Project Title: A Hybrid Security Framework for IoT Networks

Project Report

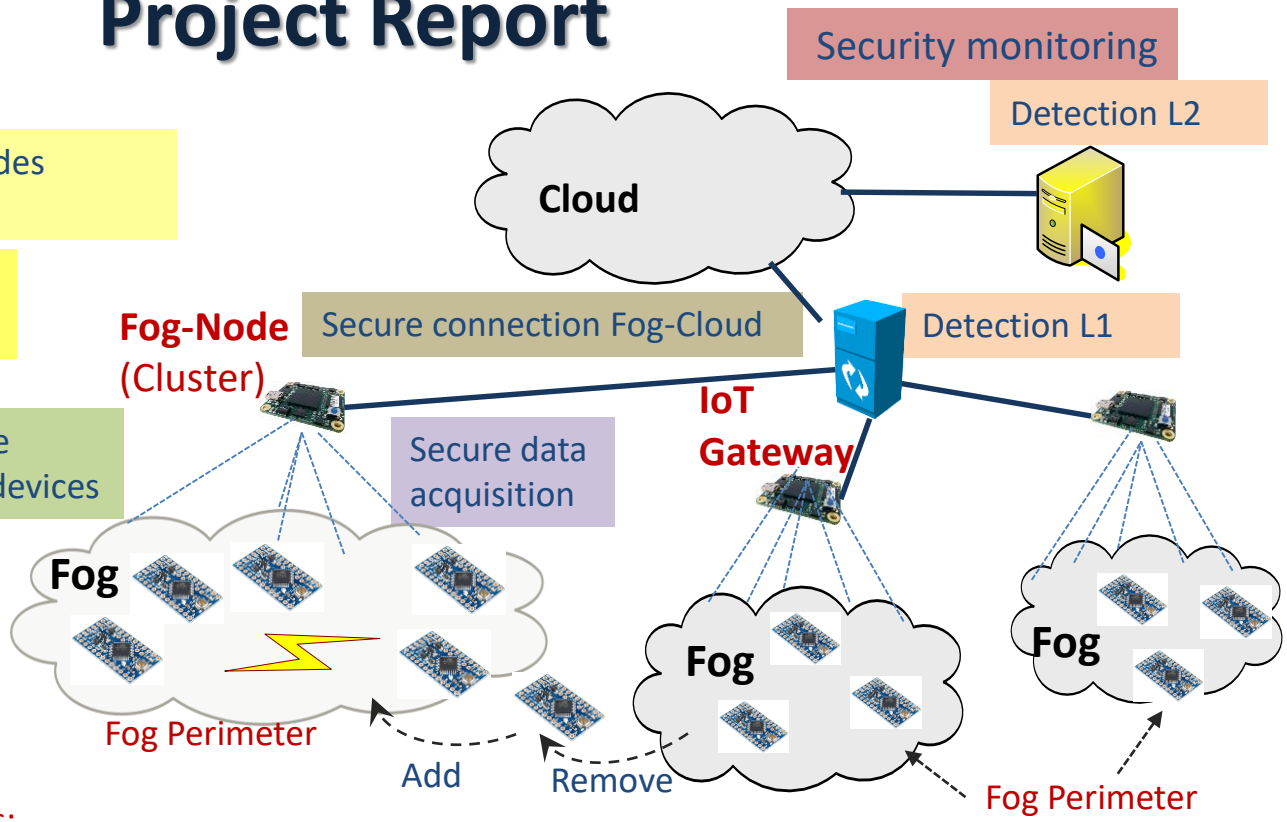
Background:

Different Security Levels of Fog-Nodes (protection priorities for fogs)

Identity, access control, authentication /watermark

Lightweight secure transmission bw. devices

- Scalable Perimeter for Fog (add, remove w. authentication)



Targets:

1. Research targets:
   - + Hybrid framework (fog architecture, level mapping, security level assignment)
   - + Lightweight secure data transmission / identity & authentication
   - + Monitoring, Detection, secure sharing
   - + Testbed for secure IoT data collection (air pollution data)
2. Research links / common paper publishing / exchanging & sharing experiences, knowledge
3. Contribution to technology/market development, promoting ASEAN IVO research

