Information Security (SEC) Research Team

Dr. Montida PATTARANANTAKUL
Researcher

Information Security Research Team
Communication and Networks Research Group,
National Electronics and Computer Technology Center (NECTEC), Thailand

Computer Networks in Southeast Asia (CNSEA) Virtual Lab Tour
Jul 27, 2023

Team members

- **SEC Research Team Leader**
  - Dr. Soontorn Sirapaisan, Researcher
- **Researchers**
  - 4 researchers (3 PhDs from UK and France)
- **Research Assistants and Engineers**
  - 5 research assistants and engineers
- **Pursuing the Doctoral Degree**
  - 1 studying PhD in Belgium
  - 1 studying PhD in Australia

Dr. Soontorn Sirapisan, Team Leader

Dr. Chalee Vorakulpipat

Dr. Montida Pattaranatakul

Ekkachan Rattanalerdnusorn

Phithak Thaenkaek
(PhD candidate)

Kajornsak Piyoungkorn

Sineenat Tienkouw

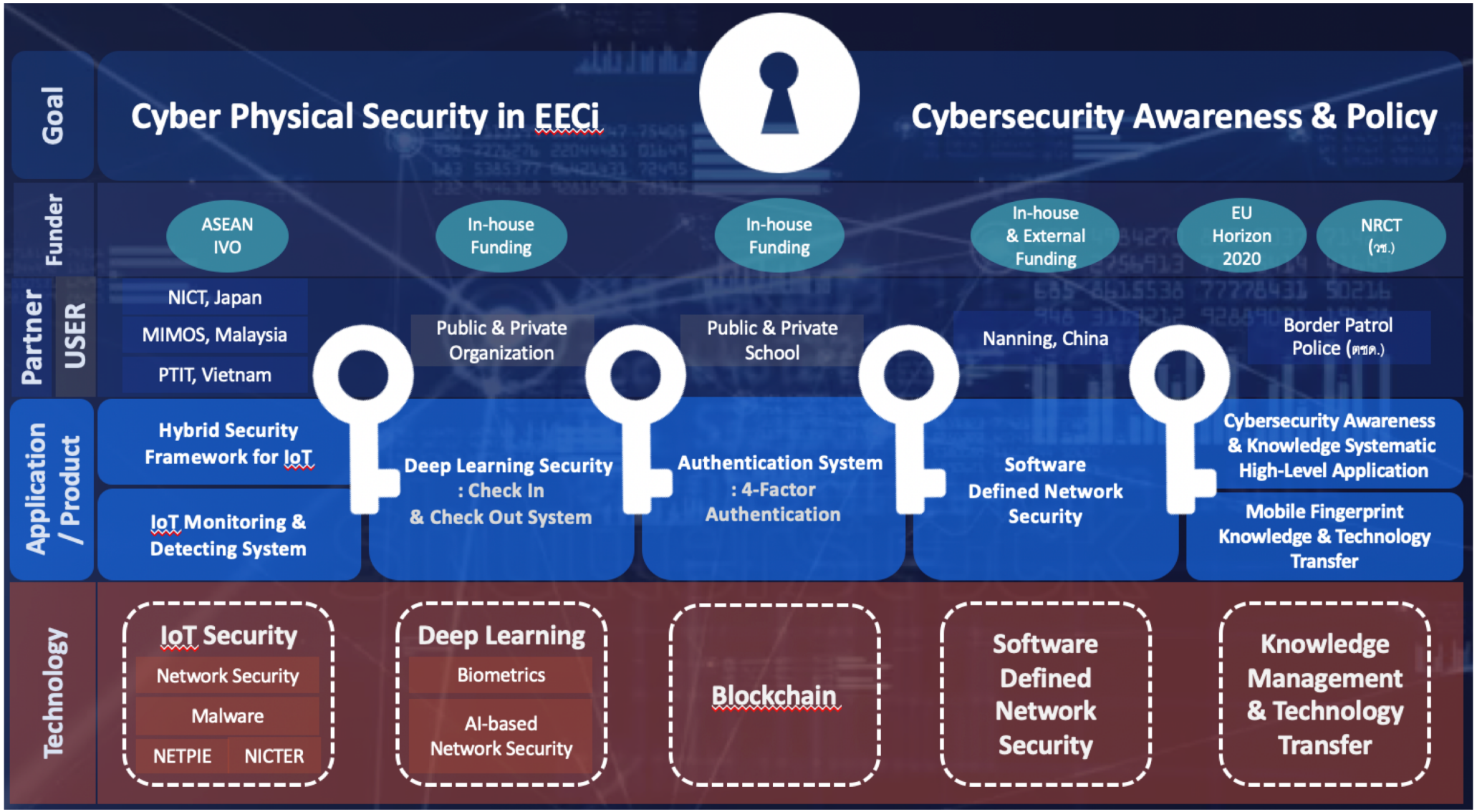
Sasakorn Pichetjamroen

Siriboon Chaisawat
(PhD candidate)

