**[PROJECT TITLE: Artificial Intelligence Powered Comprehensive Cyber-Security for Smart Healthcare Systems (AIPOSH)]**

**[OPEN WORKSHOP: Intelligent Embedded Security for Internet of Things Systems]**

**Report Form**

**I. Organizer:**

|  |  |
| --- | --- |
| Name: | Hoang Van Phuc |
| Position: | Associate Professor |
| Institution: | Le Quy Don Technical University, Hanoi, Vietnam |

**II. Program:**

Date: 22-24, July 2024

Venue: Convention Hall, Nanyang Technological University, Singapore.

Address: 50 Nanyang Avenue, Singapore 639798

**Program Agenda:**

|  |  |  |
| --- | --- | --- |
| **Date** | **July 22nd, 2024** |  |
| **Time** | **Agenda** | **Speaker** |
| 9:30 AM | Welcoming | Prof. Gwee Bah Hwee, NTU |
| 9:40 AM | Introduction of research and education in cyber-security and information security at LQDTU | Mr. Tran Van Thuong, Vice President of LQDTU |
| 10:00 AM | Approach toward a platform for comprehensive IoT cyber-security solutions in ASEAN | Prof. Hoang Van Phuc, LQDTU |
| 10:30 AM | **Tea break** |  |
| 10:45 AM | Keynote 1: Physical Security Evaluation for IoT Devices | Prof. Gwee Bah Hwee, NTU |
| 12:00 PM | Lunch |  |
| 1:30 PM | Keynote 2: Security Evaluation for IoT Devices in Smart Healthcare Systems | Dr. Keisuke Furumoto (NICT, Japan) |
| 2:30 PM | A System-Level Approach for Poisoning Prevention in Edge Data Collection | Norrathep Rattanavipanon (PSU, Thailand) |
| 3:30 PM | **Tea break** |  |
| 4:00 PM | NTU Lab and Security Center tour |  |
| **Date** | **July 23rd, 2024** |  |
| **Time** | **Agenda** | **Speaker** |
| 9:30 AM | Keynote 3: Intellectual Property Protection of Deep Neural Networks | Prof. Chang Chip Hong (NTU & IEEE Fellow) |
| 10:30 AM | Advanced Internet of Things (IoT) in Industry | Dr. Le Van Duc (NTU, Singapore) |
| 10:15 AM | **Tea break** |  |
| 10:30 AM | Keynote 4: A deep learning approach to IoT network intrusion detection | Prof. Tran Nguyen Ngoc (National Lab for Security, Vietnam) |
| 11:15 AM | Invited talk: Leaking AI: A Look into Physical Attacks on EdgeML Devices | Dr. Shivam Bhasin (NTU) |
| 12:00 PM | **Lunch** |  |
| 1:30 PM | Improving Security in RISC-V Based IoT Systems | Prof. Hoang Van Phuc (LQDTU, Vietnam) |
| 2:30 PM | Keynote 5: Advanced side channel analysis methods | Prof. Kazuo Sakiyama (UEC, Japan) |
| 3:15 PM | **Tea break** |  |
| 3:45 PM | Energy Efficient Power Management IC for Edge IoT Devices | Dr. Nguyen Van Trung (LQDTU, Vietnam) |
| 4:45 PM | Keynote 6: Low power, secure signal processor for medical applications | Dr. Le Duc Hung (VNU, Vietnam) |
| **Date** | **June 24th, 2024** |  |
| **Time** | **Agenda** | **Speaker** |
| 9:30 AM | Hardware Trojan Detection Using Machine Learning for IoT Systems | Prof. Hoang Van Phuc (LQDTU, Vietnam) |
| 10:15 AM | MAppGraph: Mobile-App Classification on Encrypted Network Traffic using Deep Graph Convolution Neural Networks | Prof. Tram Truong Huu, (Singapore Institute of Technology) |
| 11:00 AM | **Tea break** |  |
| 11:15 AM | Green IC Design for IoT Edge Devices | Ms. Hoang Hong Hanh (NUS, Singapore) |
| 12:00 PM | **Lunch** |  |
| 1:30 PM | Training on Physical Security Evaluation for IoT Devices | Prof. Gwee Bah Hwee, NTU |
| 3:30 PM | **Tea break** |  |
| 4:00 PM | Panel discussion and follow-up plan | Chair: Prof. Hoang Van Phuc, LQDTU |
| 5:00 PM | Closing | Prof. Gwee Bah Hwee, NTU |

**III. Participants:**

|  |  |  |  |
| --- | --- | --- | --- |
| **No.** | **Name** | **Organization** | **Itinerary** |
| 1 | Van Phuc Hoang | LQDTU | 21-25, July 2024 |
| 2 | Nguyen Van Trung | LQDTU | 21-25, July 2024 |
| 3 | Tran Van Thuong | LQDTU | 21-25, July 2024 |
| 4 | Keisuke Furumoto | NICT | 21-25, July 2024 |
| 5 | Bah Hwee Gwee | NTU | 21-25, July 2024 |
| 6 | Norrathep Rattanavipanon | PSU | 21-25, July 2024 |
| 7 | Tran Nguyen Ngoc | National Lab for Security, Vietnam | 21-25, July 2024 |
| 8 | Le Duc Hung | VNU, Vietnam | 21-25, July 2024 |
| 9 | Le Van Duc | NTU | 21-25, July 2024 |
| 10 | Massimo Alioto | NUS | 21-25, July 2024 |
| 11 | Hoang Hong Hanh | NUS | 21-25, July 2024 |
| 12 | Kazuo Sakiyama | UEC | 21-25, July 2024 |
| 13 | Shivam Bhasin | NTU | 21-25, July 2024 |
| 14 | Cheah Jun Wei Jason | NTU | 21-25, July 2024 |
| 15 | Liang Zhenkai | NUS | 21-25, July 2024 |
| 16 | Arun Dasse Aroquiadasse | NUS | 21-25, July 2024 |
| 17 | Liu Yuancheng | NUS | 21-25, July 2024 |
| 18 | Seah Choon Meng | NUS | 21-25, July 2024 |
| 19 | Yvonne Goh Ai Qin | Secure-IC SAS, Singapore | 21-25, July 2024 |
| 20 | Chang Chip Hong | NTU | 21-25, July 2024 |
| 21 | Kwen Siong Chong | Async2Secure Pte. Ltd.,  Singapore | 21-25, July 2024 |
| 22 | Kohei Masumi | NICT | 21-25, July 2024 |
| 23 | Do Anh Tuan | A\*STAR, Singapore | 21-25, July 2024 |
| 24 | Jakapan Suaboot | PSU | 21-25, July 2024 |
| 25 | Warodom Werapun | PSU | 21-25, July 2024 |