Speaker: Assoc. Prof. Dr. Dsc. Hoang Dang Hai

Project Title: A Hybrid Security Framework for IoT Networks

Project Members :

- **PTIT (Vietnam):** Assoc. Prof. DrSc. Hoang Dang Hai – Project Leader

  (others: Dr. Hoang Trong Minh, Dr. Vu Huu Tien, Hoang Manh Thang, Le Van Ngoc, Nguyen Tuan Lang)
- **NECTEC (Thailand):** Dr. Chalee

  (others: Ekkachan Ratteanalerdnusorn, Phitak Thaenkaew, Tinthid Jaikla)
- **MIMOS Bhd (Malaysia):** Dr. Choong (others: Dr. Kok, Chrishanton)
- **HUST (Vietnam):** Assoc. Prof. Dr. Ngo Quynh Thu
- **NUCE (Vietnam):** Dr. Pham Thieu Nga

  (others: Bui Thanh Phong, Nguyen Ha Duong, Le Thi Thuy Duong, Le Duc Quang, Tran Van Tho)
- **NICT Security Labs (Japan):** Dr. Takeshi Takahashi, Dr. Ryoichi Isawa, Dr. Daisuke Inoue
- **NES /NEC (Japan):** Dr. Tamoyuki Kuroda

Project Duration: from April 2017 to March 2020 (extended)

Project Activities (1):

Scientific & Technology Development:

- **Kick-off:** 25 July 2017
- **Organizing workshops, seminars**
  - Invited talk of Dr. Takeshi Takahashi (NICT cybersecurity labs)
  - Research presentations of members (PTIT, NICT, NECTEC, HUST, NUCE, MIMOS)
  - Internal meetings of each research team (1 for all, 1 of NECTEC/NICT, 1 of PTIT/NUCE/HUST, 1 of PTIT)
  - Meeting with NES / NEC (Dr. Tamoyuki Kuroda)
- **Doing research work of each team**
  - PTIT team works on: Modelling framework, IoT security survey, fog design, hierarchy architecture for monitoring, detection methods, honeynet, identification / authentication /watermark, data crawling, lightweight secure transmission, encryption, log collection & analysis
  - NECTEC team works on: NICTER/Daedalus, NETPIE platform, Monitoring & detection, access control, authentication schemes, smart application
  - NUCE team works on: IoT simulation, data analysis methods, secure data collection / transmission
  - HUST team works on: data transmission
  - MIMOS team works on: media gateway, secure presentation sharing
- **Conducting research results, common paper publishing**
- **Work on security report with NES / NEC, 01 report to NES/NEC**
- **Temporal reports to ASEAN IVO (3 reports)**

Project Activities (2):

Experiments including field testing:

- **Labs preparation & experiment using self existing equipment**
  - PTIT: Setup fog /cloud networks using virtual servers.
  - PTIT: Setup simulation tools (Contiki/Coja) for simulation of secure transmission, device authentication. Setup simulated honeynet (virtual machine with cowrie).
  - PTIT: Crawling data, analysis and detection using pre-built datasets
  - NECTEC: Setup NICTER/Daedalus, NETPIE platform for monitoring.
  - NECTEC: simulation using WIFI network, using IoT devices to study authentication
  - MIMOS: Setup existing media gateway, investigation of presentation sharing
  - NUCE: Simulation using Contiki/Coja, existing Waspmote sensors
- **Purchase of equipment, setting up labs at PTIT, NUCE. Experiments using equipment (since Dec.2018).**
  - PTIT: Setup test-labs, cloud/fogs using 3 servers, Arduino/Raspberry Pi boards
  - PTIT: Experiments with equipment: secure perimeter, secure transmission, etc.
  - NUCE: Setup test-labs, cloud/fogs using 2 servers, Arduino/Raspberry Pi boards
  - NUCE: Experiments with equipment: secure data collection / transmission, smart application (AirTracker).

