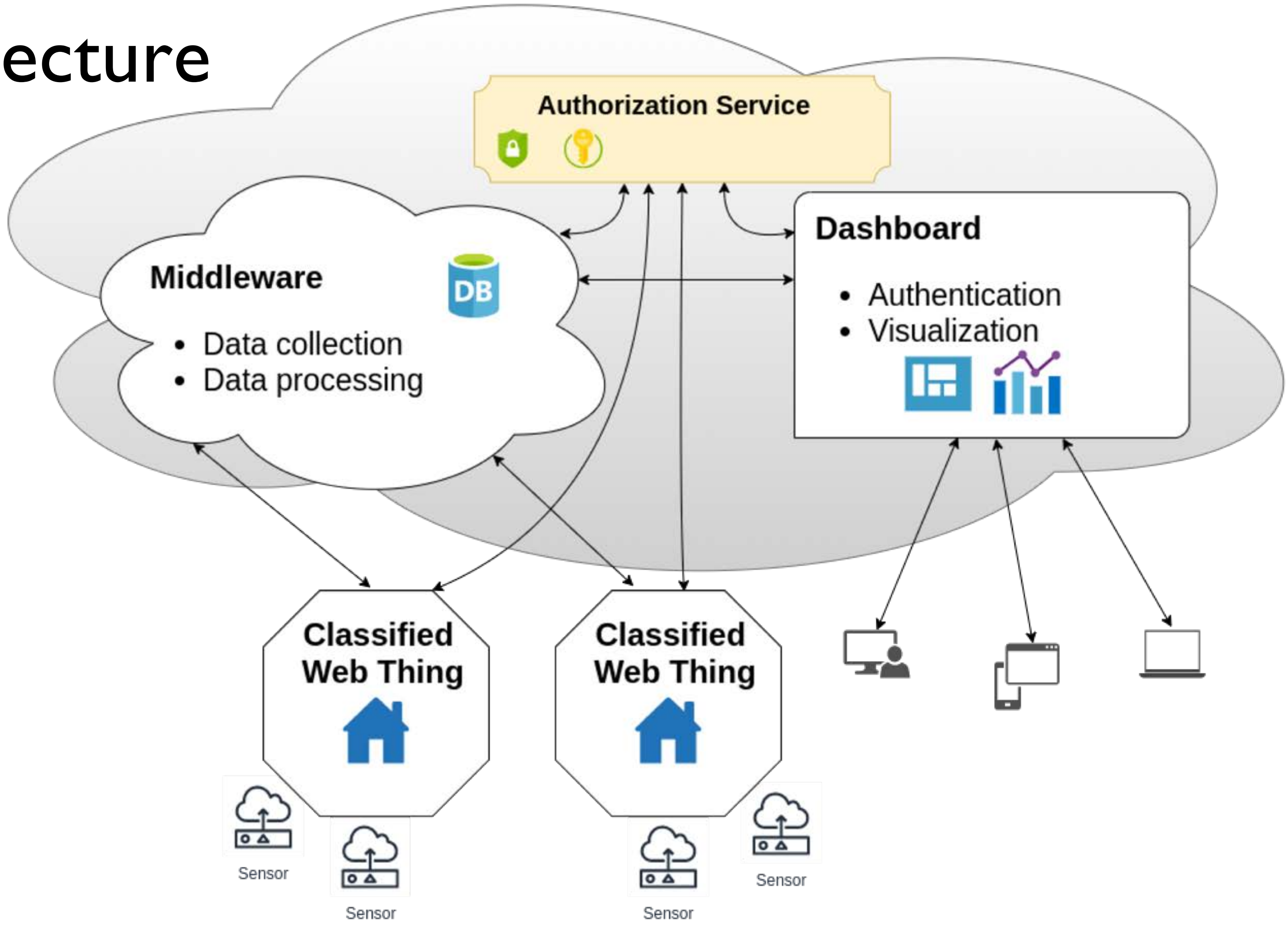
Middleware

- Data collection
- Data processing

Dashboard

- Authentication
- Visualization

Architecture



Authorization Service

Middleware

- Data collection
- Data processing