Total: 25 people at the venue

**IV. Summary of the activities corresponding to the objectives.**

1. Objective

The main objective of this workshop is to provide a forum for exchange of ideas and latest research results in advanced cyber-security techniques and solutions for IoT-based smart healthcare systems, especially the intelligent embedded security solutions. The workshop is necessary for this project in gathering leading experts in different fields to solve the issues of providing an intelligent embedded cyber-security platform for IoT based smart healthcare systems in ASEAN region. The workshop aims to provide the overall solutions and an efficient roadmap for this project implementation. It should be taken place in Nanyang Technological University (NTU), Singapore due to several reasons. Firstly, as the leading country in high technologies and education, Singapore has leading experts in different fields of IoT systems which are also main topics of our project and famous universities. NTU is a leading university in the world, esspecially in the field of this workshop. Secondly, it is convenient to gather leading experts from leading universities in Singapore (NTU, NUS, SIT) without budget from IVO project thank to its convenient travel. Also, some local companies in Singapore are willing to join the workshop. Moreover, experts from Japan will have invited/keynote talks in this workshop without budget from the project. Speakers are leading experts in the field. The first keynote talk presents the advances and implementation of physical security evaluation for IoT devices which can be used for IoT based smart healthcare systems in this project. In the keynote 2, the methods of security evaluation for IoT devices in smart healthcare systems have been investigated to point out the security threats and solutions for IoT based smart healthcare systems. Keynote 3 mentioned the intellectual property protection of deep neural networks which will be useful for this project. Keynote 4 presented the solutions and methods of the deep learning approach to IoT network intrusion detection. Keynote 5 presented the advanced side channel analysis methods. Moreover, in the keynote 6, author presented low power, secure signal processor for medical applications including smart healthcare systems. The inviteted talk from a leading researcher in Singapore also delivered the emerging topics in the field of secure intelligent edge computing for IoT systems. Especially, the short training physical security evaluation for IoT devices will give detailed guidelines for participants in performing security evaluation in this project.

2. Activities corresponding to the objectives

1. Review the progress of project:

* Prof. Gwee Bah Hwee (NTU) gives welcome message of the workshop.
* Mr. Tran Van Thuong (Senior Vice President of LQDTU) gives opening remarks of the workshop and introduction of research and education in cyber-security and information security at LQDTU.
* Prof. Hoang Van Phuc presents the project achievement and the approach toward a platform for comprehensive IoT cyber-security solutions in ASEAN.

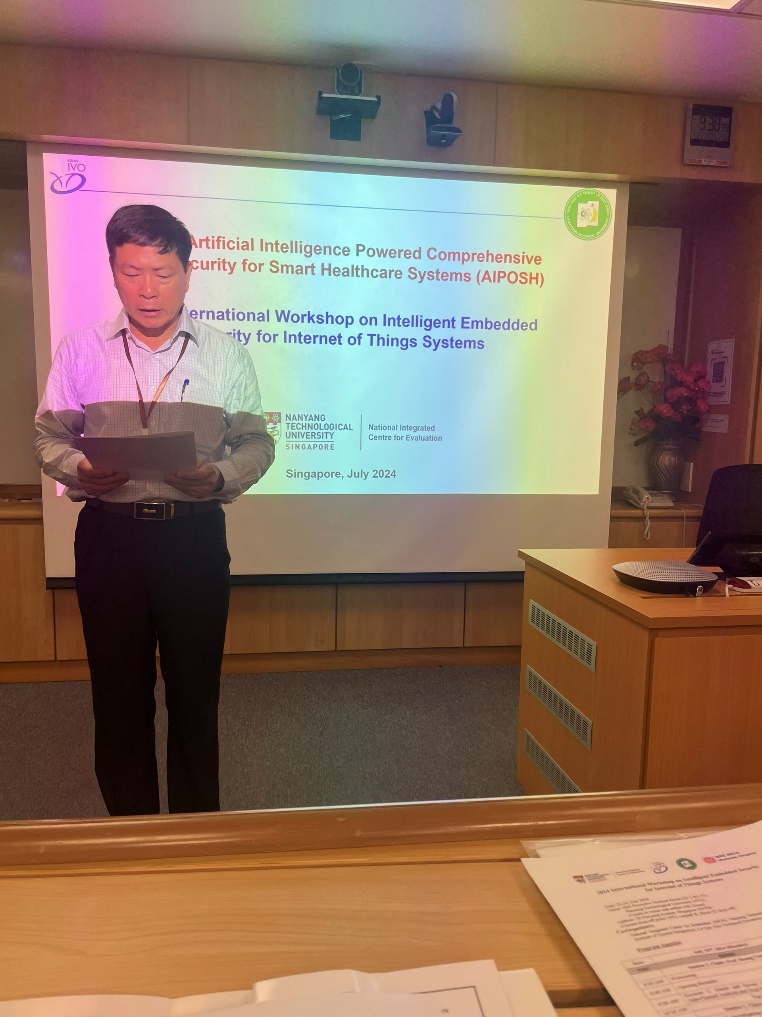
1. Present, discuss the latest research results in intelligent embedded security solutions for Internet of Things systems, and conclusions:

* Prof. Gwee Bah Hwee presents the keynote talk on physical security evaluation for IoT devices with the focus on Attack and Secure of Crypto Chip based on Side-Channel Analysis and Dual-Hiding Countermeasures.
* Dr. Keisuke Furumoto gives a keynote talk on Security Evaluation for IoT Devices in Smart Healthcare Systems. Moreover, Mr. Kohei Masumi (NICT, Japan) presents the NICT darknet analysis results.
* Prof. Norrathep Rattanavipanon talks about A System-Level Approach for Poisoning Prevention in Edge Data Collection.
* Prof. Chang Chip Hong gives a keynote talk on Intellectual Property Protection of Deep Neural Networks.
* Dr. Le Van Duc gives a talk on Advanced Internet of Things (IoT) in Industry.
* Prof. Tran Nguyen Ngoc delivers a keynote talk on a deep learning approach to IoT network intrusion detection.
* Dr. Shivam Bhasin presents an invited talk on Leaking AI: A Look into Physical Attacks on EdgeML Devices
* Prof. Hoang Van Phuc presents about Improving Security in RISC-V Based IoT Systems.
* Prof. Kazuo Sakiyama delivers a keynote talk on Advanced side channel analysis methods.
* Dr. Nguyen Van Trung presents Energy Efficient Power Management IC for Edge IoT Devices.
* Dr. Le Duc Hung delivers a keynote talk on Low power, secure signal processor for medical applications.
* Prof. Hoang Van Phuc presents about Hardware Trojan Detection Using Machine Learning for IoT Systems.
* Prof. Tram Truong Huu presents on MappGraph - Mobile-App Classification on Encrypted Network Traffic using Deep Graph Convolution Neural Networks.
* Ms. Hoang Hong Hanh presents about Green IC Design for IoT Edge Devices.
* Prof. Gwee Bah Hwee chairs the session of NiCE and Hardware Security Project Visit as well as Training on Physical Security Evaluation for IoT Devices.
* Prof. Hoang Van Phuc chairs the discussions, gives follow-up plan for the project and closing remarks. In conclusion, the project has achieved remarkable results with qualified published papers and scientific exchange activities. For the follow-up plan, the project team will add new members, publish more papers, perform the site experiments, prototype system development and prepare the new proposals after this project.

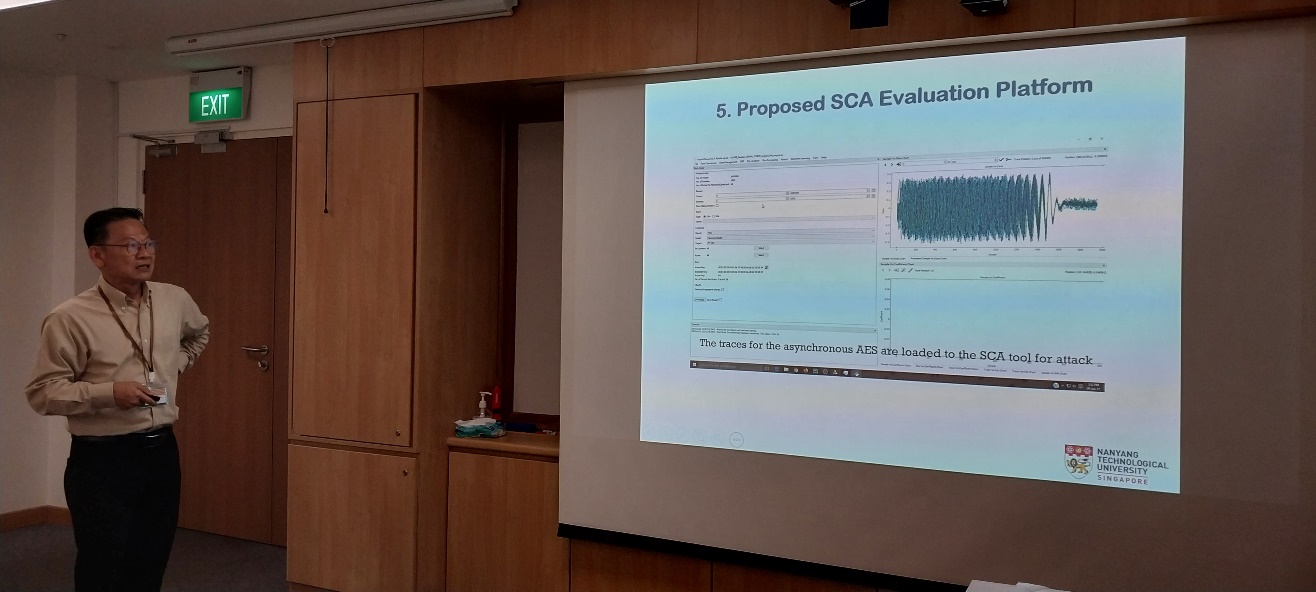
3. Detailed changes from the initial proposal: In general, the main workshop content is unchanged. We only change three speakers and the order of presentations for the convenience of speakers.

