Attack demonstration took kits for Industry 4.0 using AI and cloud

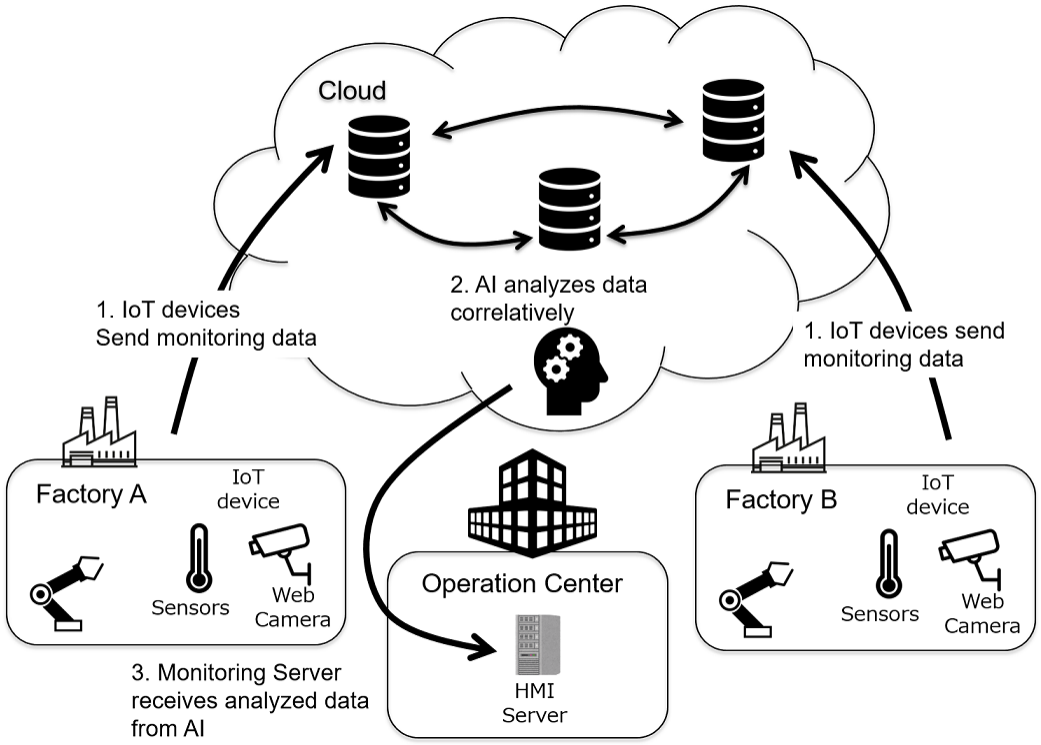
The University of Tokyo
Wataru Matsuda,
Mariko Fujimoto,
Takuho Mitsunaga

Background

- **Industry 4.0 is a new concept of automation and data exchange in manufacturing.**
- **Devices are supposed to connect, and that can create more attack surfaces and risks of cyberattacks. Therefore, risk assessment for cybersecurity in ICS is necessary.**
- The penetration test is one of the essential processes in risk assessment to assess the possibilities of attacks. We focus on **penetration tests using actual machines**.

Overview of Industry 4.0

- Industry 4.0 is a name given to the current trend of automation and **data exchange** in manufacturing technologies.
- Autonomous judgment and execution are required for the cyber-physical system, **it is based on information exchange using AI and cloud technologies.**



