Project Title: Artificial Intelligence Powered Hardware Security for Sustainable Cities of Future (AIPOSC)

Van-Phuc Hoang[1]; Quang-Kien Trinh[1]; Van-Trung Nguyen[1]; Thi-Nga Dao[1]; Cong-Kha Pham[2]; Massimo Alioto[3]
[1]Le Quy Don Technical University (LQDTU), Vietnam
[2]The University of Electro-Communications (UEC), Japan
[3]Faculty of Engineering, National University of Singapore (NUS)

November, 2020

Introduction

Background:

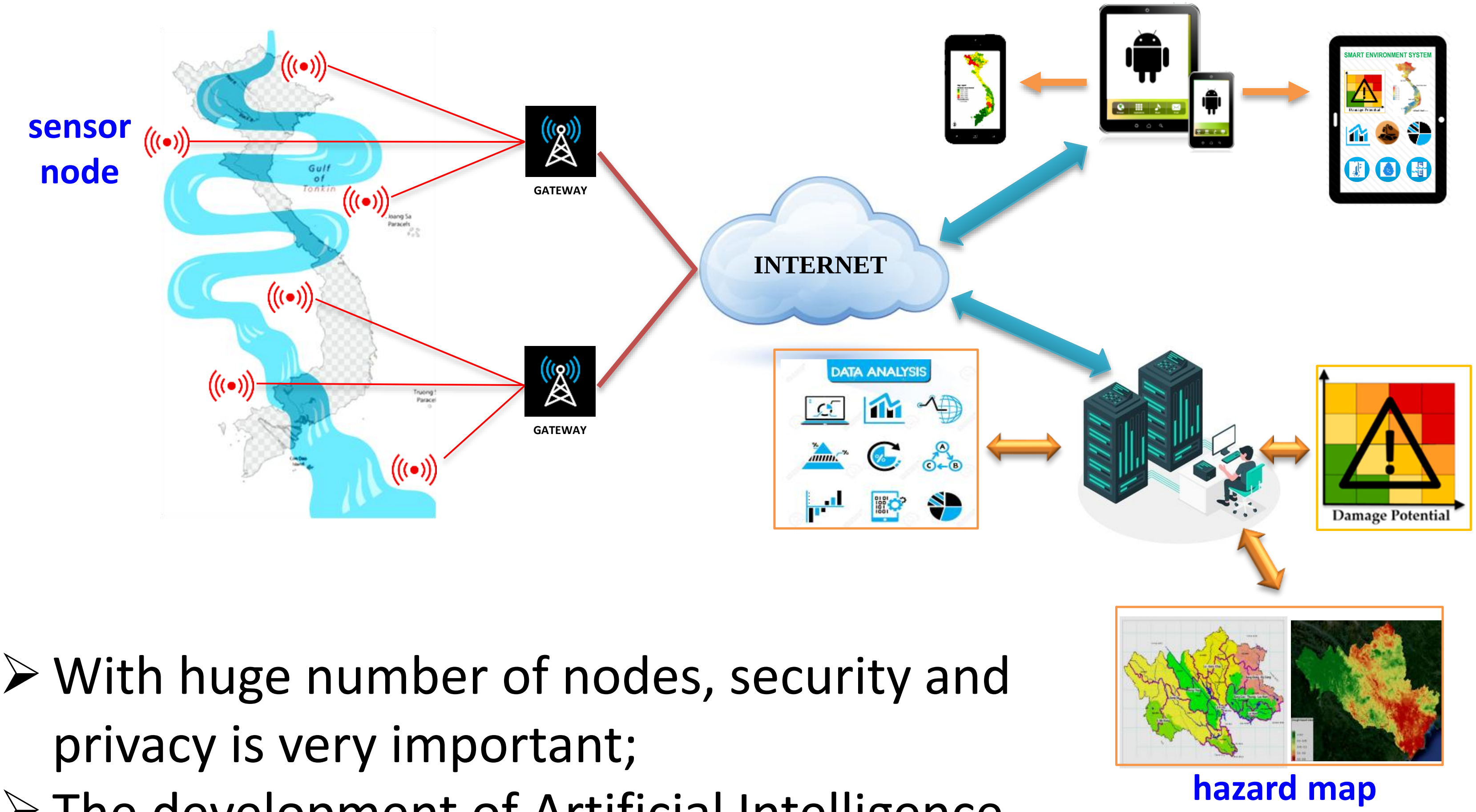
Recent attacks against IoT devices have posed serious security and privacy issues. It was reported that over 70% of IoT devices in Vietnam are vulnerable to cyber-attacks. As the developing countries, the vulnerability of the supply chain in ASEAN countries can cause damage and disruption since it is extremely difficult to secure the supply chain due to the vulnerabilities can be inherent, or introduced and exploited at any point in the supply chain.