Project Activities (3):

Other project activities:

- **Research exchange (2 of NECTEC at NICT, 1 of NUCE at NICT) on security monitoring, dataset building, etc.**
  - 3 NICT researchers visited NECTEC & install NICTER in Aug. 2017 (NICT budget).
  - 2 researchers of NECTEC visited NICT in Sept 2017 (NECTEC budget).
  - 1 researcher of NUCE joined training internship for one month at NICT in Japan, Oct. 2018 for learning dataset building, honeynet, data collection, data analysis (ASEAN IVO project budget).
- **Student projects**
  - Pollution detection machine using environmental sensors (NUCE student project – completed 8/2019)
  - Air Tracker (NUCE student project – completed 8/2019)
- **Master thesis**
  - Secure data transmission between IoT devices (01 PTIT master thesis – completed Jan. 2019)
  - Dynamic key exchange for identification and authentication in IoT Networks (01 PTIT master thesis – completed Jan. 2019)
  - Identity-based authentication for agents in network monitoring system (01 PTIT master thesis – will be completed in Dec. 2019)
- **PhD thesis**
  - Lightweight identification and authentication mechanism for IoT networks (01 PhD joined)

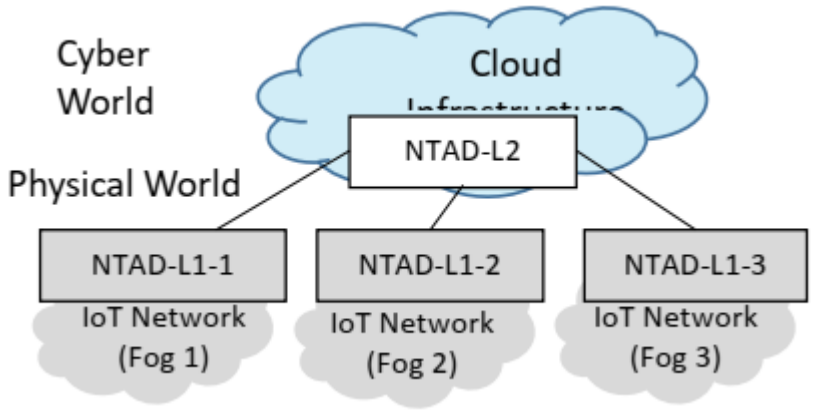
R&D results (1):

I. Scientific

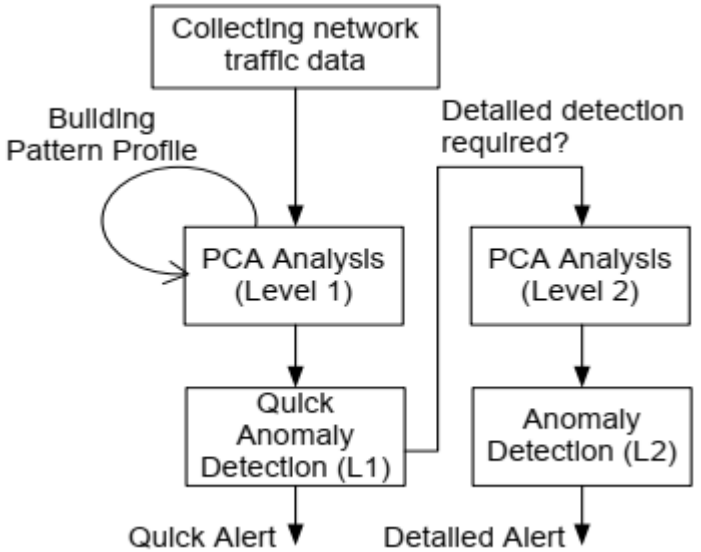
1) Secure fog architecture, IoT security framework:
   + Model for security level assignment using system theory, Markov chain with two state: Stable state (secure), Unstable state (vulnerable state, unsecure) == PTIT (1 paper).
   + Model for security level evaluation, weight assignment to 11 functional classes. Mapping mechanism for security levels == PTIT, NUCE (1 paper)
2) Secure data transmission:
   + Mechanisms for secure data transmission between IoT devices using encryption (secret, public key)
   == PTIT: 2 master theses.
3) Mechanisms for identity, watermarking, authentication:
   + Study of recent challenges and trends == NECTEC, PTIT (1 paper).
   + IoT device authentication using Brownian behavior, Role-based access control, Biometric authentication,
   == PTIT, NECTEC, NICT Security Labs: (6 papers).
4) Study and Building dataset: == PTIT, NUCE (setup cowrie honeynet testbed)
5) Method for monitoring with NETPIE platform:
   == NECTEC, NICT Security Labs: (2 papers).
6) Method for data aggregation, analysis, secure sharing of data:
   + Secure data sharing using media gateway: == MIMOS (1 paper).
   + Data aggregation, analysis using sensors, secure sharing.
   == PTIT, NUCE: (1 paper, 2 student projects).
7) Mechanism for quick attack detection, monitoring using 2 levels, network dimensioning:
   == PTIT, NUCE: (3 papers).