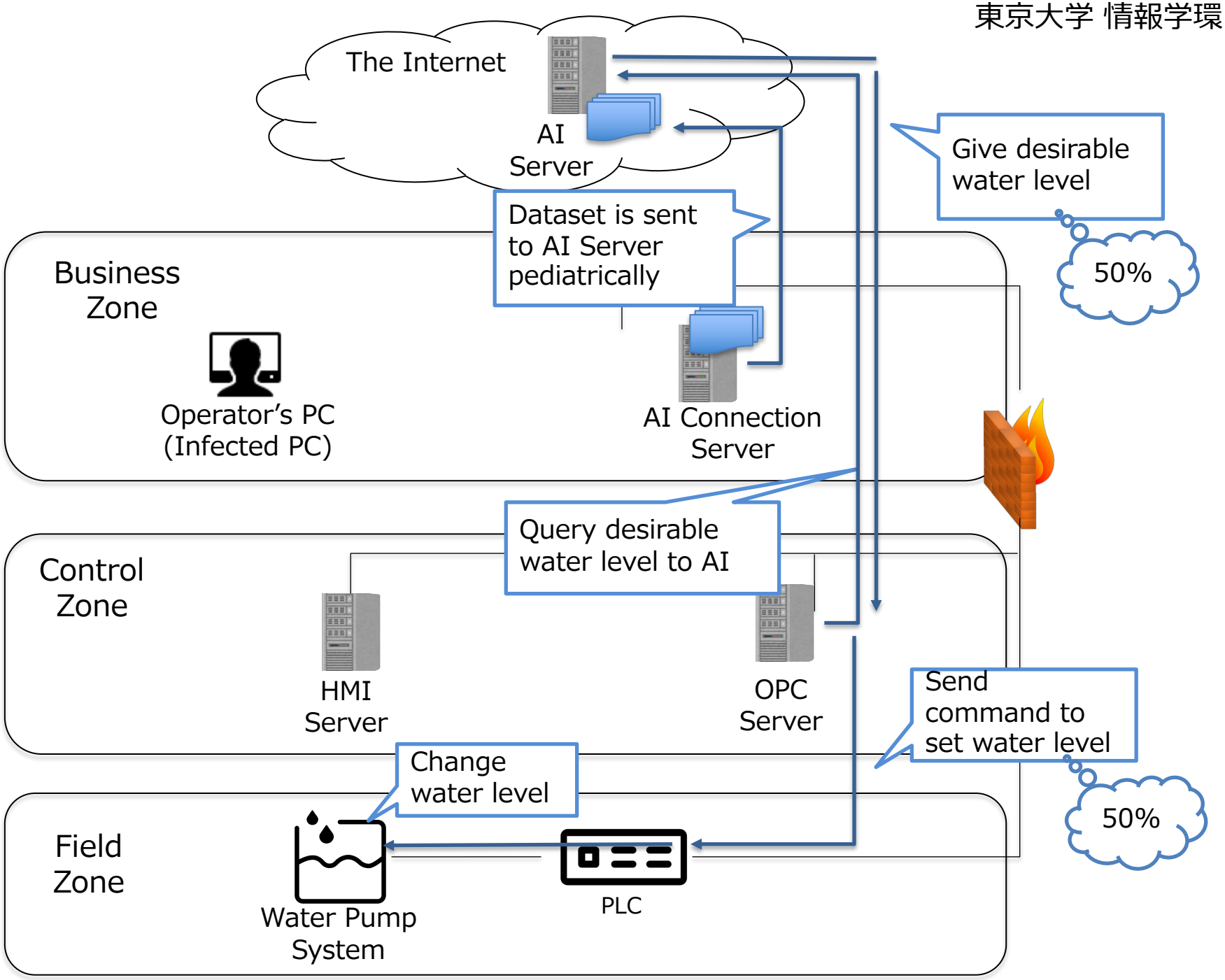
AI technology in Industry 4.0

- In Industry 4.0, the cyber-physical system is required to judge and execute processes autonomously, so AI is required technology.
- Massive real-time data will be collected from ICS, and they should be analyzed effectively.
- **AI is suitable for analyzing a large amount of data**. Also, it is applicable for complex data such as image or sentence, etc.
- It is expected that AI will be used in ICS. Therefore, we evaluate security risks **when AI is used for controlling the ICS**.
- In our ICS testbed, machine learning is used to detect anomalies of the psychical state in ICS.