**V. Others**

The workshop related pictures as below:



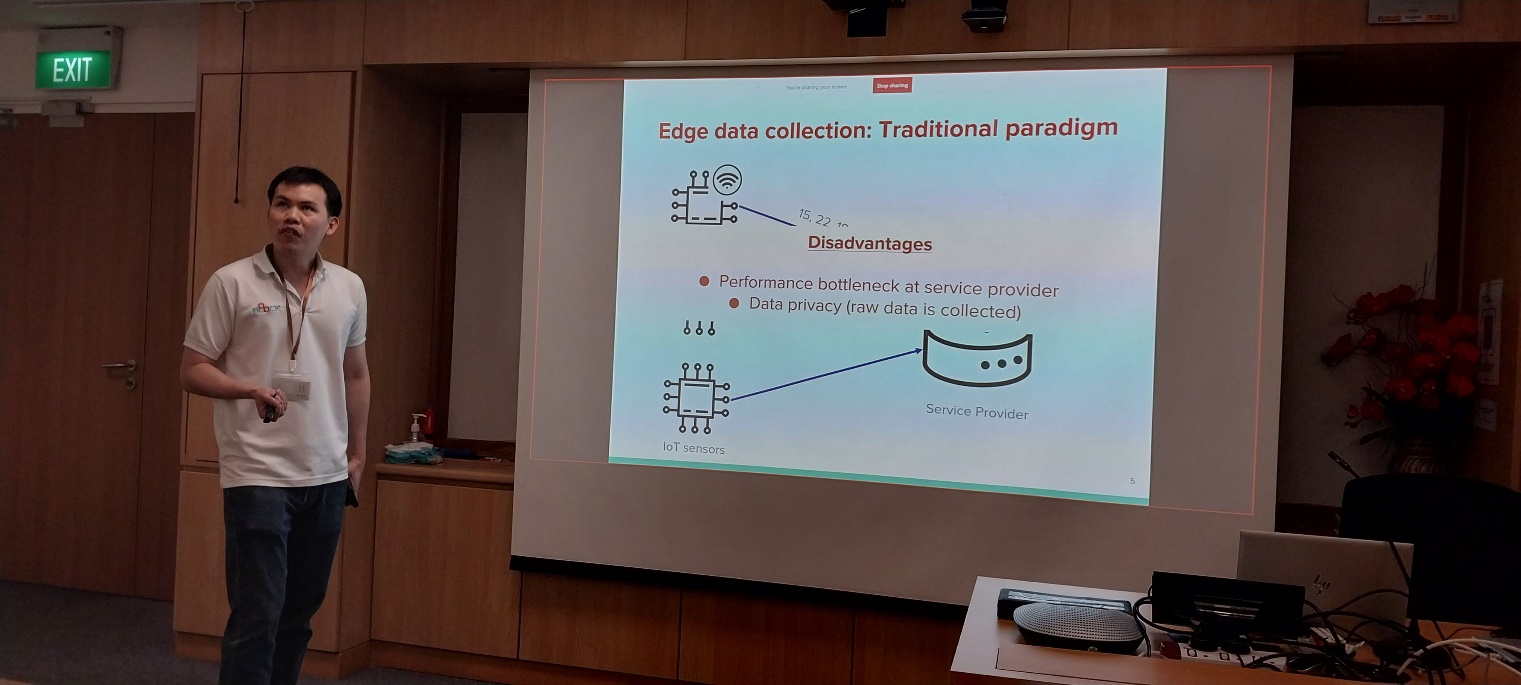
Mr. Tran Van Thuong (Senior Vice President of LQDTU) gives opening remarks of the workshop and introduction of research and education in cyber-security and information security at LQDTU.



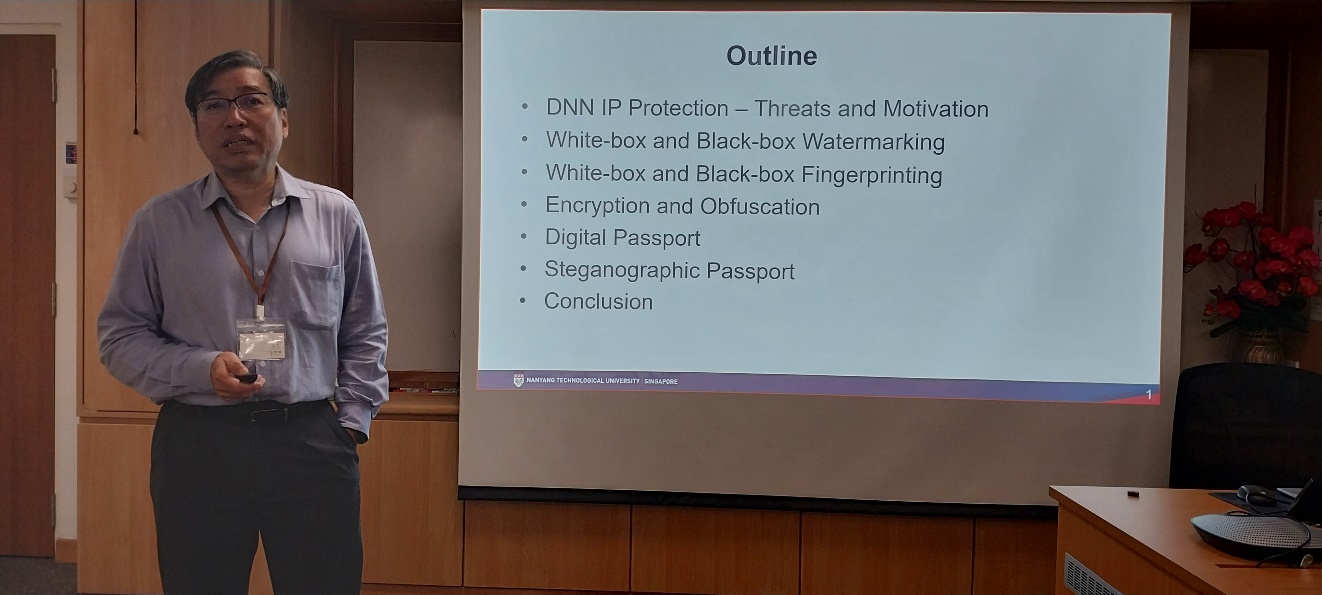
Prof. Gwee Bah Hwee presents the keynote talk on physical security evaluation for IoT devices.



