15TH ITU ACADEMIC CONFERENCE

ITU KALEIDOSCOPE
NEW DELHI 2024

Innovation and digital transformation for a sustainable world

Investigating Agricultural IoT Devices and Services from Cybersecurity Perspective

21-23 October 2024
New Delhi, India

Kosuke Tanizaki[1]

(Coauthors: Keisuke Furumoto[2], Kohei Masumi[2],
Trong-Minh Hoang[3], Yoshiaki Shiraishi[1] and Takeshi Takahashi[2])

1: Kobe University, Japan
2: National Institute of Information and
Communications Technology, Japan
3: Posts and Telecommunications Institute of Technology, Vietnam

Session 8.1

Outline

- Introduction
- Creating taxonomies of agricultural IoT
- Investigation of emerging threats
- Investigation of potential threats
- Current standards as potential countermeasures
- Contribution and recommendations

Contribution

❖Security issue of agricultural IoT

- There is lack of comprehensive research focusing on security of IoT devices

→ This work provide a large-scale study on the security of agriculture IoT devices

↓

- Developing a taxonomy of 175 agricultural IoT devices
- Conducting a large-scale survey using Shodan's observation network

Introduction

Agricultural IoT is a combination of edge devices, network devices, and elements such as the cloud and WAN

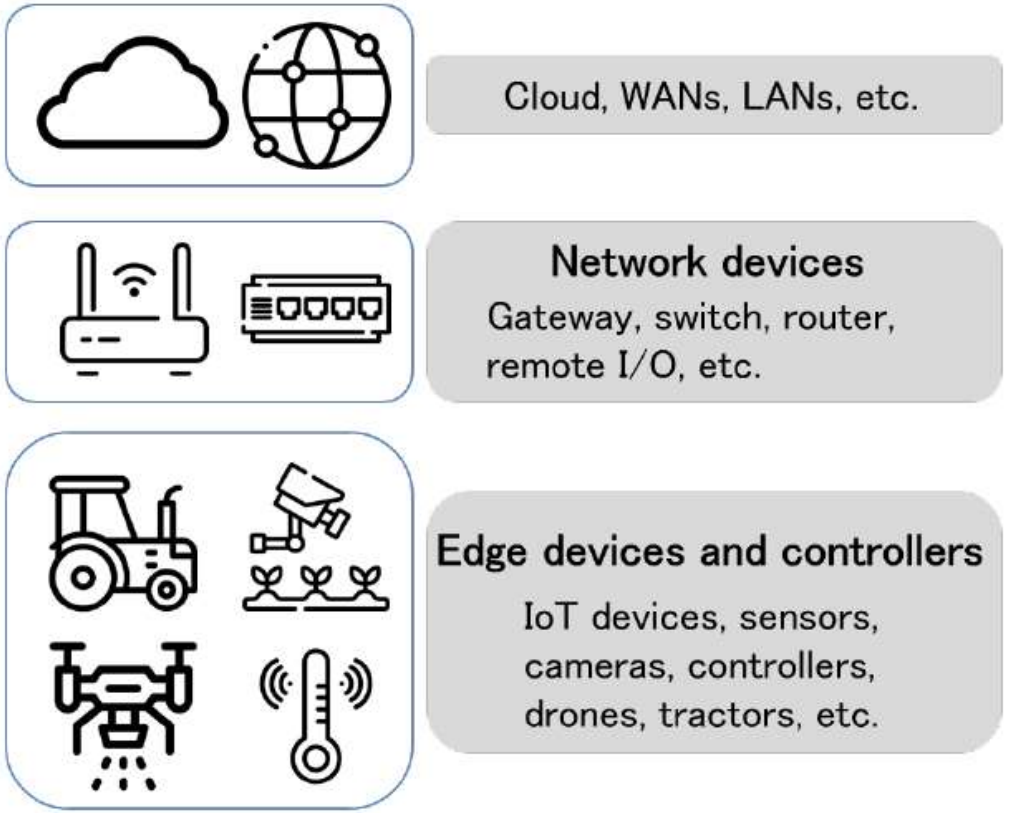
↓

Increase efficiency, improve quality, and reduce labor

↓

Agricultural IoT will gain popularity

◆ **Smart Farm Configuration**



Taxonomy for agricultural IoT

❖Purpose

- To investigate the vulnerabilities in practical scenario

❖Method

- We divide the survey product into devices and system/service, then divide them again into smaller categories