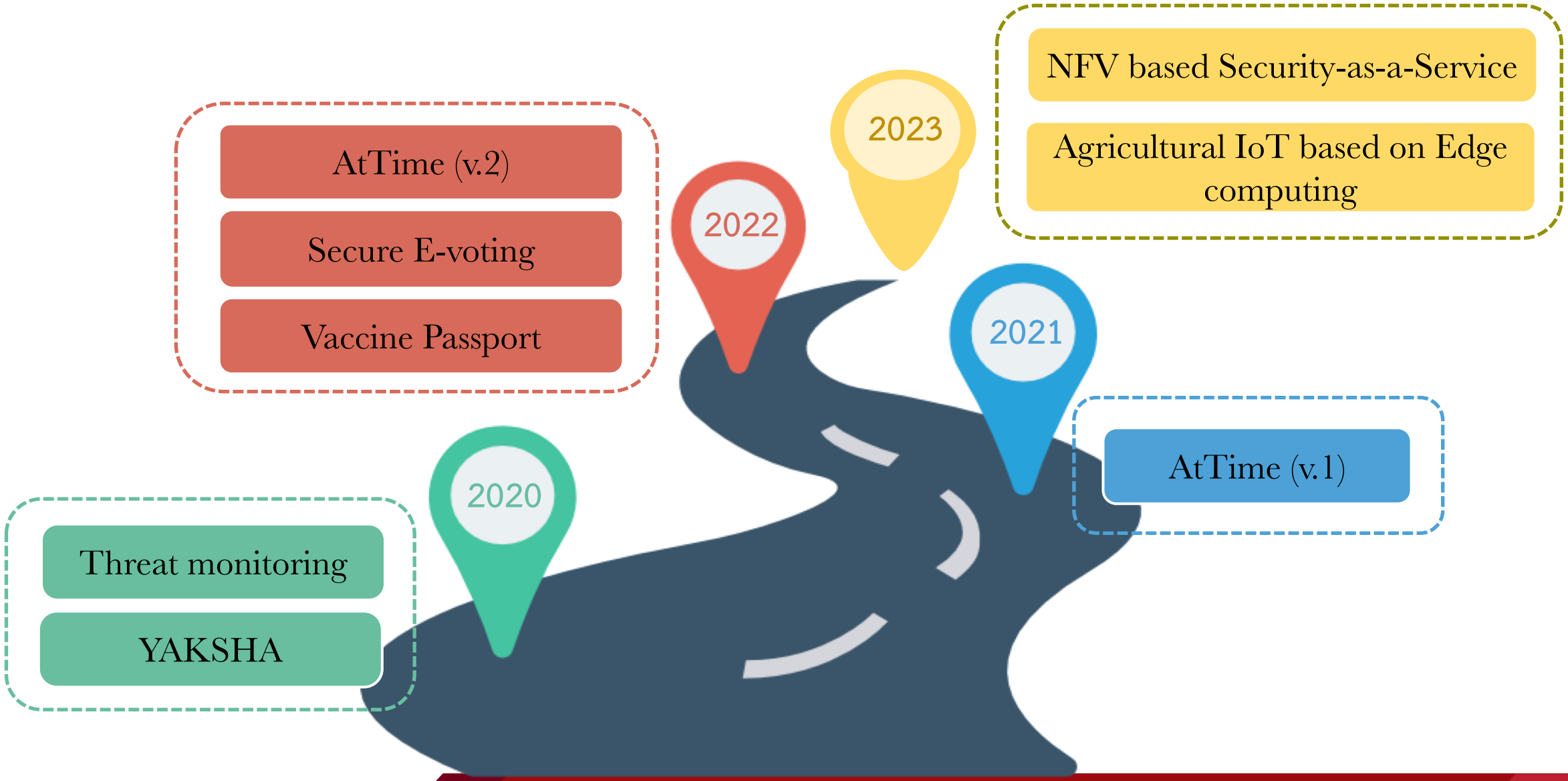
Apiwat Chantawibul

Parn Sirimapron

Research interests



SEC's Road Map

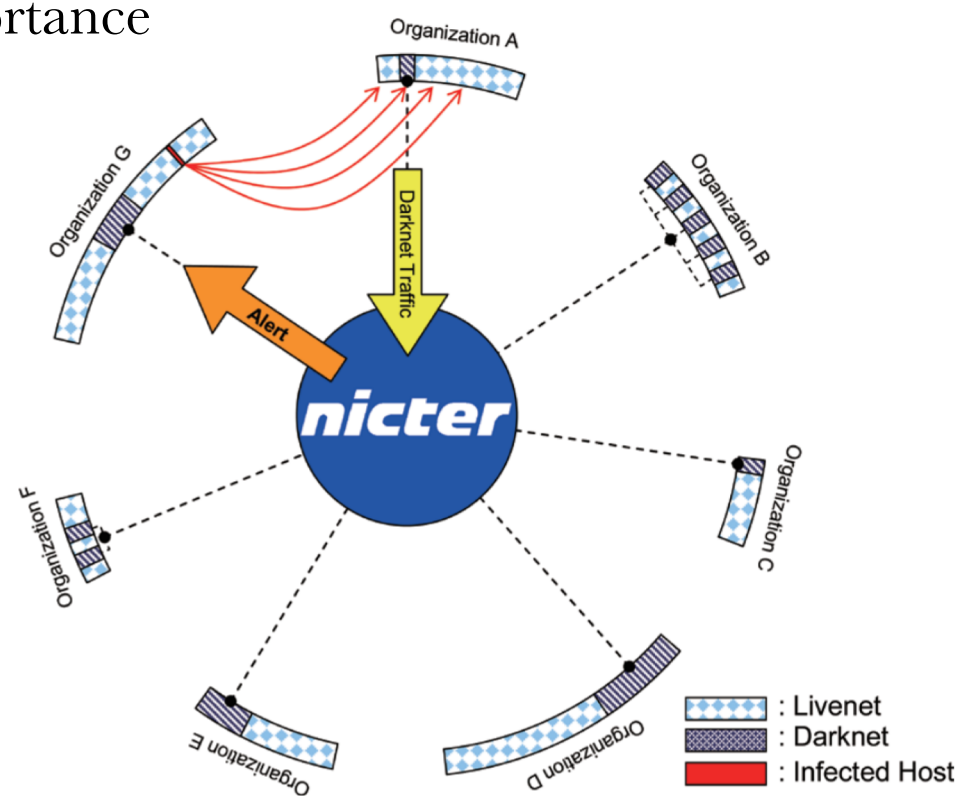


1. Threat monitoring

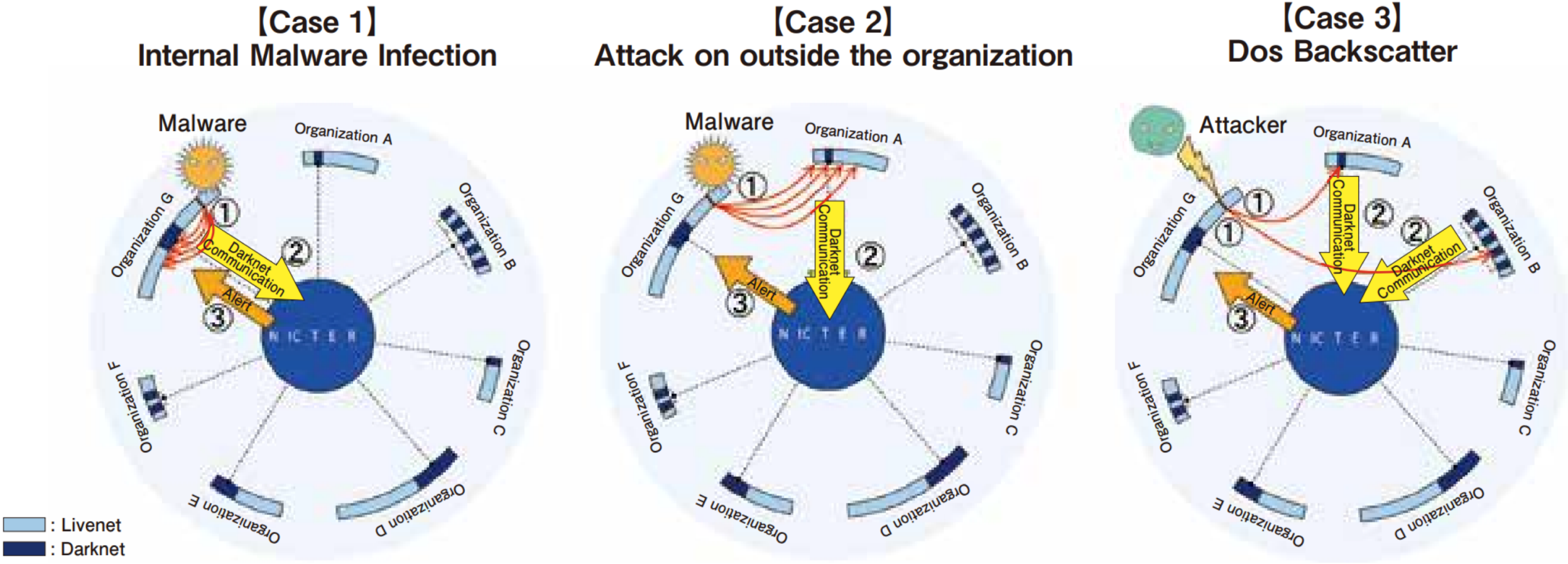
- Malwares are spread all over cyberspace and often lead to serious security incidents
- A darknet (a set of unused IP addresses) is an example of attack surface
- The availability of cyber monitoring is of a paramount importance