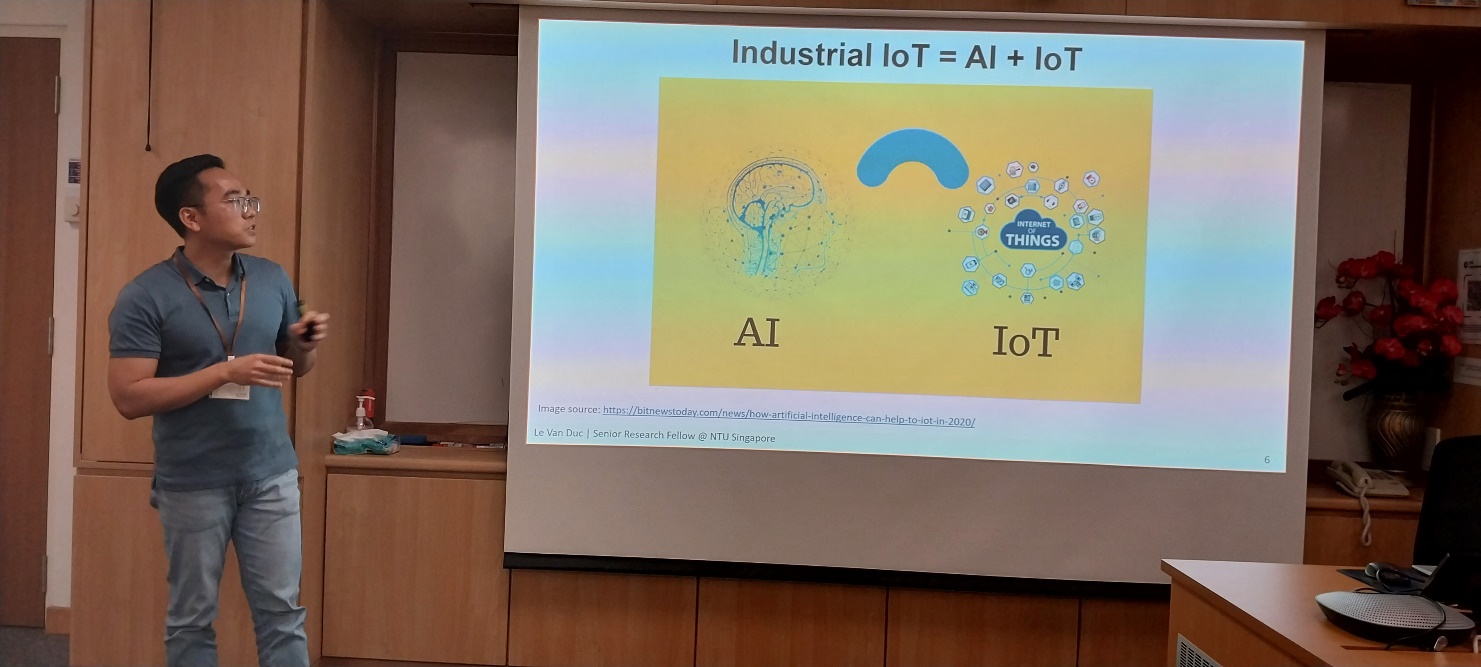
Dr. Keisuke Furumoto gives a keynote talk on Security Evaluation for IoT Devices in Smart Healthcare Systems



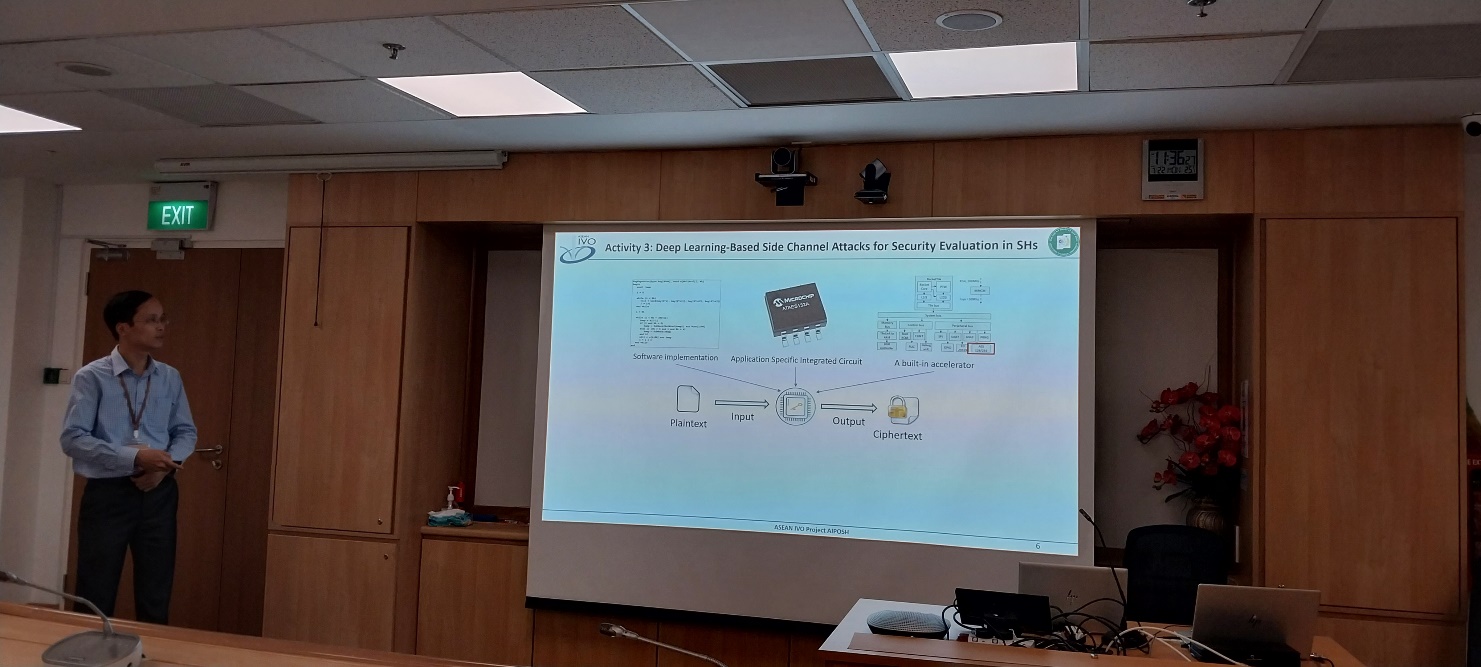
Prof. Norrathep Rattanavipanon talks about A System-Level Approach for Poisoning Prevention in Edge Data Collection