Dashboard

- Authentication
- Visualization

Classified Web Thing

Classified Web Thing

Prototype implementation

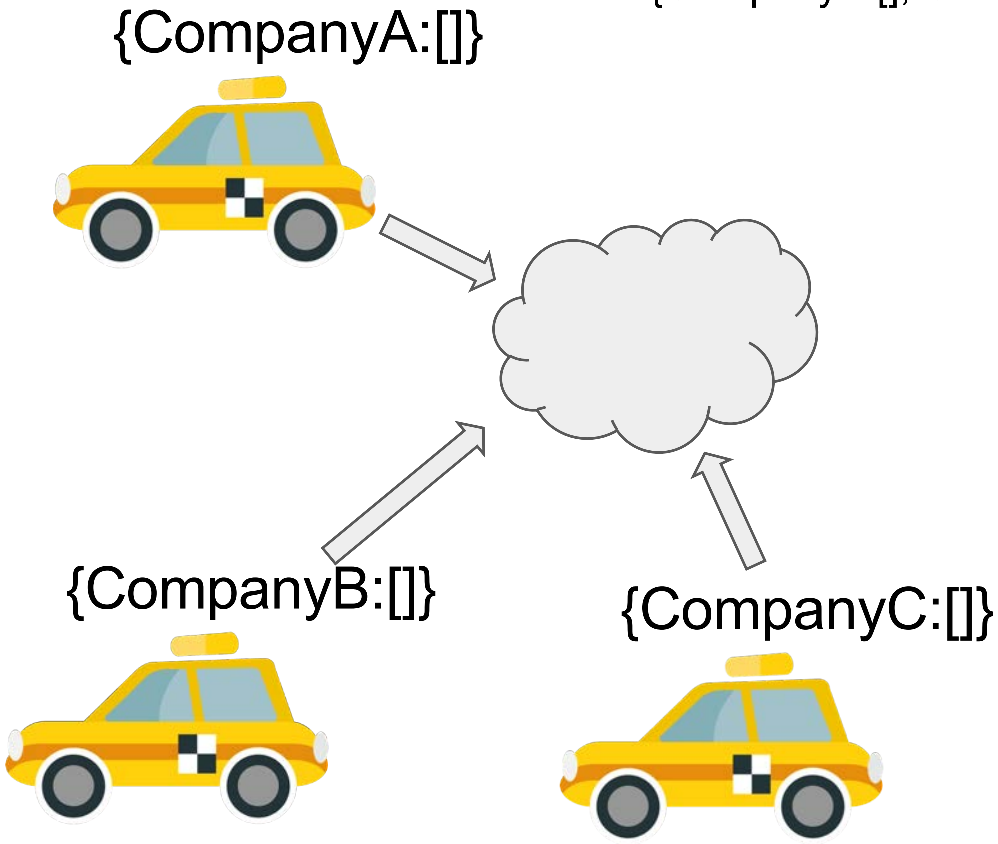
Mocked IoT-devices using the Web of Things standard