Contributions:

- An effective approach for analyzing the global trends of network threats is mandatory
- Therefore, we develop the **threat monitoring** platform for monitoring and analyzing the traffic destined to allocated or routable to unused IP address space (known as Darknet)

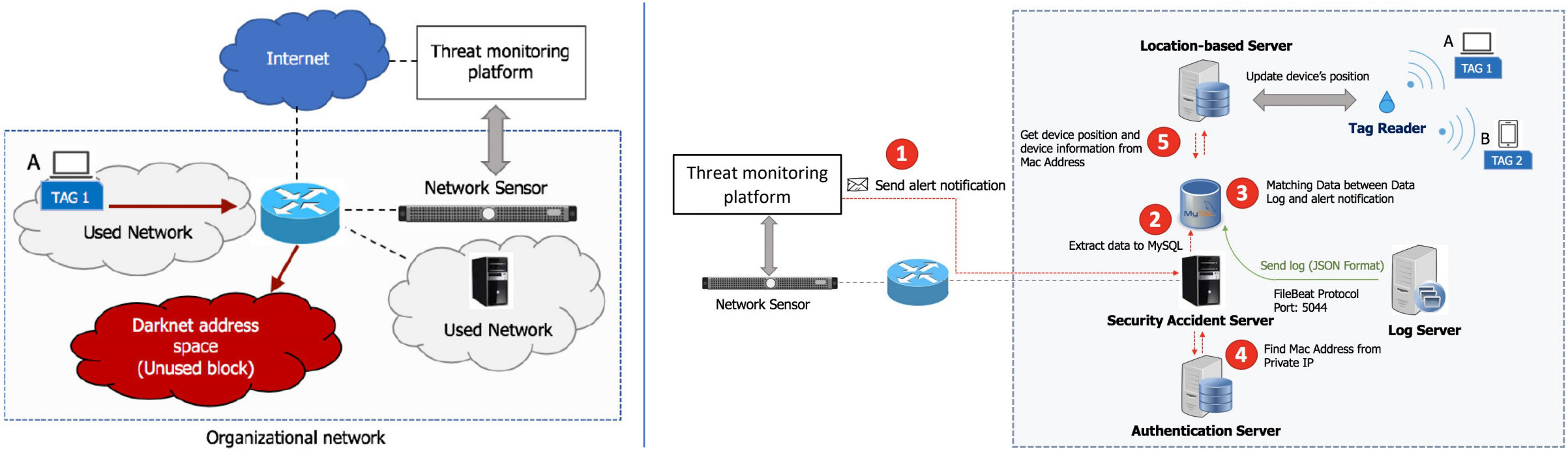


- If there is any traffic attempting to connect to the Darknet space, the system will notify alert about this aberrant behaviors



2. IoT-based monitoring and detecting system

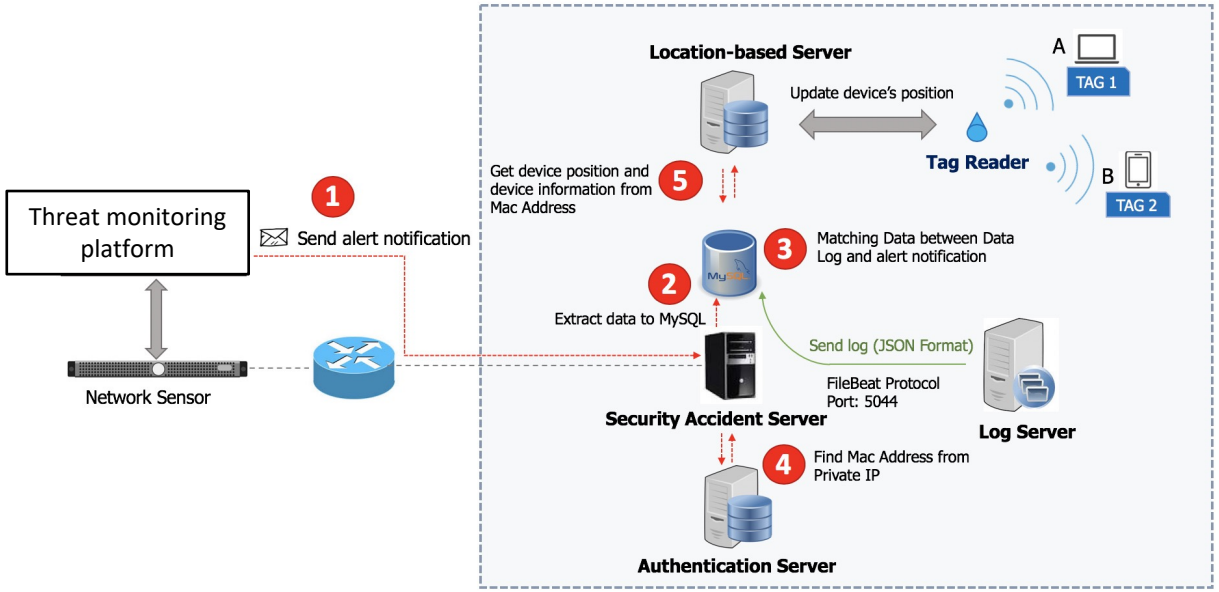
- When IoT devices attempt to connect to other network nodes, all related packets will be captured by a network sensor and consequently analyzed by threat monitoring platform
- To pinpoint the actual locations of the compromised IoT devices, we deploy **a security accident server** for IoT device tracking