❖Range of the investigation:

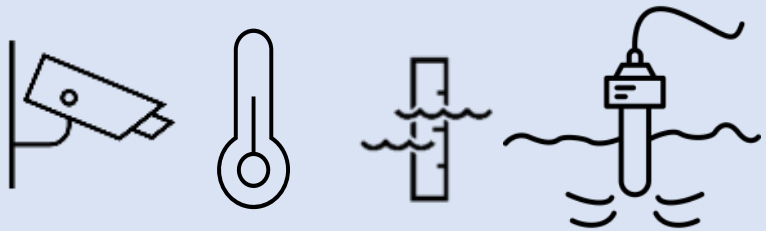
- Focus on devices in the farming event called Japan Agri Innovation in 2023
- Products that are showed on the websites of exhibitors are included too

➢In total, 175 products was included

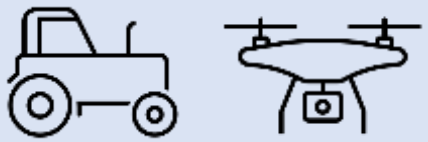
Taxonomy for agricultural IoT device

Agricultural IoT devices

Sensors



Stand-alone Sensors



Build-in Sensors

Controllers

Environment control

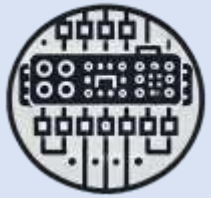
Nutrient control

Lighting control

Network devices

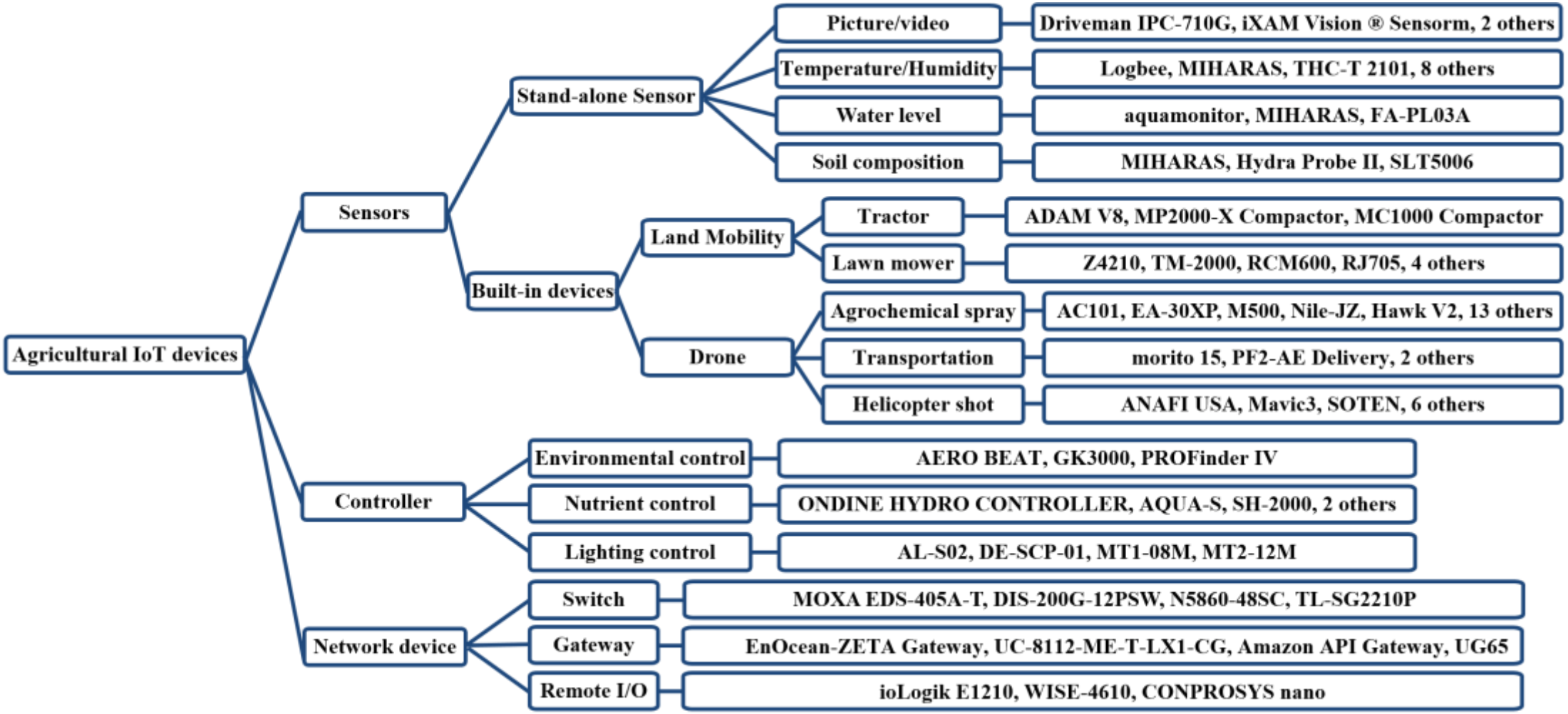