R&D results (2):

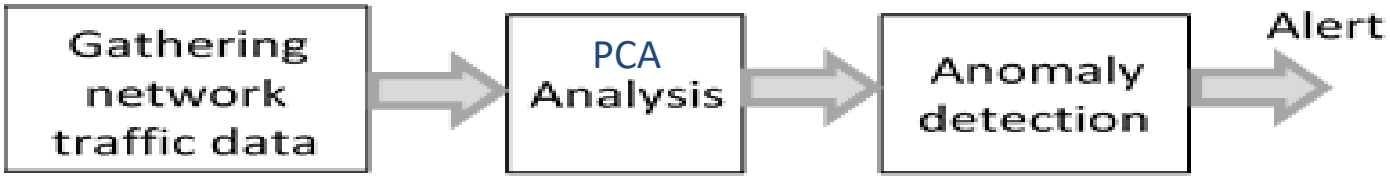
Security monitoring: Two Level detection



NTAD = Network Traffic Anomaly Detection



Detection model: Detection at 2 levels



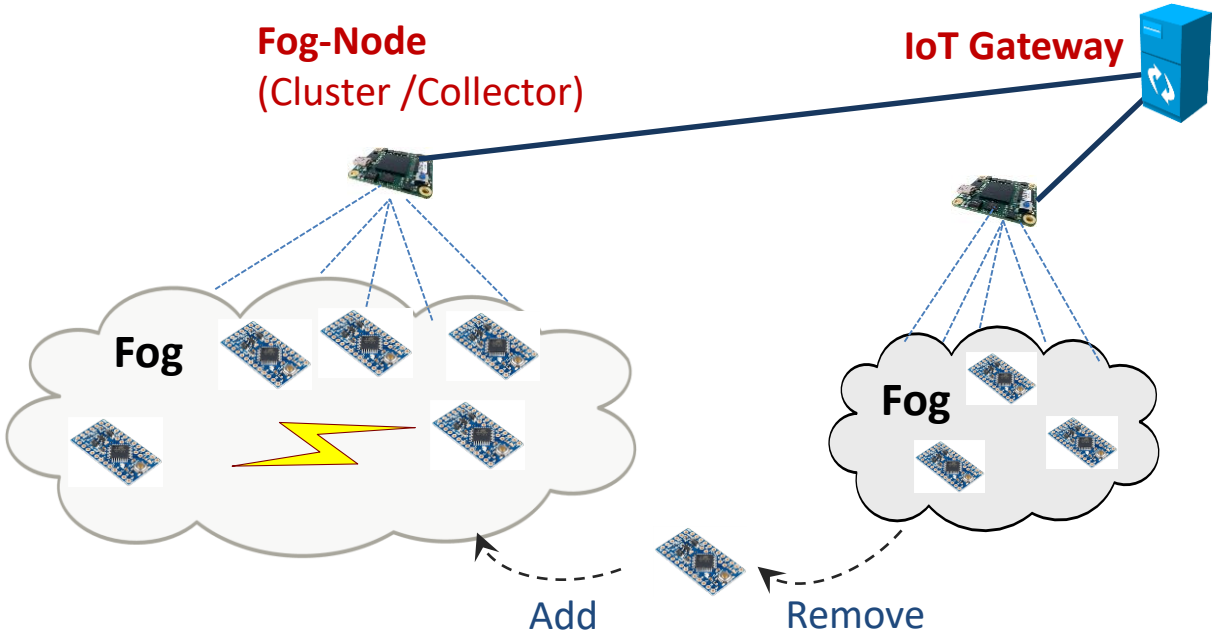
$$d = \sum_{i=r}^{q} w_i \left| y_i \right|^c$$

