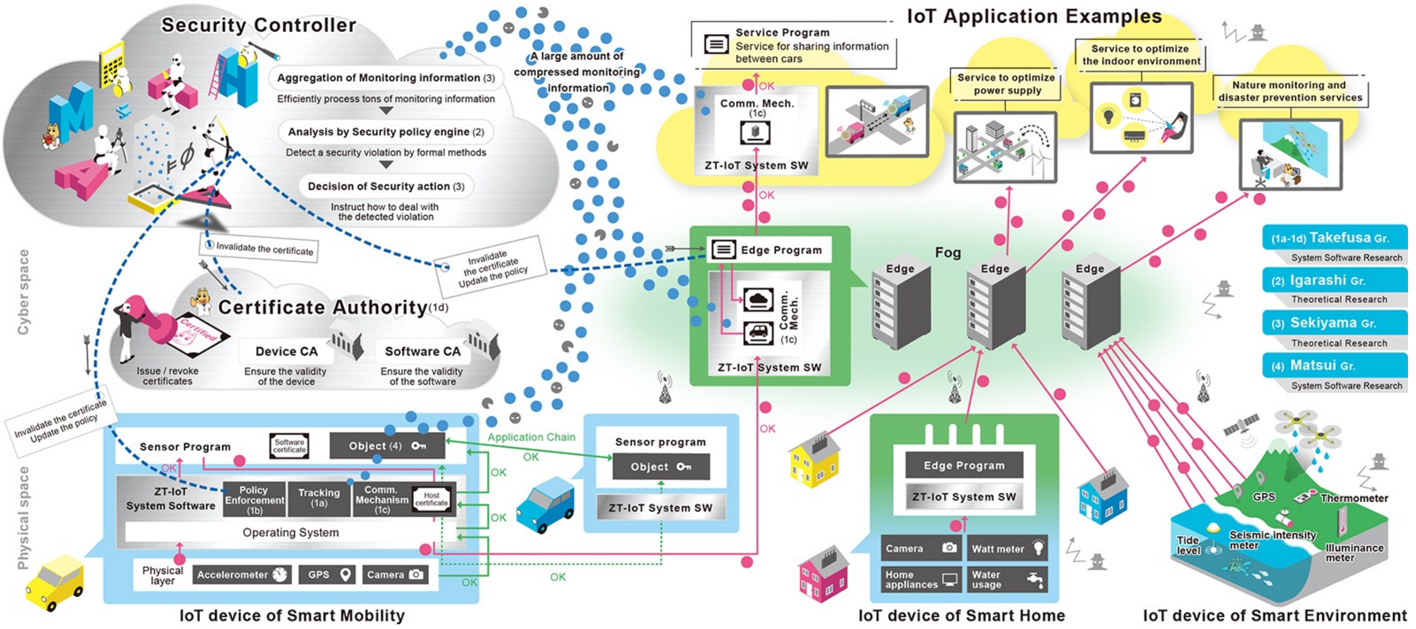
Zero Trust based IoT Security

https://zt-iot.nii.ac.jp/en/

This project aims to realize **secure Internet of Things (IoT)** systems by the concept of **zero trust** by the fusion of **formal verification** and **system software** technologies. In the field of study on formal verification, we provide mathematical proof for the legitimacy of IoT trust chains and address undiscovered threats by combining static and dynamic verification. In the field of system software research, we develop mechanisms for isolated execution, automatic detection, and automatic countermeasures in conjunction with the theoretical results to demonstrate **zero trust IoT (ZT-IoT)**. We also promote social acceptance of IoT by ensuring accountability.



Security Controller

Aggregation of Monitoring information (3)
Efficiently process tons of monitoring information

Analysis by Security policy engine (2)
Detect a security violation by formal methods

Decision of Security action (3)
Instruct how to deal with the detected violation

A large amount of compressed monitoring information

Invalidate the certificate

Invalidate the certificate
Update the policy

Certificate Authority(1d)

Issue / revoke certificates

Device CA
Ensure the validity of the device

Software CA
Ensure the validity of the software

Invalidate the certificate
Update the policy

Cyber space

Physical space

Sensor Program
Software certificate
Object (4)

ZT-IoT System Software
Policy Enforcement (1b)
Tracking (1a)
Comm. Mechanism (1c)
Host certificate

Operating System

Physical layer
Accelerometer
GPS
Camera

OK

Application Chain

Sensor program
Object
ZT-IoT System SW

IoT device of Smart Mobility

IoT Application Examples

Service Program
Service for sharing information between cars

Comm. Mech. (1c)
ZT-IoT System SW

Service to optimize power supply

Service to optimize the indoor environment

Nature monitoring and disaster prevention services

Edge Program
Comm. Mech. (1c)
ZT-IoT System SW

Fog

Edge

(1a-1d) Takefusa Gr.
System Software Research

(2) Igarashi Gr.
Theoretical Research

(3) Sekiyama Gr.
Theoretical Research

(4) Matsui Gr.
System Software Research

Edge Program
ZT-IoT System SW
Camera
Watt meter
Home appliances
Water usage

IoT device of Smart Home

GPS
Thermometer
Tide level
Seismic intensity meter
Illuminance meter

IoT device of Smart Environment

Zero Trust IoT (ZT-IoT) Project

- What is **Zero Trust**?
  - "Zero trust (ZT) is the term for an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources." [NIST SP 800-207]
  - Assumes there is **no implicit trust**.
  - Improving security measures through continuous monitoring and analysis.
- The **ZT-IoT** project aims to apply the concept of zero trust to IoT systems.
  - Managing a large number of IoT devices.
  - Overcoming the limitations of resource performance, power consumption, and remote management of IoT devices.
  - Ensuring accountability through mathematical theory.

ZT-IoT Research Topics

- Trust chain among resources such as IoT devices, edge/fog, and cloud servers.
  - Root of trust (RoT) and secure boot.
  - Public Key Infrastructure (PKI)-based ***key management leveraging Trusted Execution Environment (TEE)***.
- ***Monitoring and policy enforcement*** by system software and security controller.
- Over-the-air (OTA) update-based software life cycle management for resiliency.
- Assurance of software reliability with digital signature and ***software certification service***.
- Achieving security-by-design based on ***formal verification.***

This work was supported by JST, CREST Grant Number **JPMJCR21M3.**