Gateway

Switch



Remote I/O

Taxonomy for agricultural IoT devices



Taxonomy for agricultural IoT devices

Taxonomy for agricultural IoT systems and services

Agricultural IoT systems and services

Systems

Production management

Water level control

Growth evaluation

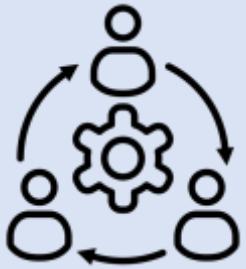
Environmental monitoring

Services

Positioning observation

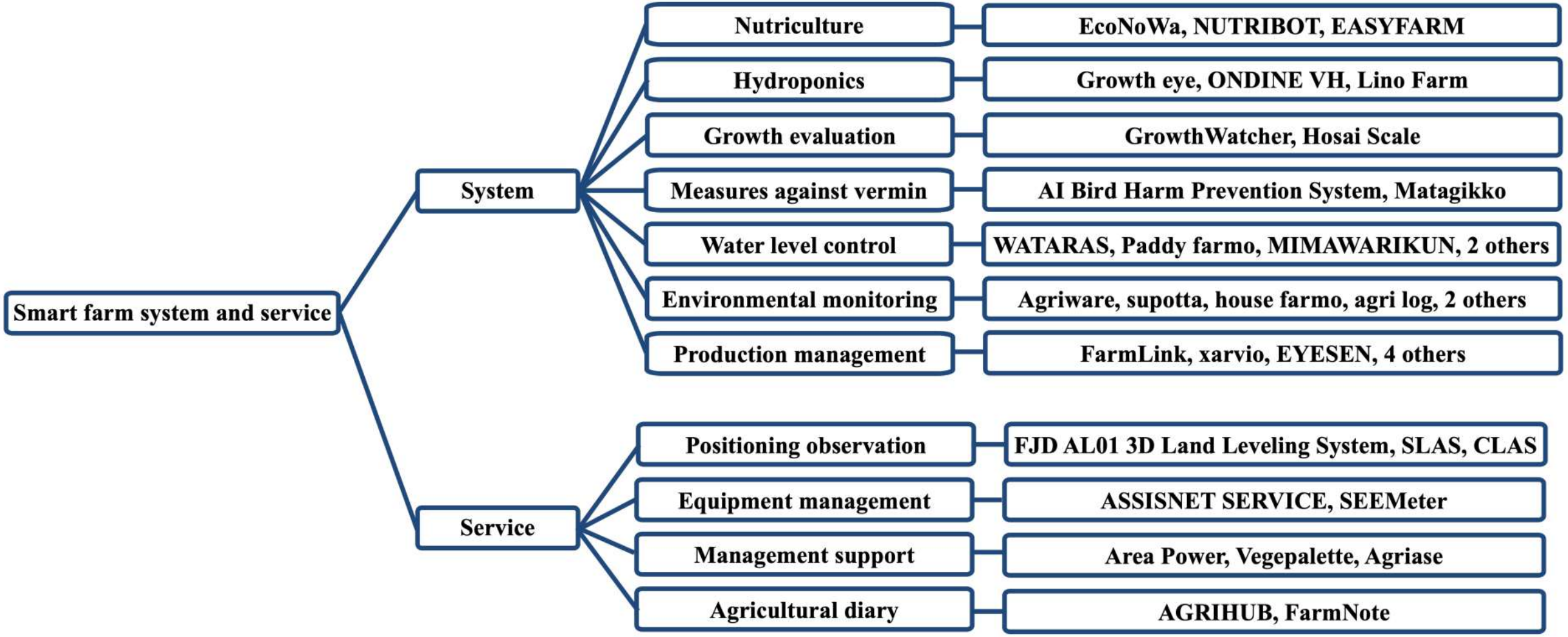
Agricultural diary

Equipment management



Management support

Taxonomy for agricultural IoT systems and services



Taxonomy of smart farm systems and services