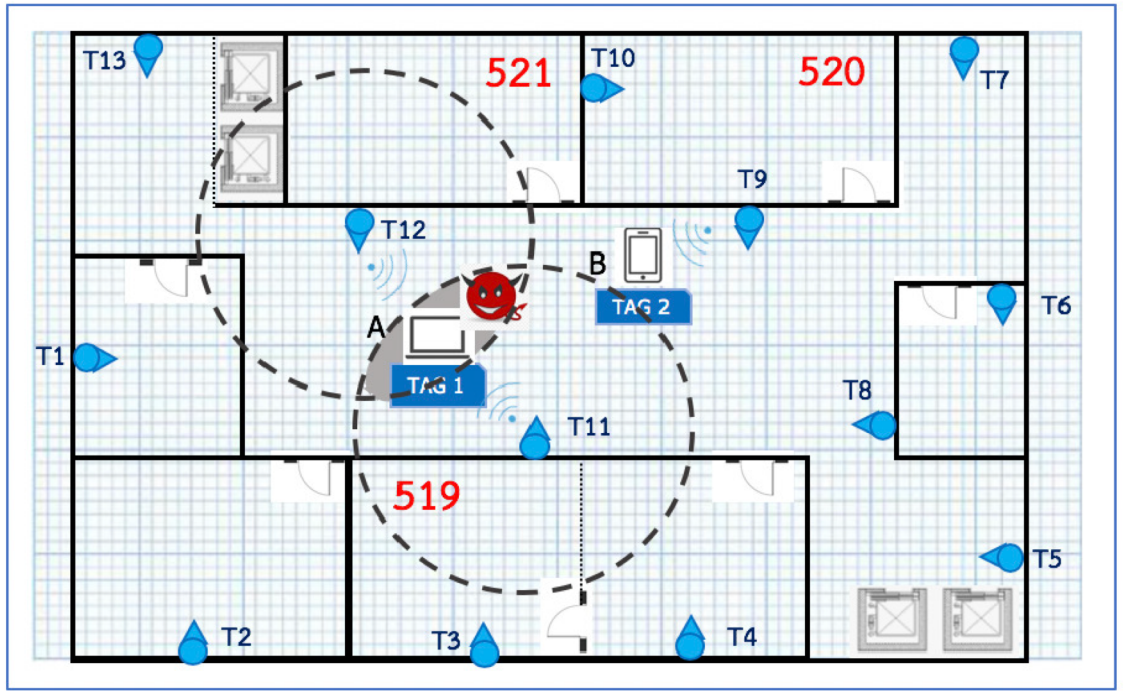


Source: E. Rattanalerdnusorn, M. Pattaranantakul, P. Thaenkaew, and C. Vorakulpipat, "IoTDePT: Detecting Security Threats and Pinpointing Anomalies in an IoT Environment", *ICSCA' 20*, Feb 18-21, 2020.

A security accident server performs two main tasks:

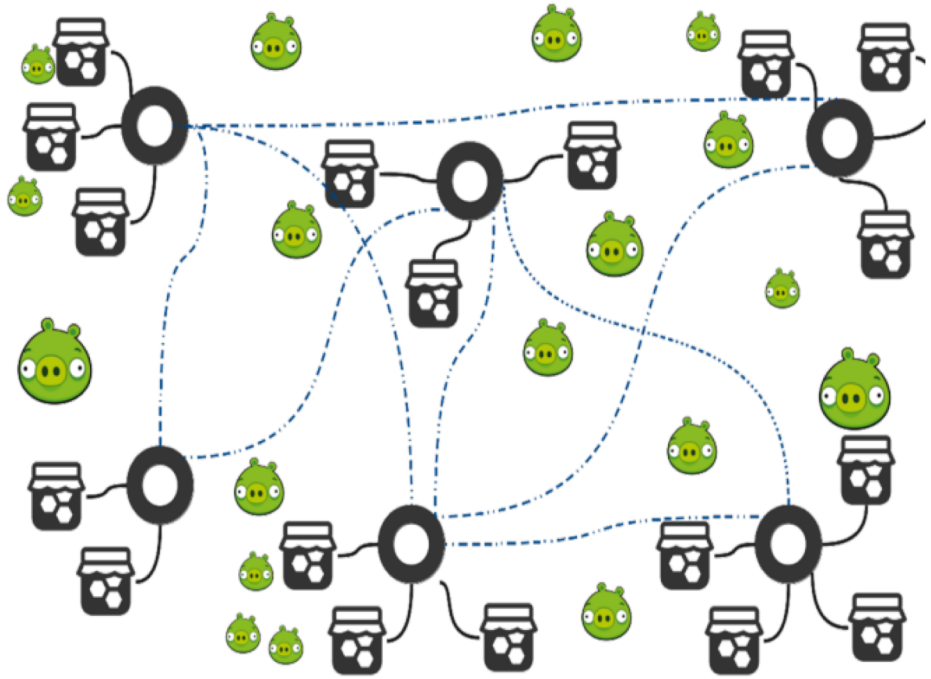
- It records incident information for future use
- It tracks the location of the compromised IoT device in the organizational network

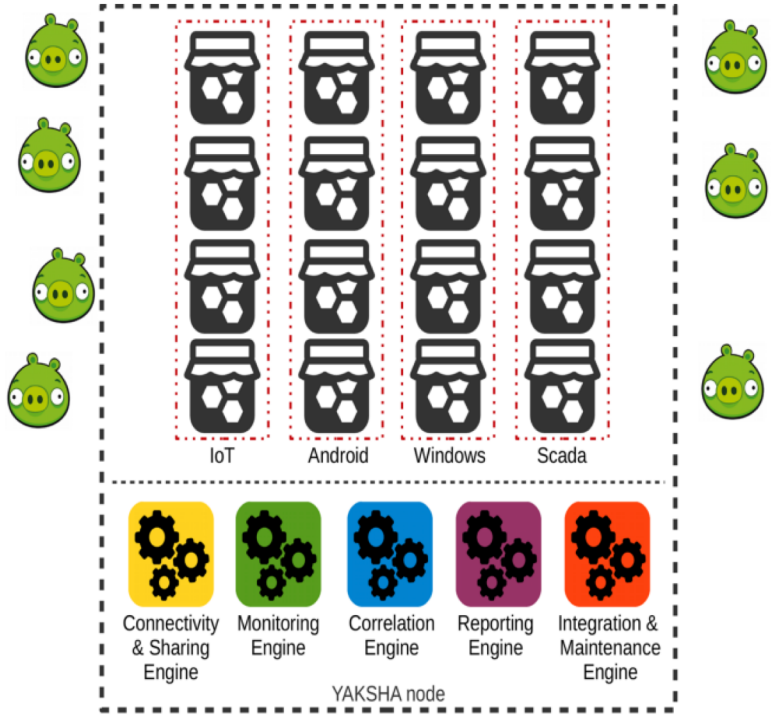




3. YAKSHA

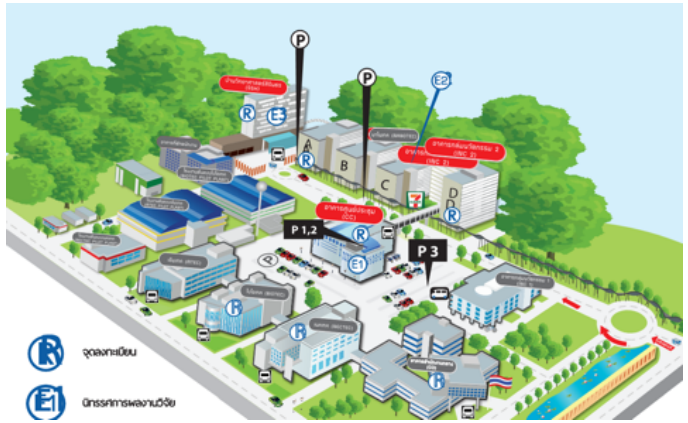
- **YAKSHA** – c**Y**ber **A**wareness and **K**nowledge **S**ystemic **H**igh-level **A**pplication
- The project aims to develop a software toolkit to improve cybersecurity of organization in the ASEAN region
- The core concept is developed based on **Honeypot Analytics as a Service**