Attack Detection: $(d_1 = \sum_{i=1}^{m} w_i \left| y_i \right|^c > d_{N1})$ OR $(d_2 = \sum_{i=r}^{p} w_i \left| y_i \right|^c > d_{N2})$

R&D results (3):

IoT device identity management and authentication

- Device identity using MAC - ID
- Watermark data for Fog is formed for recent added nodes into Fog
- Fog-Node check authentication for IoT devices to send the collected data to the IoT gateway
- Access control to IoT devices controlled by IoT gateway using network watermark



R&D results (4):

II. Technology Development

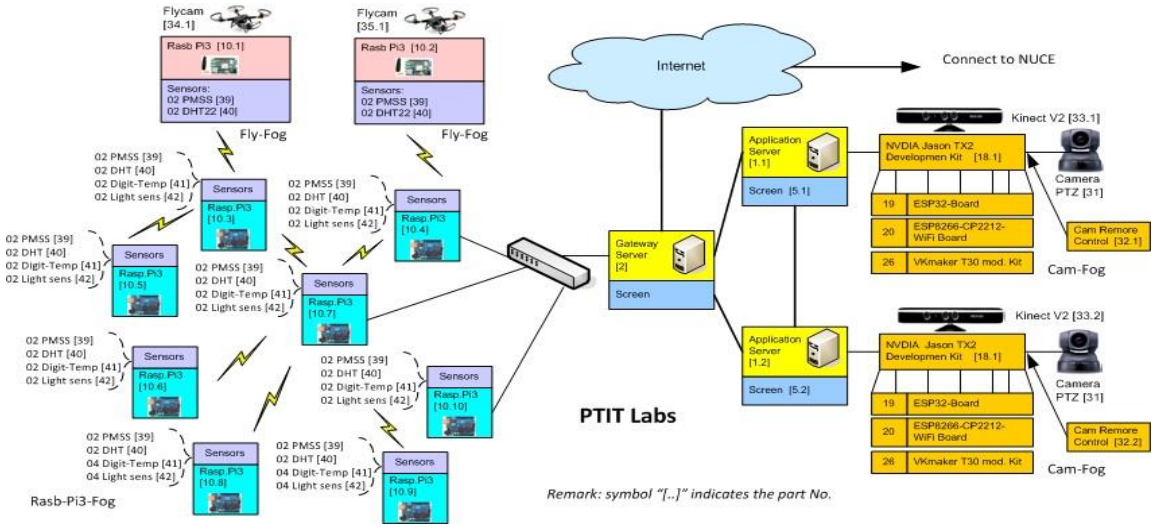
1) Method for security level assessment using ISO 15408 and fuzzy logic.
   == PTIT, NUCE
2) Method for IoT Device identification using MAC addresses, Brownian motion behavior
   == PTIT
3) Method for IoT device authentication using watermarking, Biometric, access control.
   == NECTEC, NICT Security Labs, PTIT
4) Method for device authentication using encryption.
   == PTIT
5) Method for secure sharing of presentation data
   == MIMOS
6) Method for lightweight secure data transmission between IoT devices
   == PTIT
7) Application for AirTracker using environmental sensors
   == NUCE
8) Application for controlling environmental robots
   == NUCE

R&D results (5):