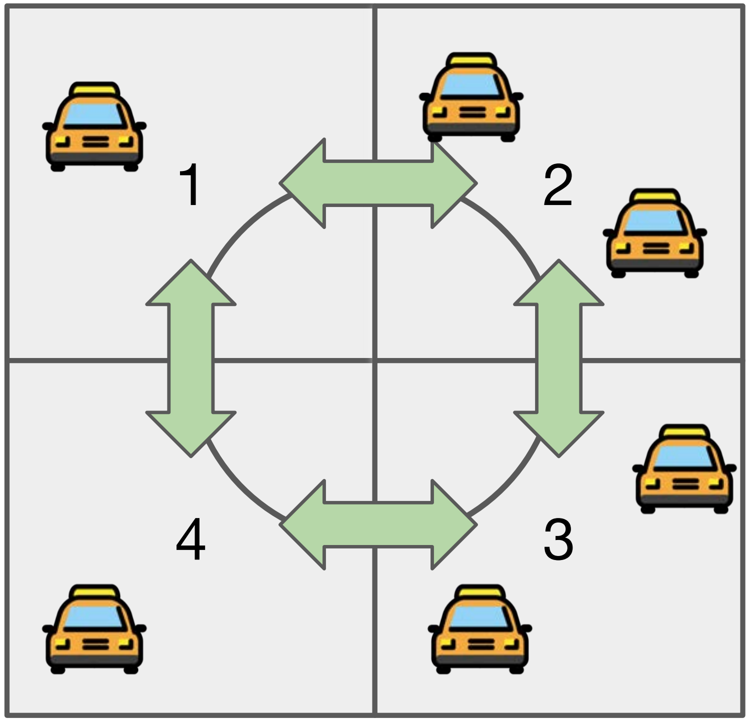
Middleware with Node-RED

Dashboard using Grafana

Use case - Smart City

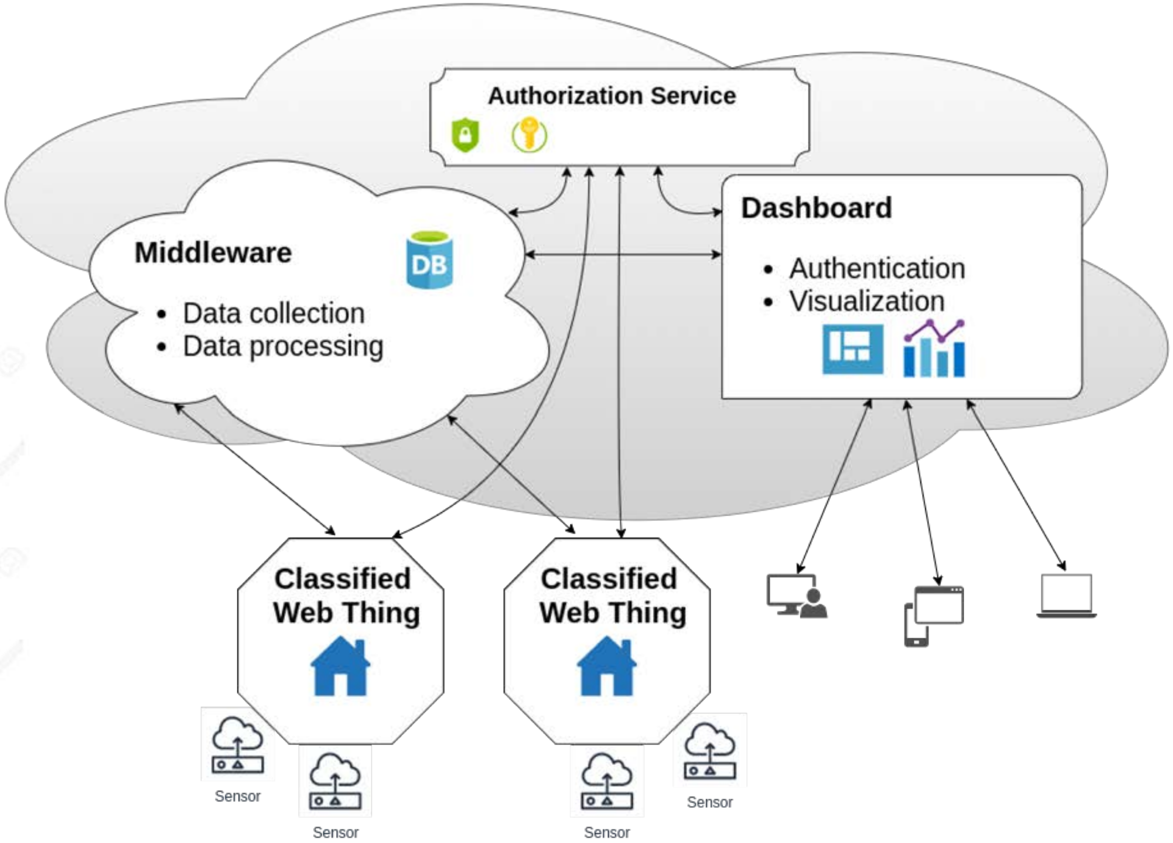
{CompanyA:[], CompanyB:[], CompanyC:[]} Declassification {City:[Public]}