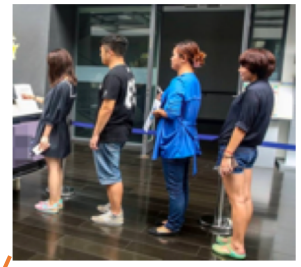


4. AtTime: Multi-factor Attendance Authentication System

- Traditional passwords aren't secure enough anymore
- Hackers may launch a brute force attack to crack user's credentials and gain unauthorized access to private accounts
- Multi-factor authentication has been widely adopt for strengthening the accuracy of user identity
- A use case of **"Time attendance using multi-factor authentication"** has been developed



Online check-in

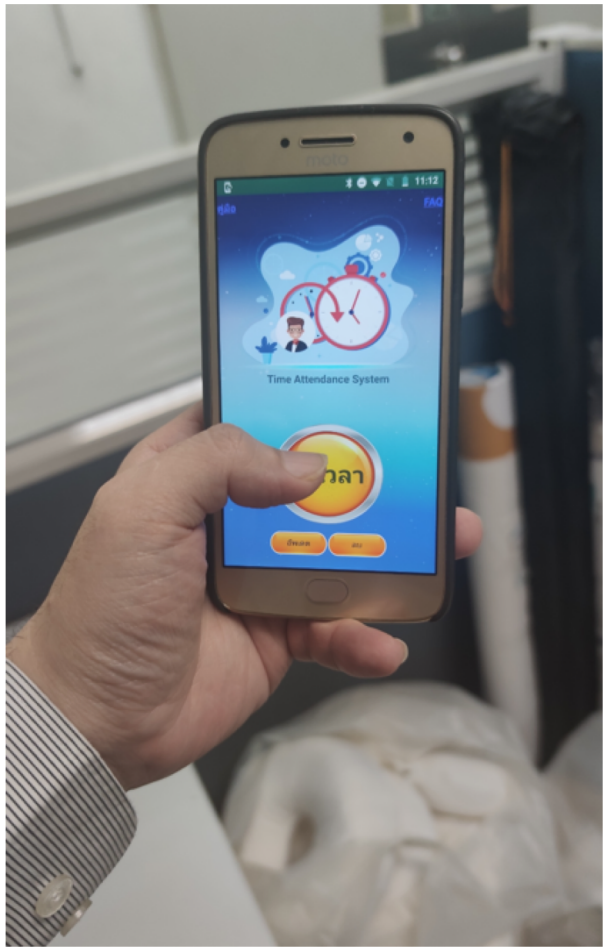


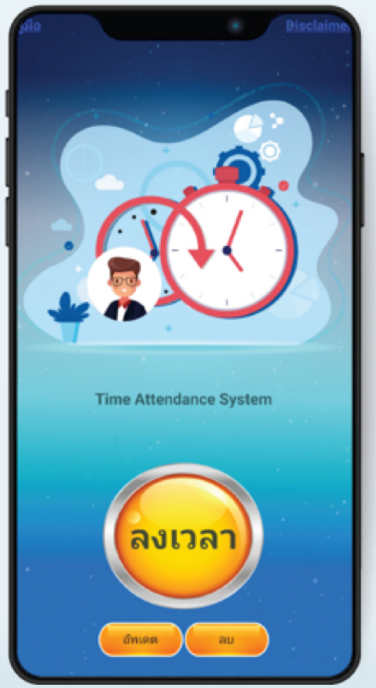
Reduce queuing time

No need an ID card

Touchless interaction

- There are three steps for use



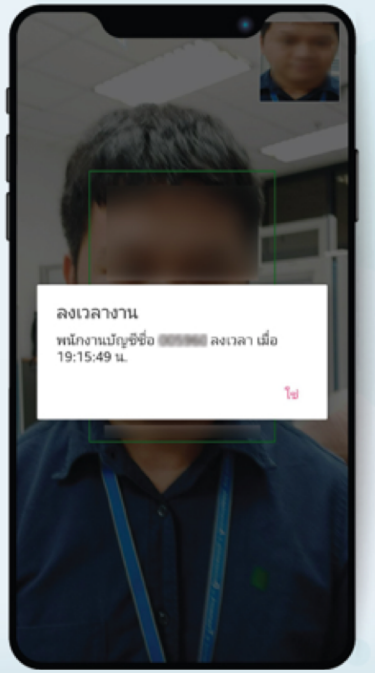


Check-in: Connect to intranet WiFi and click Chek-in botton

1

Multi-factor authentication

2



Validation: Check whether the displayed check-in time is correct, if so then click yes

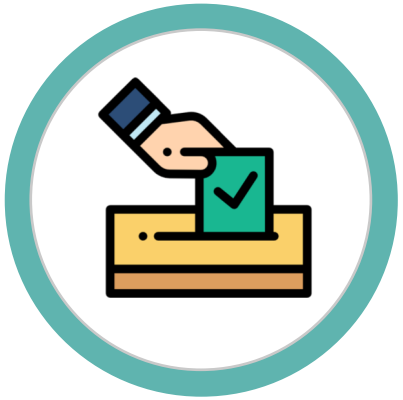
3

5. Face recognition and verification for security

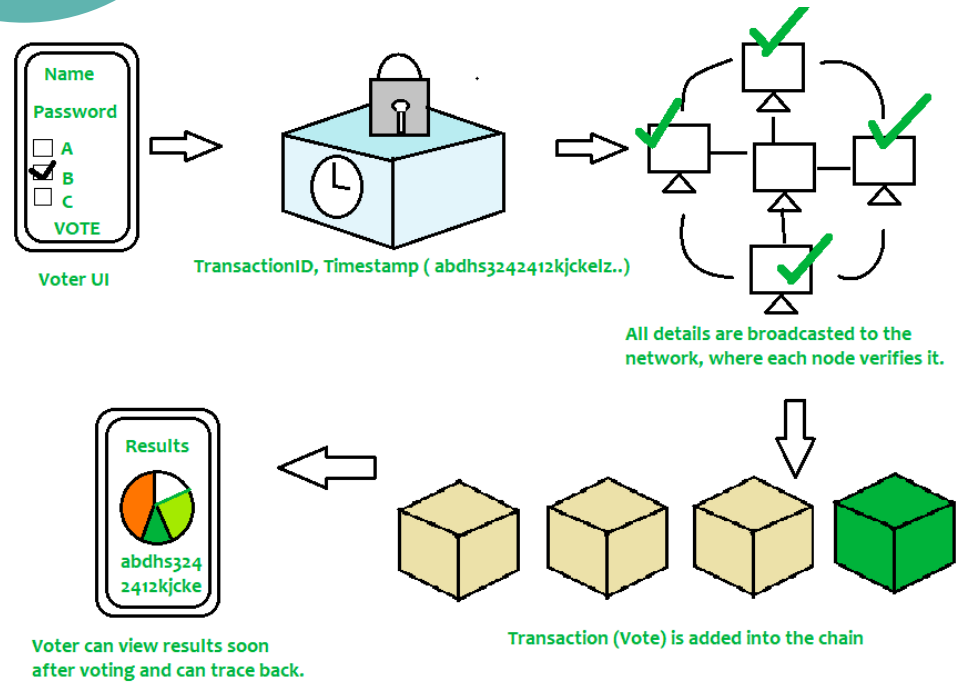
6. µTherm-FaceSense

- It is a non-contact measurement system used to evaluate the body temperature during the COVID-19 pandemic
- Two core technologies (**face recognition** and **temperature measurement**) have been applied