Cloud technology in Industry 4.0

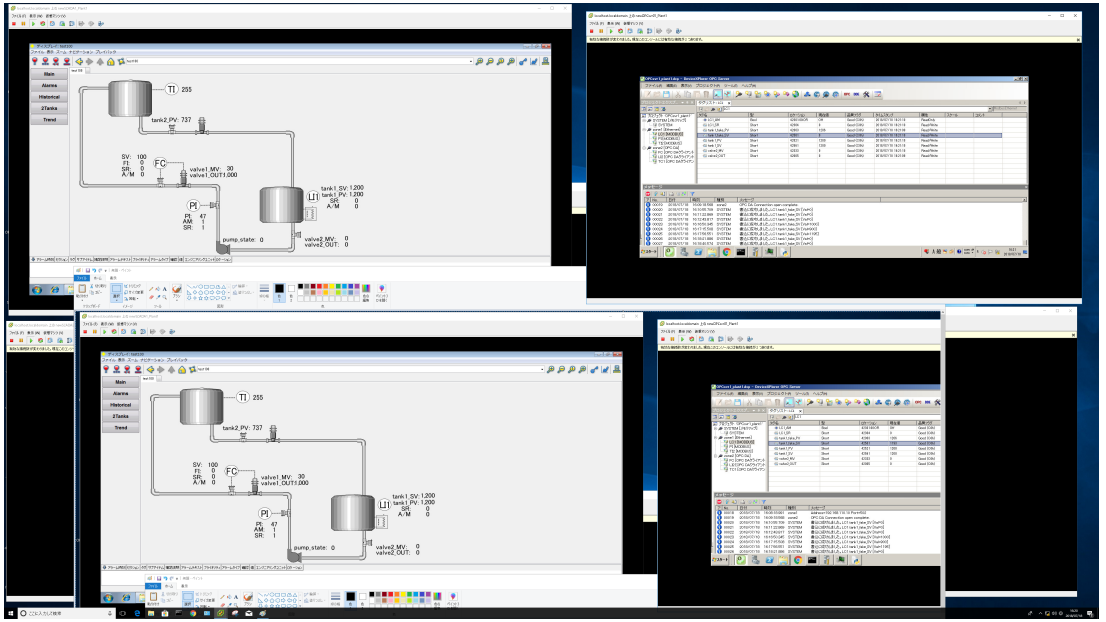
- An interface to the Internet or a similar network is necessary to extend to a cyber-Physical System.
- Devices should be **uniformly managed and monitored using a cloud system** so that all revenant parties (ICS operators, security operators, IT security people, etc.) can share real-time information.
- **In our ICS testbed, data of the psychical state in ICS is sent to the cloud, and AI analyses it.**

Demonstration tool kit


The Internet
AI Server
Give desirable water level
50%
Dataset is sent to AI Server pediatrically
Business Zone
Operator's PC (Infected PC)
AI Connection Server
Query desirable water level to AI
Control Zone
HMI Server
OPC Server
Send command to set water level
50%
Change water level
Field Zone
Water Pump System
PLC