Investigation of emerging threats

❖Purpose

- To identify security risks and network vulnerabilities

❖Method:

- We used Shodan* to search for device types, versions, locations, IP addresses, and open ports
- A high number of hits indicates the product's widespread use, large user base, and high-security importance in agriculture

❖Range of the investigation:

- All device searchable by Shodan
- 175 products exhibit at AGRI NEXT

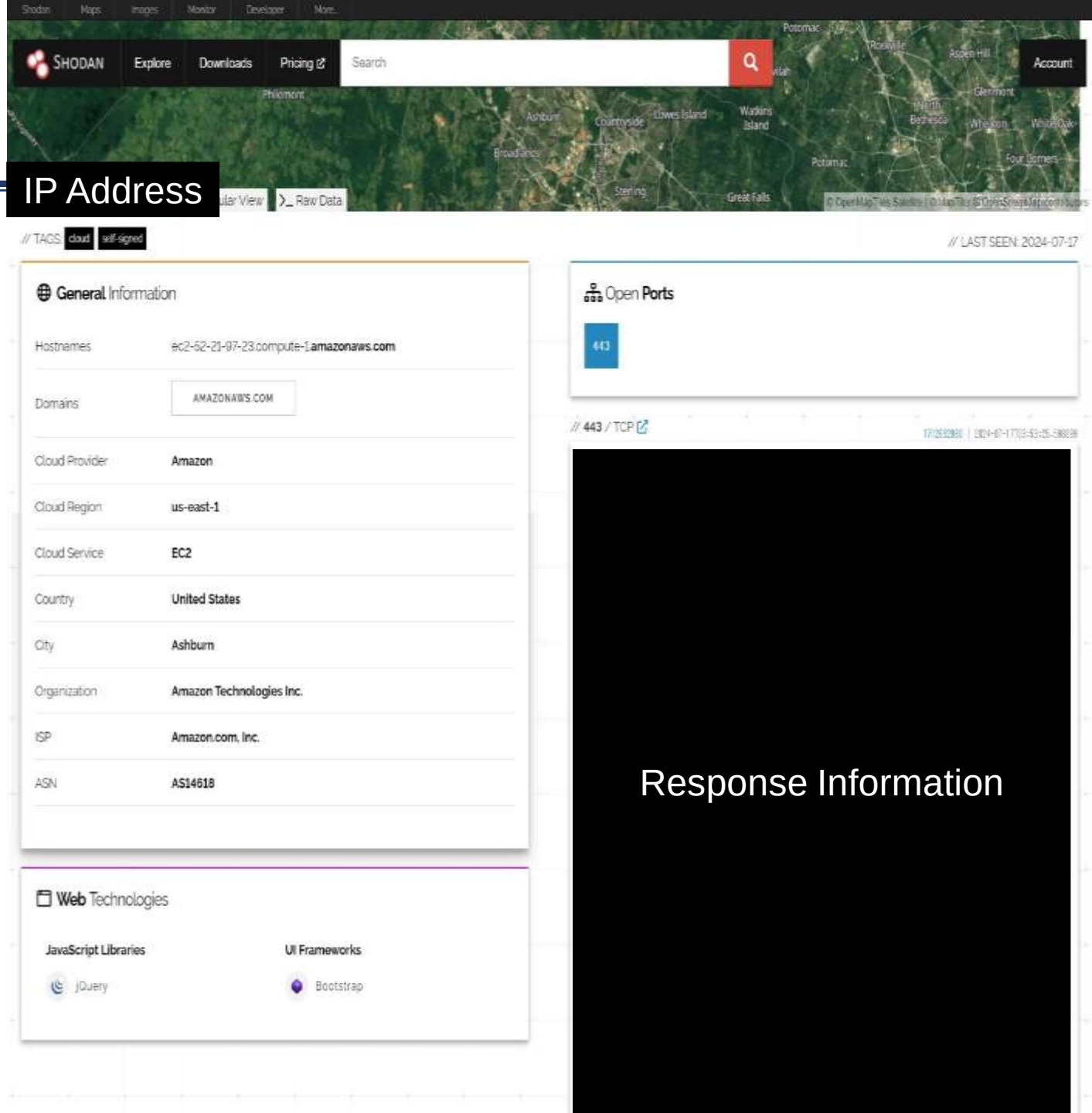
*Shodan. "Shodan: The search engine for internet-connected devices.", https://www.shodan.io/, Accessed on May 9, 2024.