7. Secure E-voting based on Blockchain technology

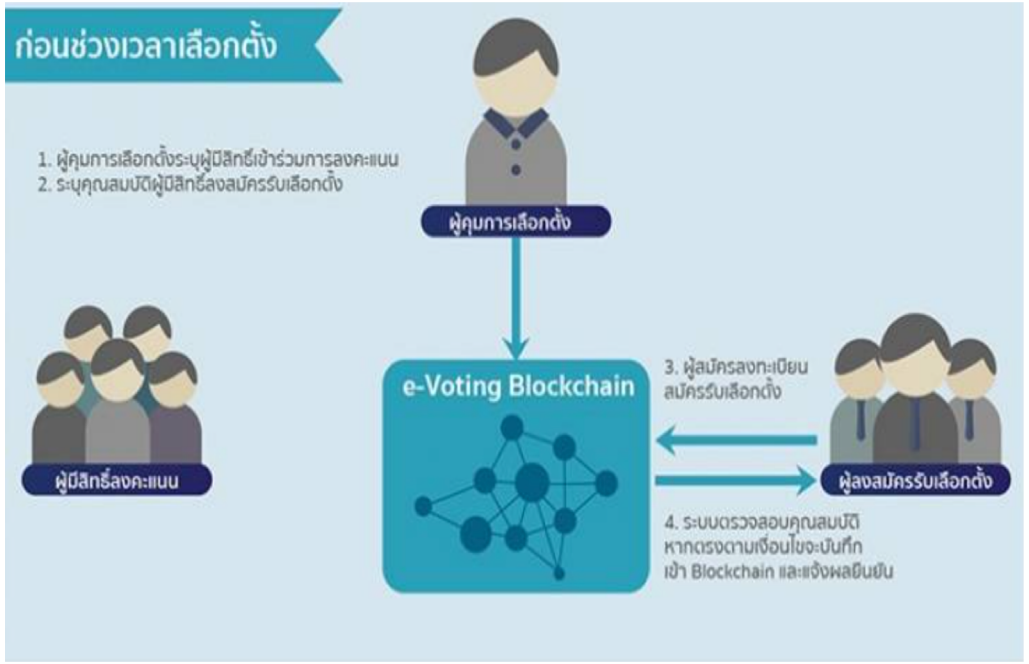


- Traditional voting suffers from several drawbacks: costly and time consuming, inefficiency, error-prone, and electoral frauds
- Election voting method must be legal, accurate, safe, and convenient

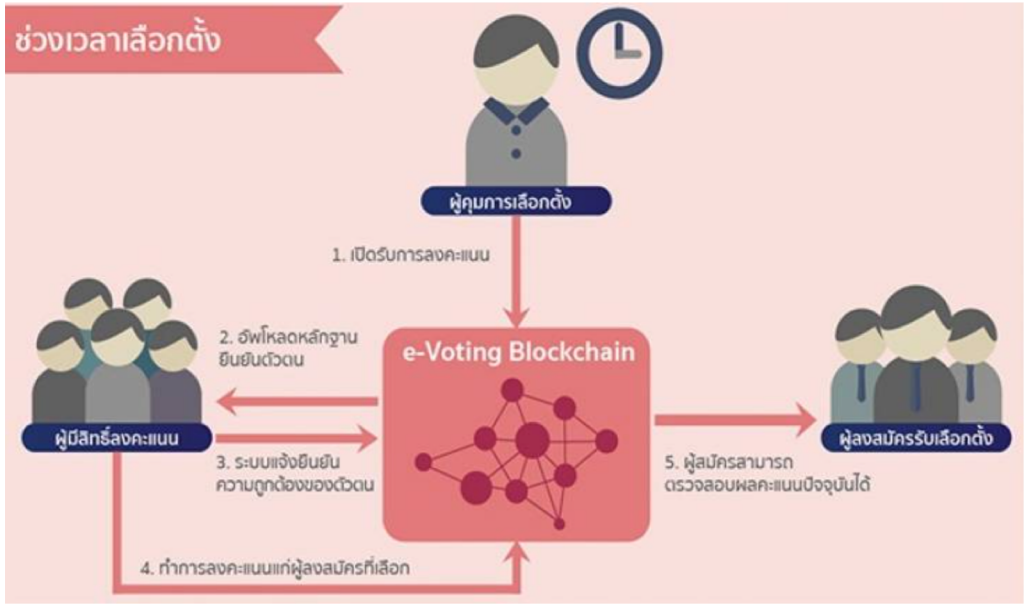


- Decentralization
- Immutability
- Data integrity
- Transparency and verifiability
- Privacy and security

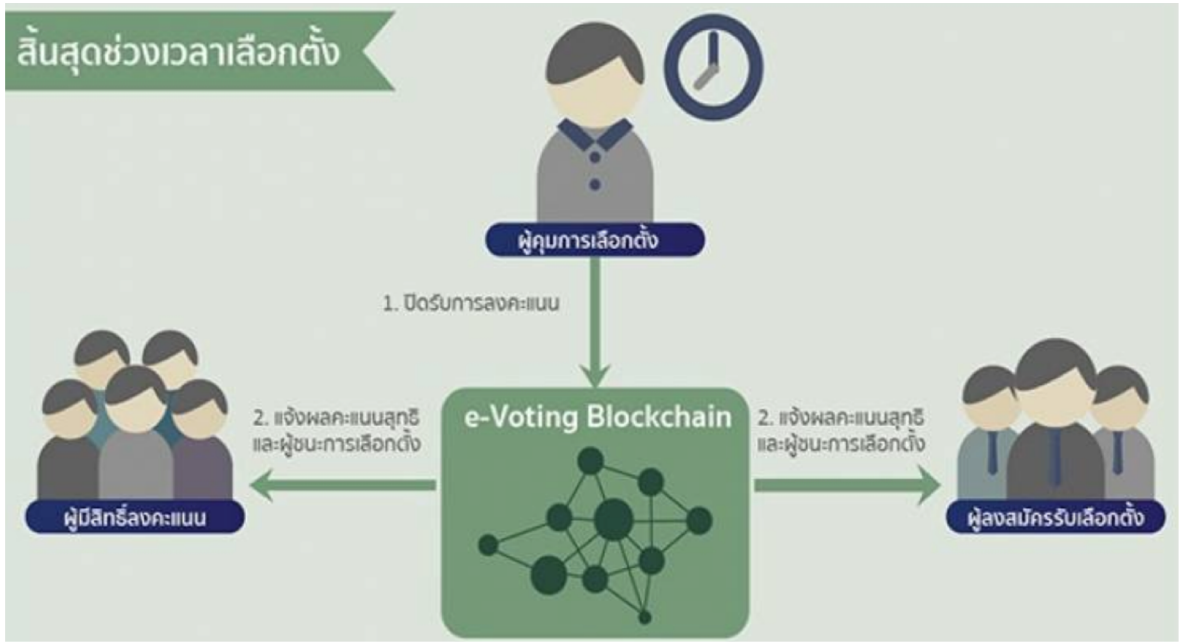
- **Before the election**
  - An election controller identifies voter qualifications
  - Candidates register in the system, through which the election controller can check their eligibility