ICS testbed environment

Water pump system

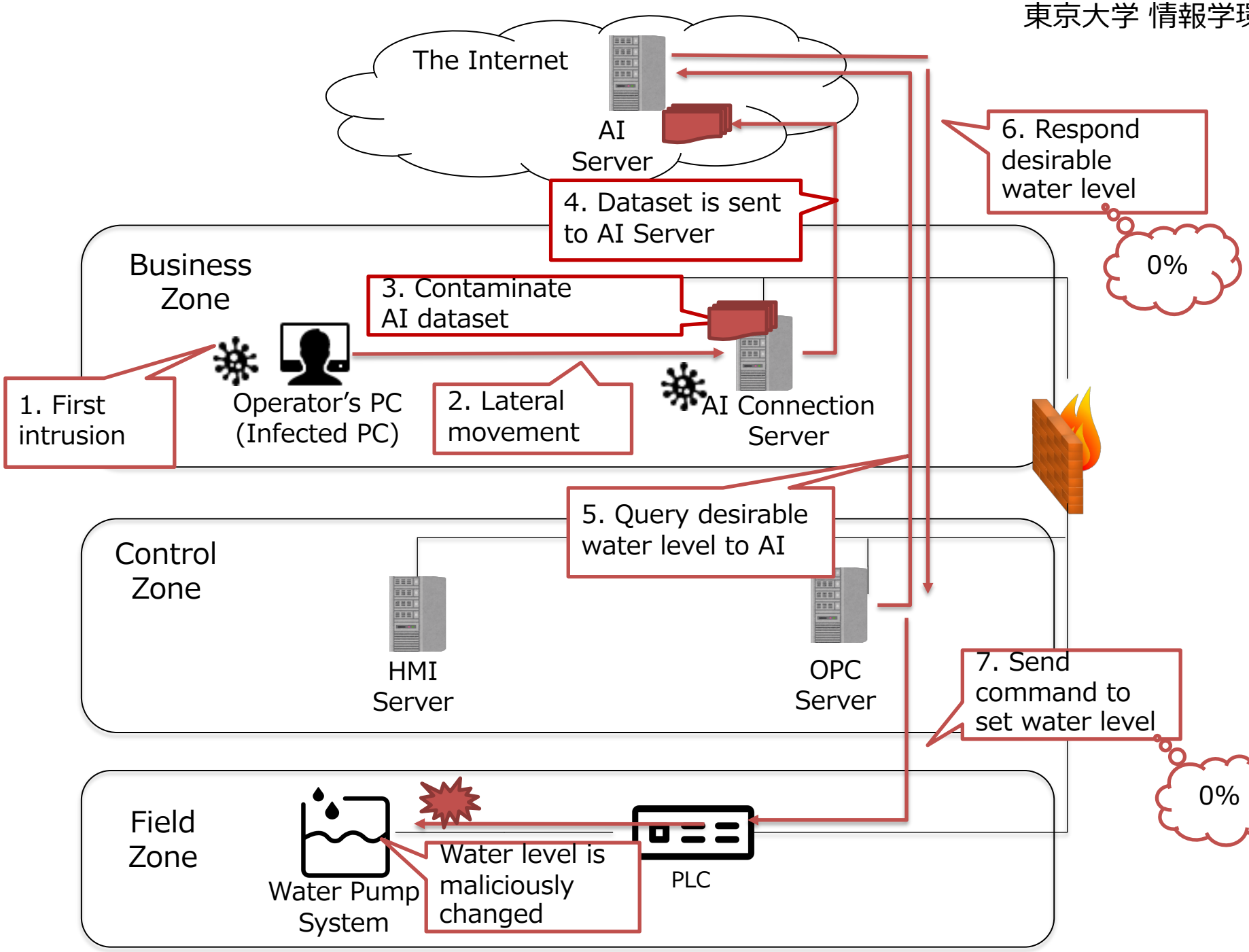


HMI

http://www.manage.nitech.ac.jp/Security/activity2018.pdf

Attack scenario

1. **Infects a PC in the Business zone**
2. **A lateral movement to AI Connection Server**
3. **Contaminate the AI dataset**
4. The contaminated dataset is sent to AI Server
5. OPC Server queries the desirable water level to the AI Server
6. AI Server returns incorrect value judged from the contaminated dataset
7. OPC Server sends incorrect SetPoint to PLC
8. The water rate is maliciously changed


The Internet
AI Server
4. Dataset is sent to AI Server
6. Respond desirable water level
0%
Business Zone
3. Contaminate AI dataset
1. First intrusion
Operator's PC (Infected PC)
2. Lateral movement
AI Connection Server
5. Query desirable water level to AI
Control Zone
HMI Server
OPC Server
7. Send command to set water level
0%
Field Zone
Water Pump System
Water level is maliciously changed
PLC

Attack result

- We conduct preterition test based on the attack scenario.
- As the result, we successfully changed the physical state of the actuator by attacks and avoid detection of AI.

Before (Normal water level)

After (Empty)

Thank you for your attention!

coe@sisoc.org