Shodan

- **Shodan** is a security search engine that allows you to search for Internet-connected devices and services

- Information on publicly available devices such as webcams, servers, and routers is collected and used for security diagnosis and vulnerability identification

- We search the agricultural IoT in Shodan to determine its location, open port numbers, etc., to see if it is vulnerable



Result of investigation (Emerging threats)

❖Shodan search result

Product	Country	Purpose	description	Devices Hit[a]
Sensor A	Japan	Temperature, Humidity, Water level	Three types of agricultural IT sensors for paddy fields, fields, and weather. Users can upload measurement data to the cloud.	2
Service A	Korea	Application	Service for storing sensor data. Graph display and Excel file downloads are provided for the user.	8
System A	Japan	water level control	A water level management system comprises a water level sensor, supply gate, and cloud infrastructure. It enables remote water management for paddy fields.	1
System B	Korea	Production management	A smart remote control system comprises sensors, controllers, and a cloud infrastructure. It enables the user to monitor sensor data and view camera footage.	5
System C	United States	Production management	This cultivation management support system enables the user to observe changes in crop growth and uneven growth within fields by acquiring imagery from satellites and analyzing it using AI.	19

[a] They are the same product type but are associated with different IP addresses.

The results showed that most of the products were not hit by the Shodan search as only 31/175 products were returned as hits.

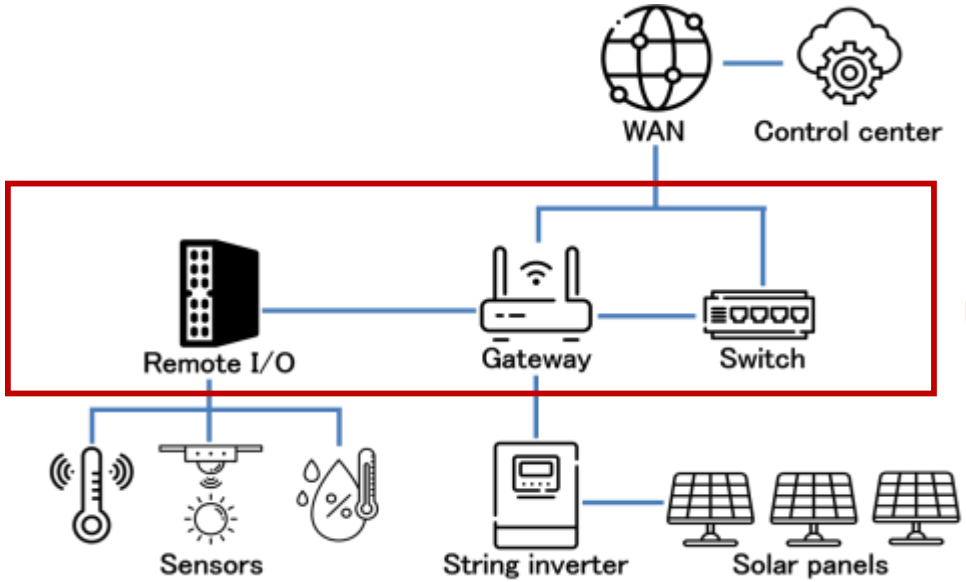
Investigation of potential threats

❖Use case of solar power plant

Focused on network devices commonly used in agriculture as well

- The official diagram includes specific product names
- Collected products with similar functions from the same vendor