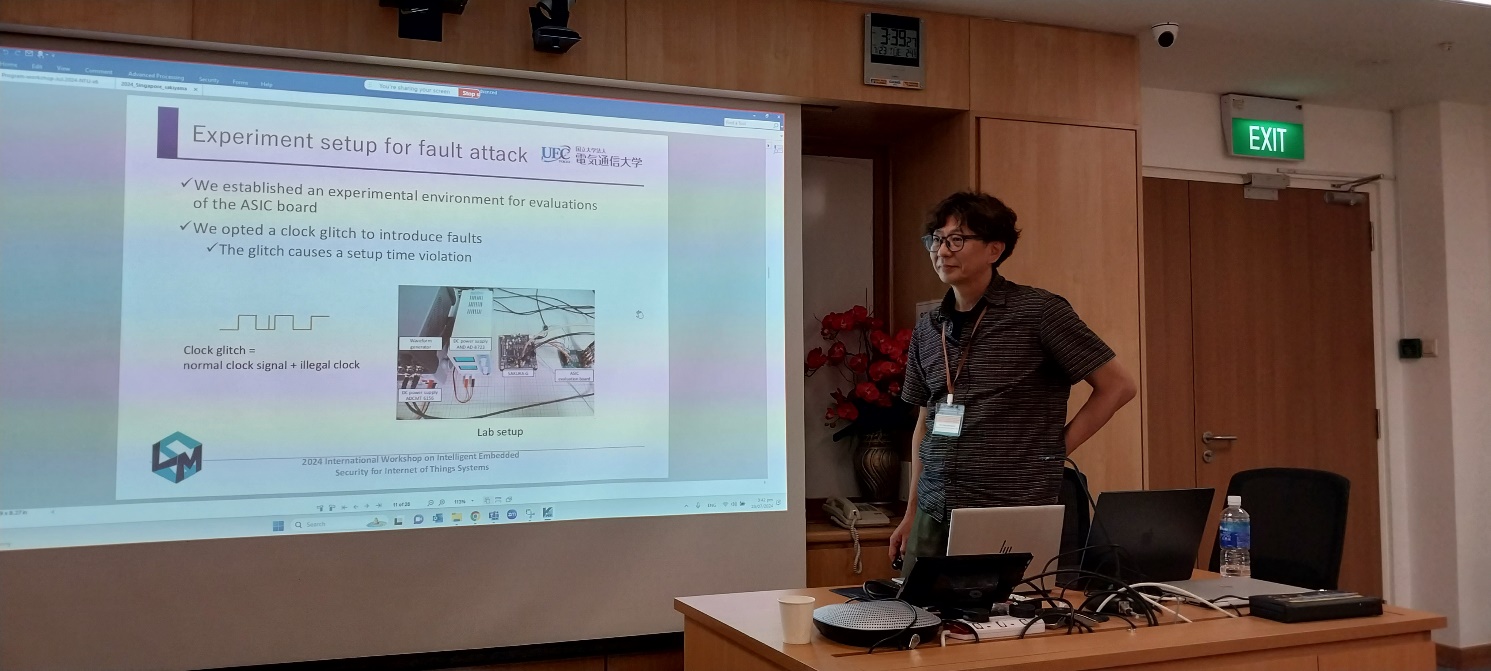
Prof. Chang Chip Hong (NTU & IEEE Fellow) gives a keynote talk on Intellectual Property Protection of Deep Neural Networks