III. Experiments including field testing

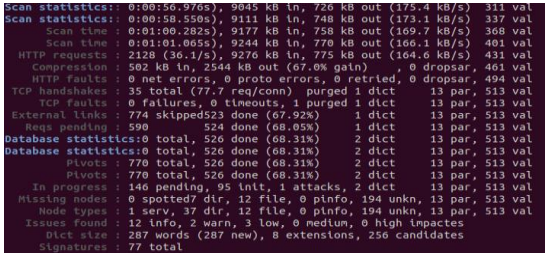
At PTIT

Diagram of Labs

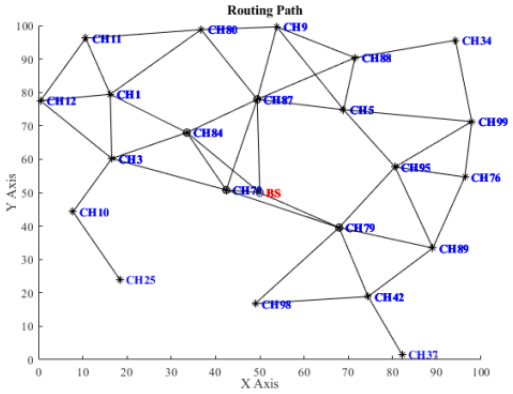


Test labs

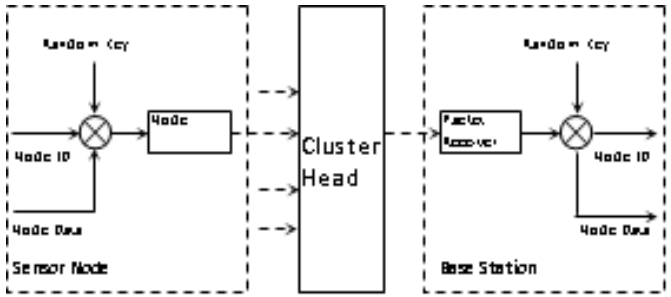
Crawling data



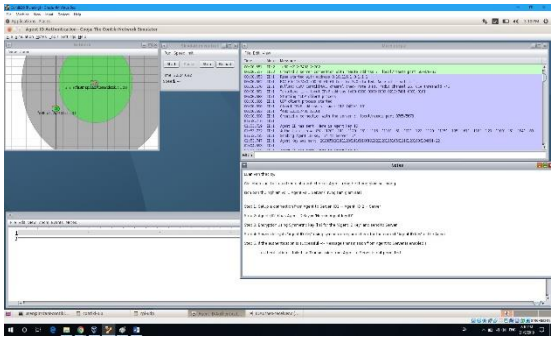
Routing path for multi-hops



Watermark block diagram



Test for secure transmission

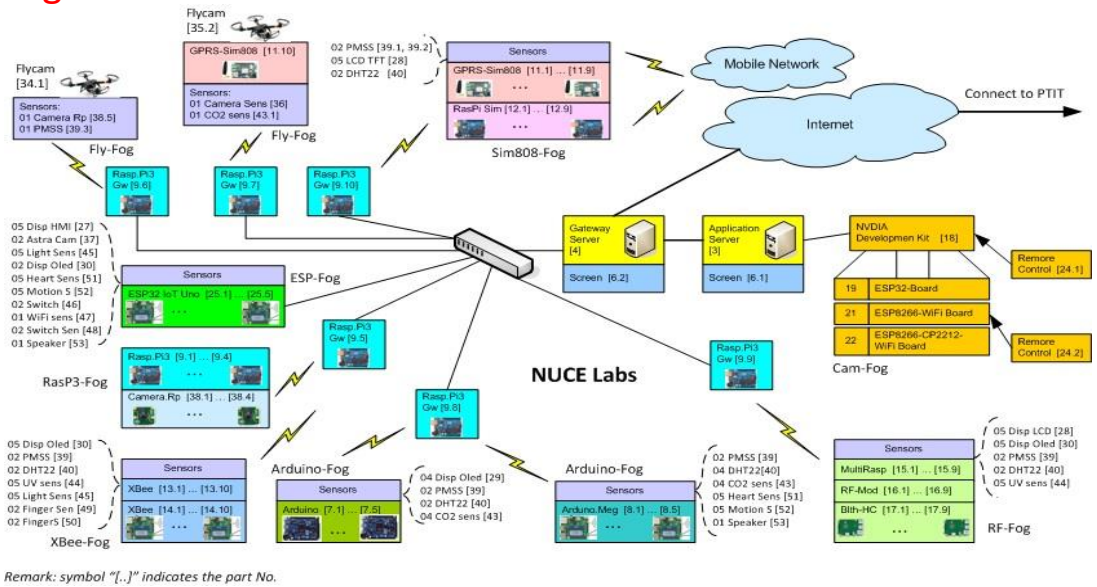


R&D results (6):