Conducted a vulnerability investigation of the collected products using **Shodan** and **NVD**, as previously described



Network devices commonly used in **agriculture** as well

Result of investigation (Potential threats)

❖Shodan search and NVD result

Product	Shodan[a]	CVEs[b]	Overview of CVE
Switch	4	4	- Certificate and password management vulnerabilities. - Cross-site scripting (XSS) vulnerability in the diagnostic ping function of the switch's management web interface. - GoAhead web server on the switch can cause a remote authenticated user to cause a denial of service (reboot) via a crafted URL. - The switch's admin web interface allows remote authenticated users to bypass the read-only protection mechanism using Firefox with a web developer plugin.
Gateway	13	1	- Vulnerability to execution with unnecessary privileges could allow an attacker with user-level privileges to gain root privileges.
Remote I/O	9	4	- Users are restricted to using short pass. - Passwords are transmitted in a format that is not sufficiently secure. - The web application does not sanitize input, enabling script injection or code execution by attackers. - Web applications may not adequately verify that the request was provided by a valid user (CROSS-SITE REQUEST FORGERY).

(a) Number of devices hit by Shodan.
(b) Number of CVEs related to products in (a).

Result of investigation (Potential threats)

❖Web GUI threats found in Shodan

Web GUI (A)

Web GUI (B)

Web GUI (C)