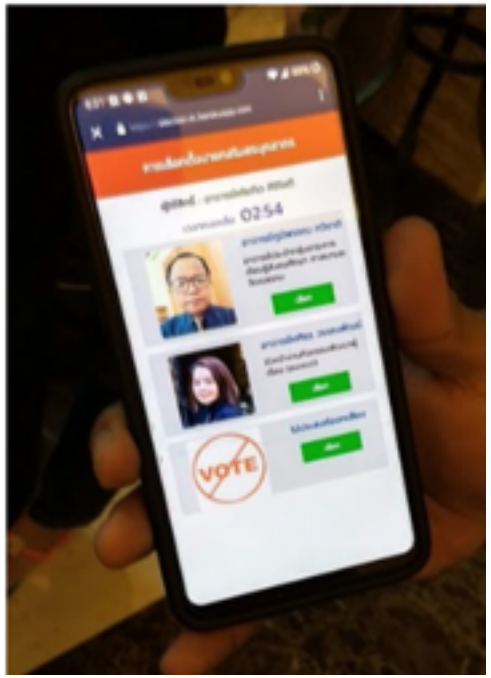
- **During the election**
  - The voters no need to know about the Blockchain
  - They can simply vote through an email and click vote electronically



- **After voting**
  - The results will be calculated and sent the election controller
  - The candidates are able to check their own votes



- A pilot project used at a student election in Saint Joseph Convent School, Bangkok



8. Vaccine Passport

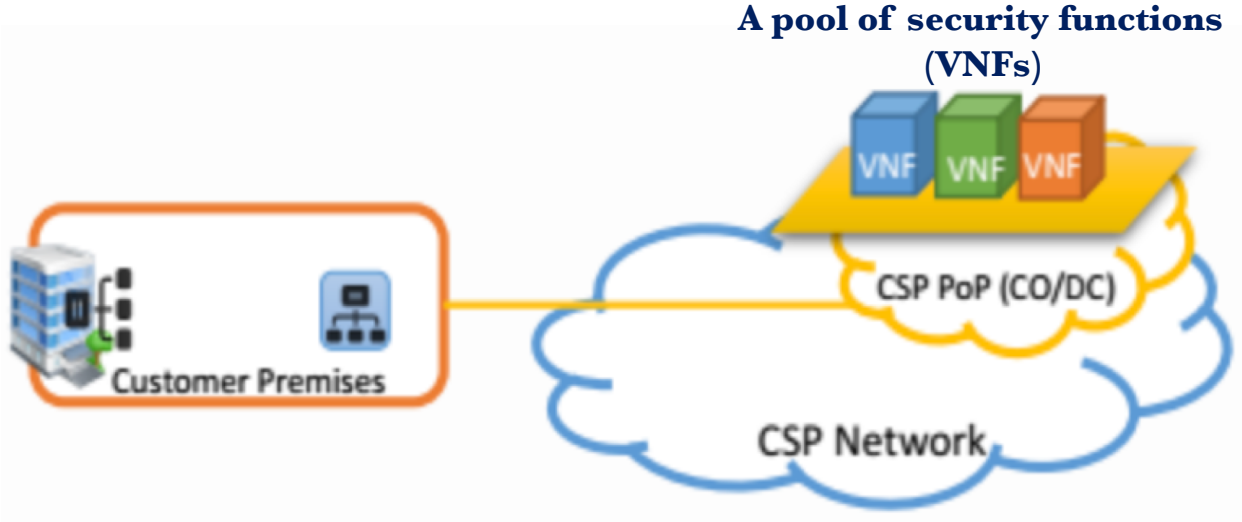
- In collaboration with the Department of Disease Control, **Ministry of Public Health (Thailand)** to issue a vaccine passport
- A platform uses to manage, issue, and verify digital vaccination certificate (e.g., showing that you were vaccinated against COVID-19)

9. NFV based Security as a Service

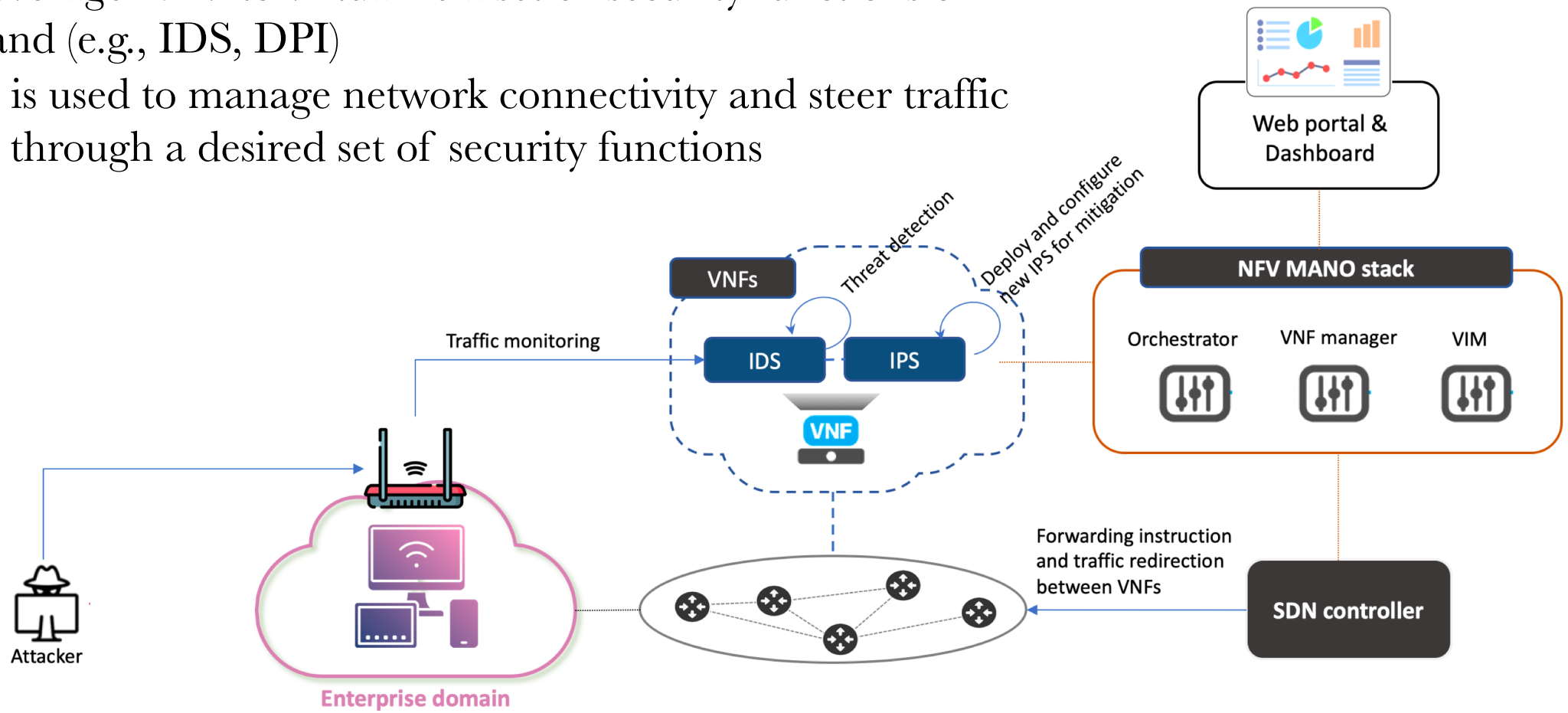
- Nowadays, many enterprises are significantly hampered by cyber-threats due to a lack of human and financial resources
- An alternative solution is to outsource security functions (i.e., VNFs) from the third-party providers