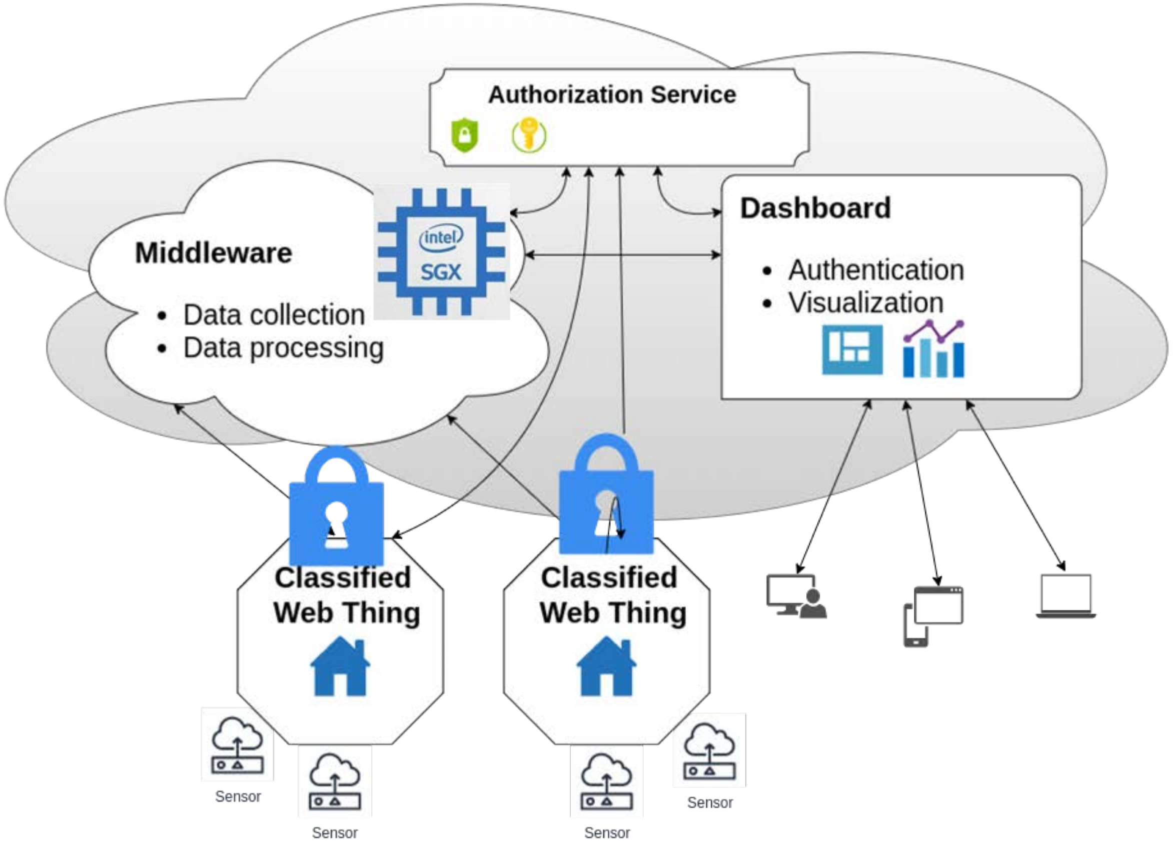


Used under CC license

Ongoing work - Reduce trust in the cloud platform



TEE - Reduce trust in the cloud platform



Summary

A Secure and Usable IoT platform

Goals:

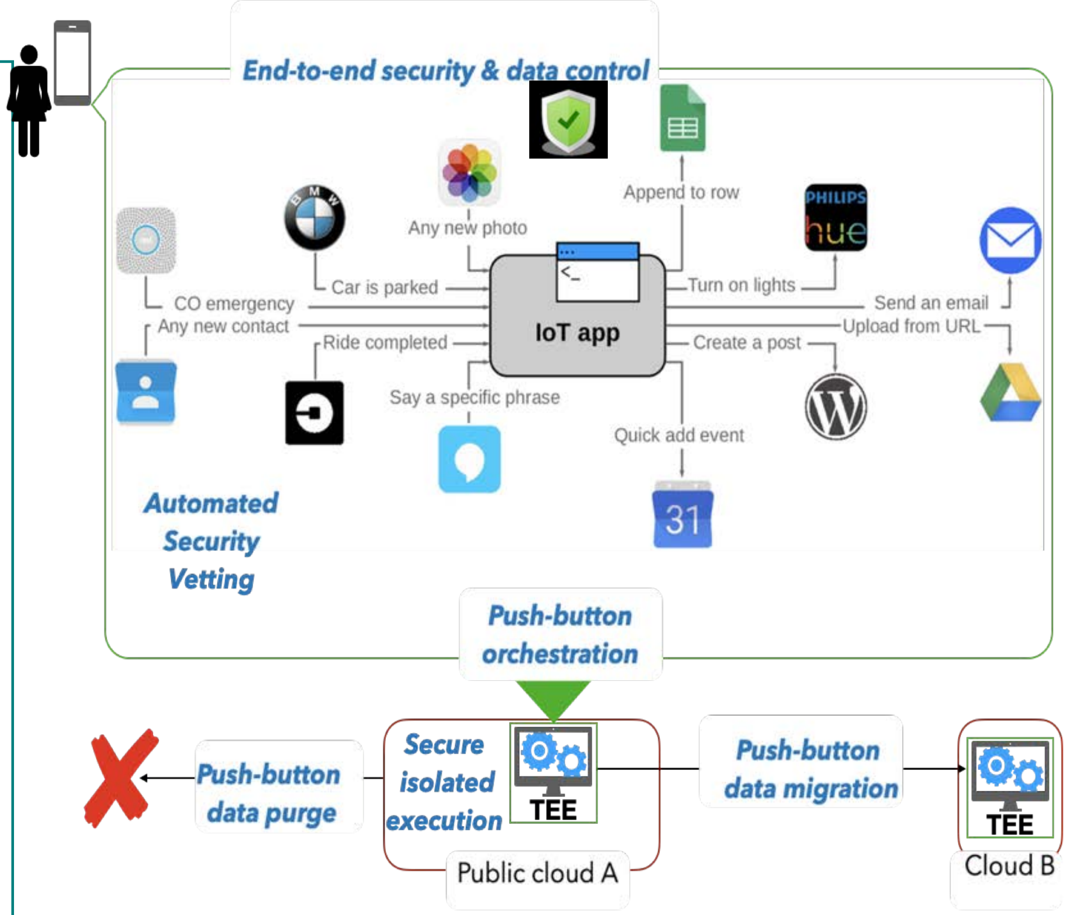
- Security **vetting and execution** of IoT apps by breaking and tracking the insecure flows.
- Support for multiple users and secure sharing
- User-friendly and **push-button orchestration** of secure IoT platforms in Trusted Execution Environments (TEEs)

Methods:

➢ Decentralized label model (DLM), Static and dynamic code analysis, fine-grained access control via sandboxing, TEEs

Results:

- Discovered major vulnerabilities in IoT platforms, IFTTT, Zapier, and Node-RED
- Built defenses based on fine-grained sandboxing for JavaScript
- **Multi-user architecture based on DLM**


End-to-end security & data control
IoT app
Append to row
Any new photo
Car is parked
CO emergency
Any new contact
Ride completed
Say a specific phrase
Turn on lights
Send an email
Upload from URL
Create a post
Quick add event
PHILIPS hue
31
Automated Security Vetting
Push-button orchestration
Push-button data purge
Secure isolated execution
TEE
Public cloud A
Push-button data migration
TEE
Cloud B