Login screens were accessible from the outside

- Exposure to unauthorized access
- Create potential for further exploitation

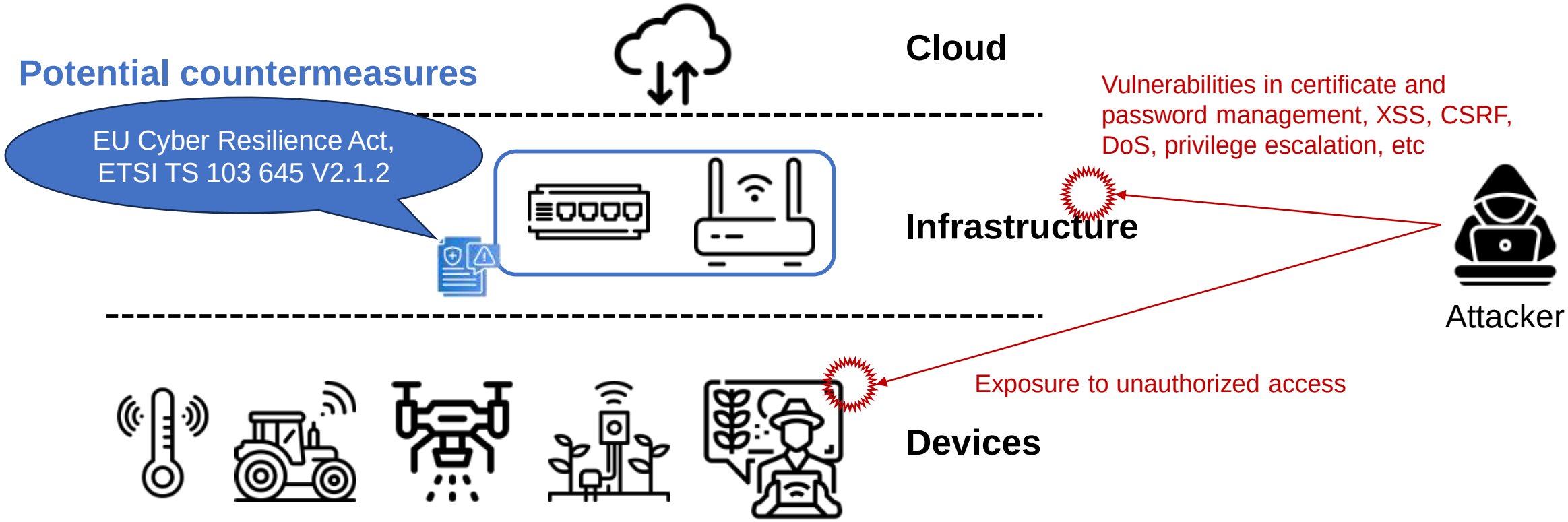
Standardization related to Agriculture

Standards	Year	Description
The IoT Cybersecurity Improvement Act	2020	This bill requires the National Institute of Standards and Technology (NIST) and the Office of Management and Budget (OMB) to take specified steps to increase cybersecurity for Internet of Things (IoT) devices. IoT is the extension of internet connectivity into physical devices and everyday objects.
SB-327	2020	SB-327 mandates that manufacturers of connected devices equip them with "reasonable security features" that are appropriate to the nature and function of the device. These features should protect the device and any information contained within it from unauthorized access, destruction, use, modification, or disclosure.
Cybersecurity Act	2019	ENISA, the EU Agency for cybersecurity, will have a key role in setting up and maintaining the European cybersecurity certification framework by preparing the technical ground for specific certification schemes. It will be in charge of informing the public on the certification schemes and the issued certificates through a dedicated website.
EU Cyber Resilience Act	2022	The proposal for a regulation on cybersecurity requirements for products with digital elements, known as the Cyber Resilience Act, bolsters cybersecurity rules to ensure more secure hardware and software products.
Product Security and Telecommunications Infrastructure Act 2022	2022	The bill establishes security standards for products that can be connected to the Internet, including smart devices and IoT devices. Among other things, it includes a ban on default common passwords and an obligation to provide information on product security.
ETSI TS 103 645 V2.1.2	2020	This specification sets forth the security standards required for IoT devices. Specifically, these include prohibiting default passwords, encryption to protect data, and providing security updates.
ISO/IEC-27400	2022	This standard provides a framework for security controls in the design, development, and operation of IoT systems. This includes risk assessment, security control selection, and security incident response.

Standardization related to Agriculture

Standards	Year	Description
CSA IoT Security Controls Framework v2	2021	CSA IoT Security Controls Framework v2 is a framework for managing the security of enterprise IoT systems. In version 2, controls have been technically clarified and new domain structures, legal controls, and security tests have been introduced. Simplified device types also facilitate the distribution of controls. An accompanying guide explains how to use the framework and provides detailed instructions to help evaluate and implement IoT systems.
GSMA IoT Security Guidelines	2024	The GSMA IoT Security Guidelines provide detailed recommendations for the secure design, development, and deployment of IoT services. They cover a broad scope, including networks, services, and endpoint ecosystems, and address security issues, attack models, and risk assessments. Specific real-world examples are also provided.
ETSI EN 303 645 V2.1.1	2020	ETSI EN 303 645 V2.1.1 is a standard that sets security standards for consumer IoT devices. Key requirements include prohibition of default passwords, mandatory security updates, and data encryption. It also requires security incident notification, vulnerability management, and continuous security monitoring. This will enhance the security of IoT devices and improve consumer data protection and privacy.
NISTIR 8259A	2020	This publication defines an Internet of Things (IoT) device cybersecurity capability core baseline, which is a set of device capabilities generally needed to support common cybersecurity controls that protect an organization's devices as well as device data, systems, and ecosystems.
ENISA Baseline Security Recommendations for IoT	2017	The IoT Security Proposal aims to improve IoT security and coordination among stakeholders through regulatory harmonization, security awareness, development of development lifecycle guidelines, consensus on interoperability, provision of economic incentives, establishment of lifecycle management, and clarification of responsibility boundaries by the European Commission. The goal is to improve the security of the IoT and coordination among stakeholders.
Securing the Internet of Things for Consumers	2020	Securing the Internet of Things for Consumers provides guidelines for enhancing consumer security for IoT devices. It defines security requirements and best practices for devices and specifies risk management and countermeasures. It also includes advice to help consumers choose and use devices safely. The goal is to make IoT devices more secure and to enhance consumer privacy and data protection.

Current standards as potential countermeasures



Limitations of current standards

- Existing IoT security standards are applicable but lack specific focus on agricultural IoT
- There is no recommendation for agricultural people to follow the latest appendix

Conclusion

❖ Contribution:

- We developed a taxonomy and conducted a security survey of agricultural IoT devices
- Currently, there are few attacks currently, but risks are expected to grow as smart farming expands

❖Recommendations

We call for specific IoT security standards and stronger collaboration within the agricultural sector

*This research result is partly supported by the ASEAN IVO project of NICT [1]

[1] Agricultural IoT based on Edge Computing
https://www.nict.go.jp/en/asean_ivo/ASEAN_IVO_2022_Project02.html

Thank you!