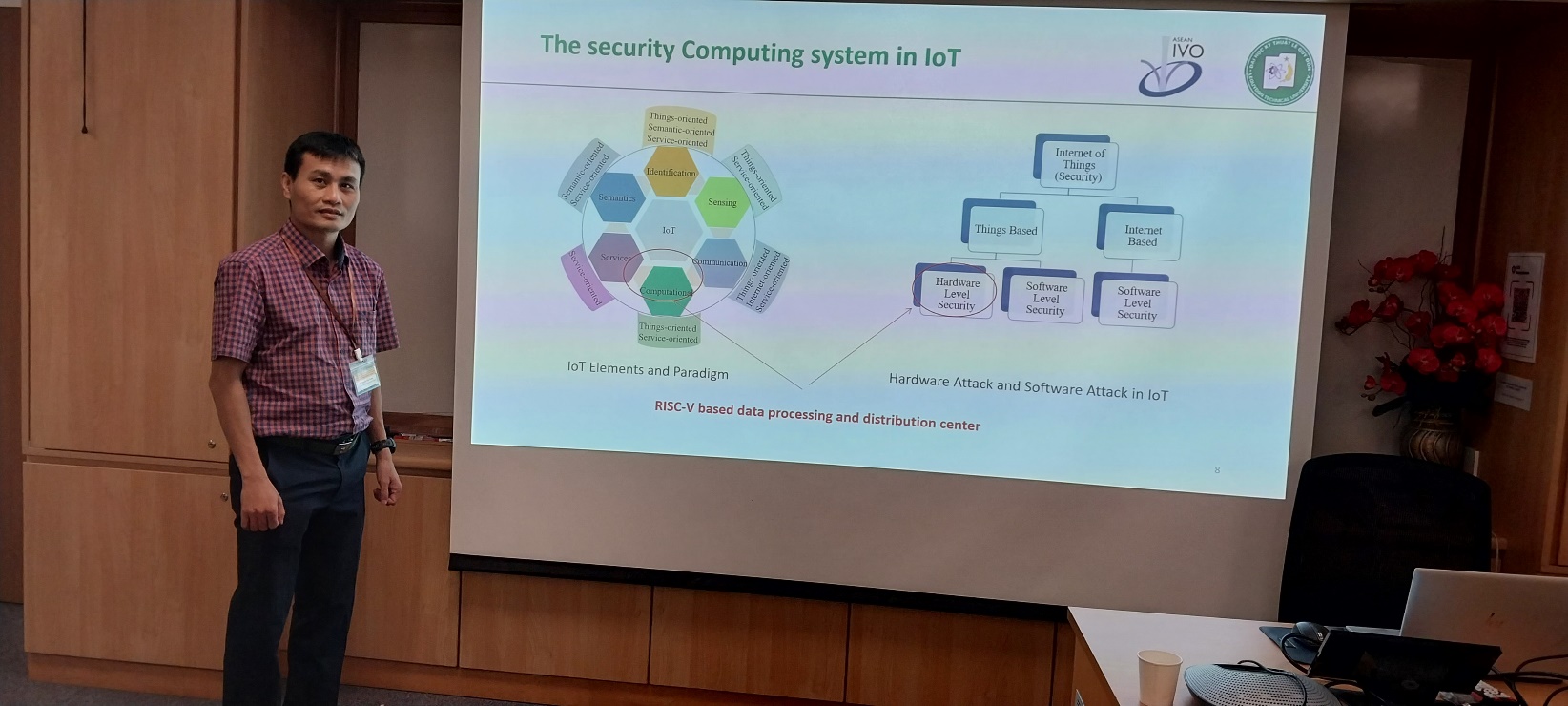
Dr. Le Van Duc gives a talk on Advanced Internet of Things (IoT) in Industry.



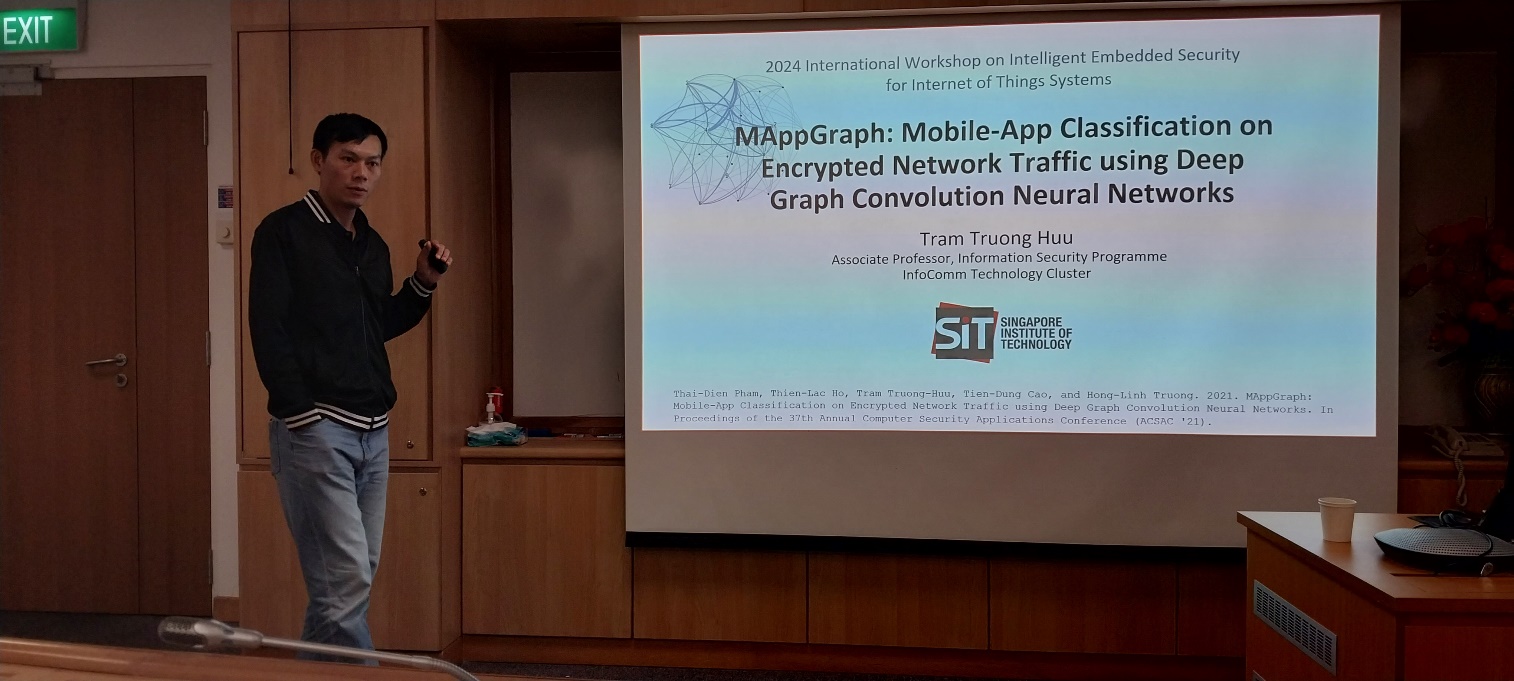
Prof. Hoang Van Phuc presents about Improving Security in RISC-V Based IoT Systems.