III. Experiments including field testing

At NUCE

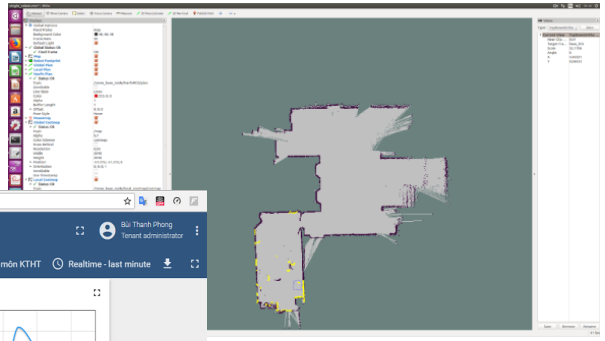
Diagram of Labs



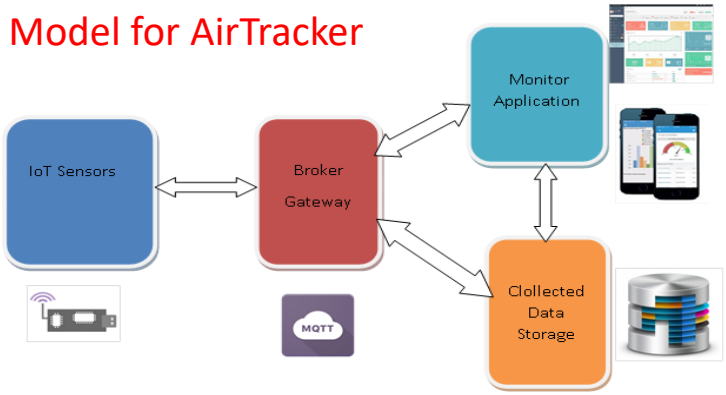
Remark: symbol "[..]" indicates the part No.

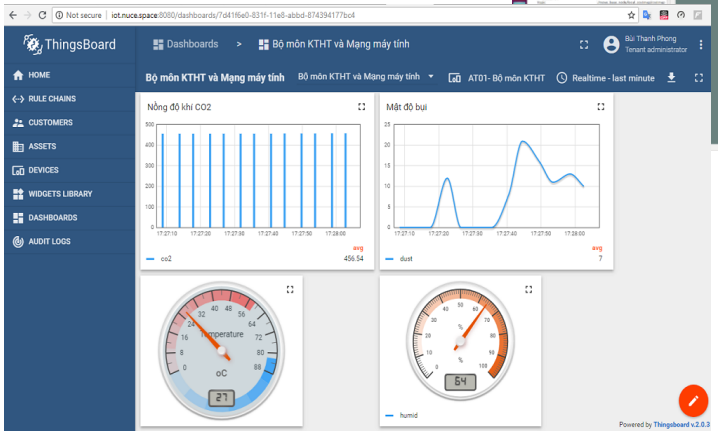
Sensors for air pollution

Web output



Model for AirTracker





Scientific Contribution (1):

Presentations at International Conferences: 14

No	Paper title:	Author names	Affiliation	Conference name	Date of conference	The venue of the conference
1	A Model for security assessment	HD.Hai, NX.Quang, HT.Thu	PTIT	Security Workshop 2017	Nov. 2017	Uni. Of Crypto Technology, VN
2	A Study on the sensor network authentication by utilizing a Brownian motion behavior	HT.Minh, HD.Hai, et.al.	PTIT	IEEE ICTC 2017	Oct. 2017	Jeju, Korea
3	Recent challenges, trends and concerns related to IoT Security	Chalee V., HD.Hai, et.al.	NECTEC, PTIT	IEEE ICACT 2018. Best paper	Feb.2018	Busan, Korea
4	A PCA-based method for IoT network traffic anomaly detection	HD.Hai, NH. Duong	PTIT, NUCE	IEEE ICACT 2018. Best paper	Feb.2018	Busan, Korea
5	Usable and secure cloud-based biometric authentication solution for IoT devices	Chalee V., Takeshi T., et.al.	NECTEC, NICT	IEEE ISCC 2018	June 2018	Rio de Janero, Brasilien
6	Automated wireless presentation system with facial images	Choong KN., et.al.	MIMOS	IEEE I2CACIS 2018	Oct. 2018	Shah Al. Malaysia
7	Evaluating the security levels of the web-portals based on the standard ISO/IEC 15408	HD.Hai, PT.Nga	PTIT, NUCE	IEEE SoICT 2018	Dec.2018	Danang, Vietnam
8	A novel fuzzy inference system based on hedge algebras to enhance energy efficiency in wireless sensor networks	HT. Minh, et.al.	PTIT	IEEE ICCIS 2018	Dec. 2018	Singapore