Contributions:

- We aim to build a platform of providing **an automated threat mitigation and remediation** against the cyberattacks:
  - Proactively monitor network traffic
  - Identify the risks and detect anomalies
  - Mitigate the attacks



- We leverage NFV to virtualize a set of security functions on demand (e.g., IDS, DPI)
- SDN is used to manage network connectivity and steer traffic flows through a desired set of security functions

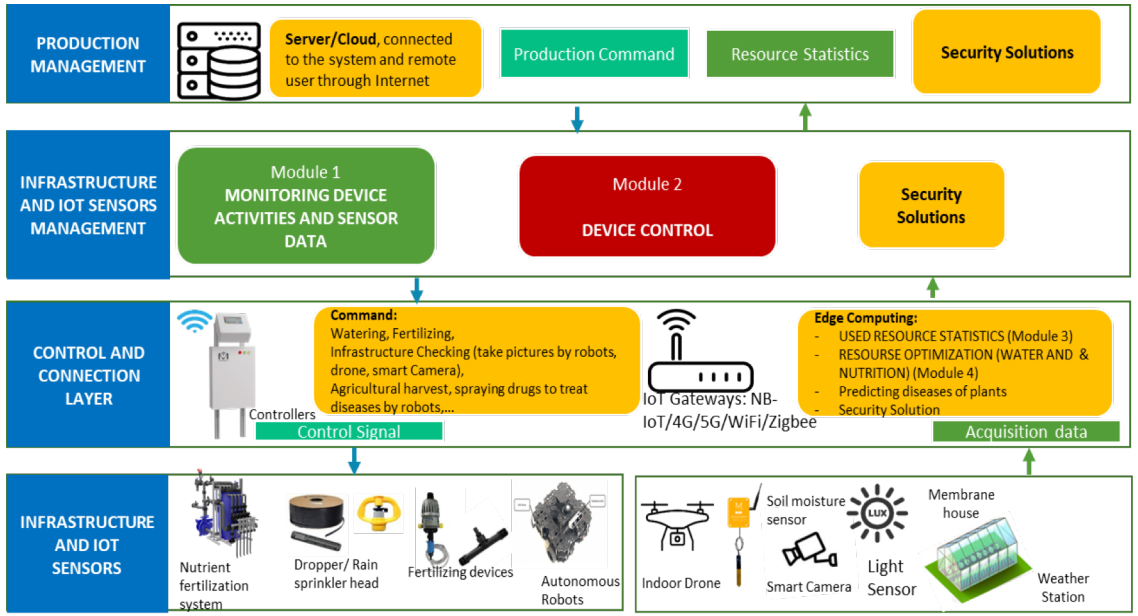


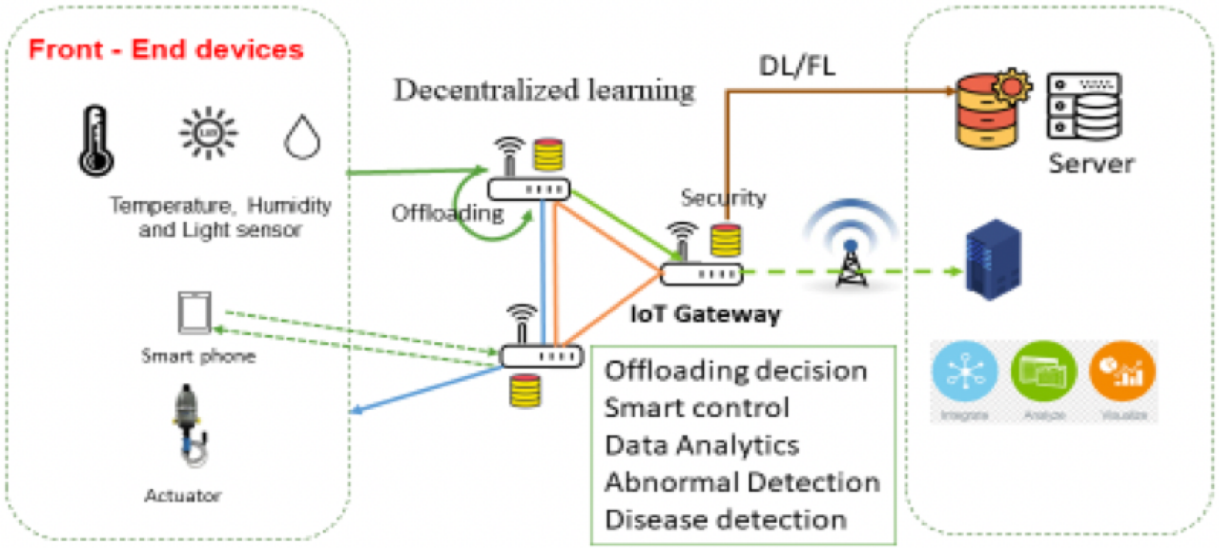
10. Agricultural IoT based on Edge Computing

- International collaboration project (ASEAN-IVO) funded by NICT, Japan

Contributions:

- Building an IoT-based smart agricultural system with intelligent edge computing capabilities
- Incorporating effective security measure in the system
- Leveraging the system automation with the employment of robot arms and drones





Opportunities

Research collaboration

Postdoctoral researchers, researchers, and research assistance

Student internship

Thank you for your attention

www.nectec.or.th
112, Phahonyothin Road, Khlong Nueng, Khlong Luang,
Pathumthani, Thailand 12120
Email: montida.pat@nectec.or.th