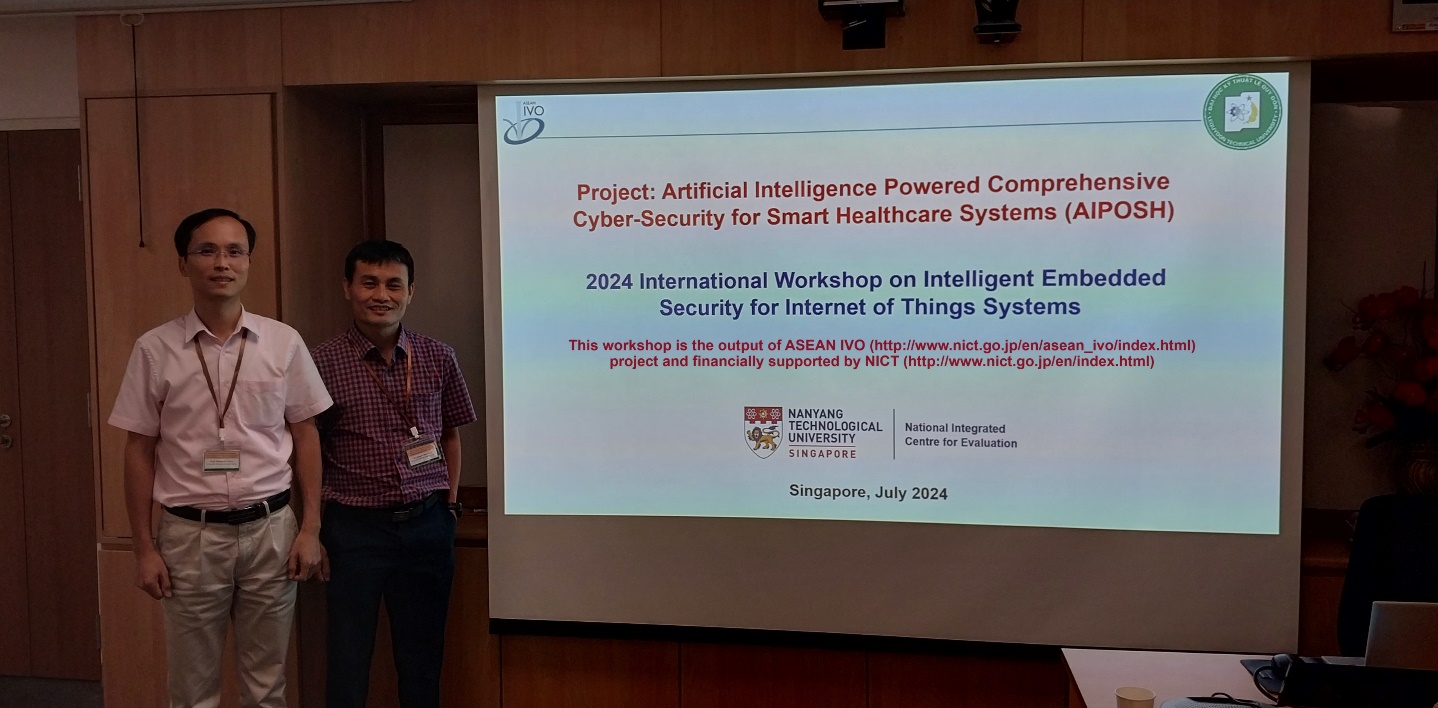
Prof. Kazuo Sakiyama delivers a keynote talk on Advanced side channel analysis methods.



Dr. Nguyen Van Trung presents Energy Efficient Power Management IC for Edge IoT Devices.



Prof. Tram Truong Huu presents on MappGraph - Mobile-App Classification on Encrypted Network Traffic using Deep Graph Convolution Neural Networks.



After panel discussion and follow-up plan.

**VI. Workshop Evaluation Questionnaire**

**WORKSHOP EVALUATION QUESTIONNAIRE #1**

**Workshop Name:** Intelligent Embedded Security for Internet of Things Systems

**Location:** 50 Nanyang Avenue, Singapore 639798

**Date:** 22-24, July 2024

**Participant Name (optional): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Institution /Company name of participant (optional): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Job Title:** Professor

**Please give us your comments here:**

The workshop provides an excellent opportunity for researchers in the field of intelligent systems and embedded security for Internet of Things applications to approach new research directions, results, and technologies. Speakers are famous experts in the field.

The workshop is well organized with an interesting program and nice talks. The discussion session is useful for future plan.

**WORKSHOP EVALUATION QUESTIONNAIRE #2**

**Workshop Name:** Intelligent Embedded Security for Internet of Things Systems

**Location:** 50 Nanyang Avenue, Singapore 639798

**Date:** 22-24, July 2024

**Participant Name (optional): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Institution /Company name of participant (optional): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Job Title:** Senior Research Fellow

**Please give us your comments here:**

This workshop is helpful for us by providing a forum to exchange the ideas, solutions and research results in the field. The topic of this workshop is very hot and important in literature.

The program agenda is reasonable, and the talk content is interesting. However, the speakers from more countries are expected in the future events.

**WORKSHOP EVALUATION QUESTIONNAIRE #3**

**Workshop Name:** Intelligent Embedded Security for Internet of Things Systems

**Location:** 50 Nanyang Avenue, Singapore 639798

**Date:** 22-24, July 2024

**Participant Name (optional): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Institution /Company name of participant (optional): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Job Title:** Research Engineer

**Please give us your comments here:**

The workshop is very important for this project. It is a good chance for researchers in this field to discuss and exchange ideas, innovative techniques, and results. Speakers are from leading universities/institutes.

The workshop has a good program with interesting talks. More workshops should be organized in the future. Thank ASEAN IVO and NICT for the financial support with this workshop.