Scientific Contribution (2):

Presentations at International Conferences: (cont')

No	Paper title:	Author names	Affiliation	Conference name	Date of conference	The venue of the conference
9	Security implementation for authentication in IoT environments	Chalee V., et.al.	NECTEC	IEEE ICCCS 2019	Feb. 2019	NTU, Singapore
10	Hybrid security framework for IoT networks (Invited talk)	HD. Hai	PTIT	ASEAN IVO workshop on Cybersecurity in Industry 4.0	Mar. 2019	VNU-UET, Hanoi
11	A Secure network architecture for heterogeneous IoT devices using role-based access control	Chalee V., HD.Hai, et.al.	NECTEC, PTIT	IEEE SOFTCOM 2019	Sept. 2019	Split, Croatia
12	A hedge algebras based fuzzy inference system for clustering in multi-hop WSNs (accepted)	HT. Minh, et.al.	PTIT	IEEE CSAI 2019	Dec.2019	Beijing, China
13	Toward automated cybersecurity: visualization and machine learning techniques (Invited talk)	Takeshi Takahashi	NICT	IEEE NICS 2019	Dec.2019	Hanoi, Vietnam
14	A lightweight mixed secure scheme based on the watermarking technique for hierarchy wireless sensor networks (accepted)	HT. Minh, et.al.	PTIT	ICOIN 2020	Jan. 2020	Spain

Scientific Contribution (3):

Published Journal Papers: 3

No	Paper title:	Author names	Affiliation	Journal Name	Publisher	Vol.No., pages
1	Security monitoring of IoT networks	HD. Hai	PTIT	S&T Information & Communications	PTIT	01(CS.01) 2018, p3-9
2	Detecting anomalous network traffic in IoT networks	HD. Hai, NH. Duong	PTIT, NUCE	Transaction on Advanced Comm. Technology (TACT)	GiRI Global IT Research Institute	Vol.7, Issue 5, p1143-1152
3	A secure authentication scheme based on Brownian motion in hierarchy wireless sensor networks	HT. Minh, HD. Hai. et.al.	PTIT	EAI endorsed Trans. on Industrial NW & Intelligent systems	EAI.EU	19(21):e1, 2019, p1-9

Societal Impact:

1) Providing method for lightweight secure transmission for IoT devices

2) Providing method for anomaly detection, attack detection

3) Providing method for IoT Device identification using MAC addresses, Brownian motion behavior

4) Providing an application for AirTracker using environmental sensors

Conclusion:

Key findings:

1) Hybrid framework =
   security level assignment + hierarchy monitoring & detection + secure transmission + identity / authentication of IoT devices
2) Security level assessment & evaluation using fuzzy logic
3) Access control using role-based
4) Hierarchy monitoring & detection for quick detection using PCA, security level assignment
5) Secure data collection = only collect from identified & authenticated IoT devices
6) Secure transmission = lightweight protocol (tiny encryption using secret & public key)
7) Identity / Authentication for IoT devices using MAC address, Brownian motion behavior, watermarking, biometric
8) Application for AirTracker using environmental sensors
9) Application for data crawler

Future works:

1) Further experiments with test labs on:
   + Security level assessment & evaluation using fuzzy logic
   + Hierarchy monitoring & detection for quick detection using PCA, security level assignment
   + Secure data collection & transmission
   + Identification / authentication
   + Application for smart city development (air pollution monitoring, smart home)
   + Preparation and processing collected data

2) Further common publication

3) Final project meeting

4) Final project report

Thank you !

Acknowledgement:
The project team thanks NICT and ASEAN IVO for all supports to this project!