Targets:

- Propose solutions for hardware security issues including: 1) secure IoT system using ML attack resistant PUF designs; 2) hardware Trojan (HT) detection for trusted supply chain and sustainable IoT systems in smart cities using advanced signal processing techniques with deep learning (DL) assistance; 3) DL assisted security evaluating, such as SCA evaluation, of the application specific processors and electronic devices;
- Contribute to capacity building of ASEAN institutions in the field of IoT hardware security;
- Develop existing links and establish new links for researchers from ASEAN, Japan and EU in the areas of hardware security for IoT based smart cities. This is attainable through interaction mechanisms during our capacity building sessions;
- Deliver both international leading-edge research and uniquely skilled researchers in the area of AI powered hardware security for IoT systems.

Project leader: Prof. Van-Phuc Hoang (LQDTU, Vietnam)

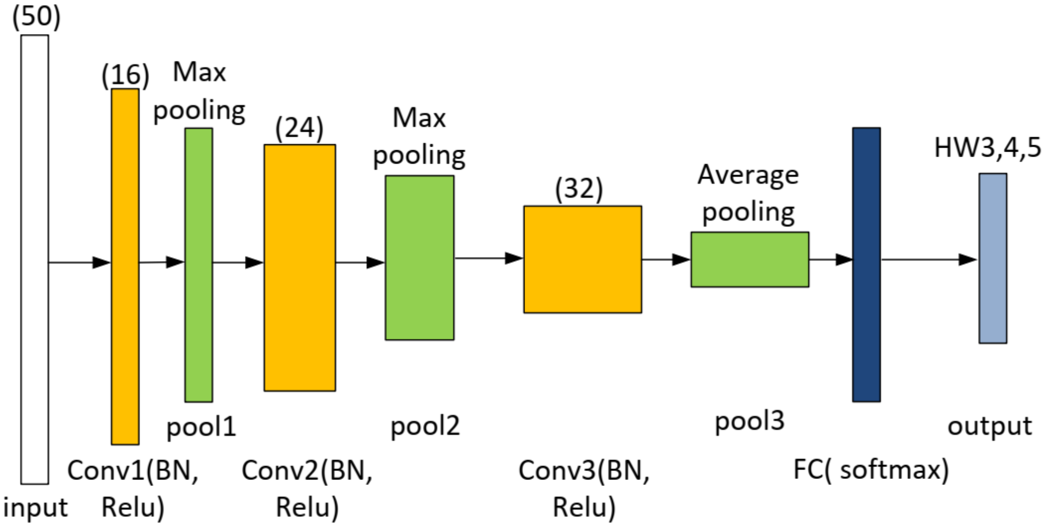
General IoT System for Smart Cities

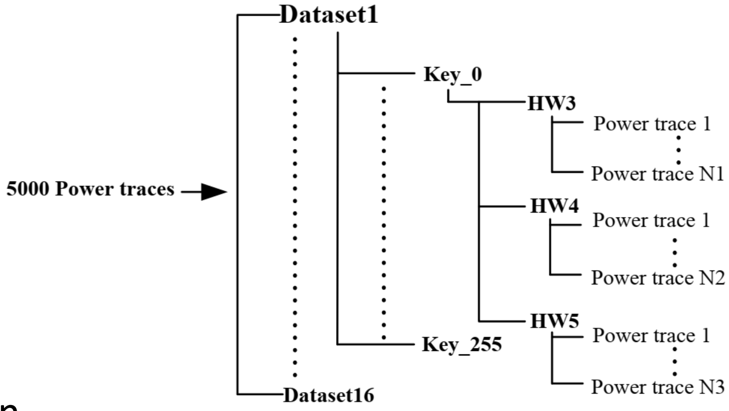


- ➢ With huge number of nodes, security and privacy is very important;
- ➢ The development of Artificial Intelligence (AI) provides efficient tools for hardware security evaluation.

Some Plenary Results

- Non-profiled side channel attacks based on convolutional neural networks with power traces for AES cryptography.
- Proposed method helps to reduce the number of required power traces.





Ngoc-Tuan Do, Van-Phuc Hoang, Van-Sang Doan, "Performance Analysis of Non-Profiled Side Channel Attacks Based on Convolutional Neural Networks," IEEE APCCAS 2020.

Intellectual Merit of Proposed Project

- This project will provide basic guidelines on several advanced technologies based on AI for hardware security and its related technologies.
- R&D results will be presented and published in renowned and impactful conferences and journal papers to share our developed technologies and to show the technical benefits of this project.
- We will contribute to the standardization activities under this collaboration to ensure international sustainability and expandability.
- We will apply for patents and collaborate with industry to transfer our technology to society for practical applications in future smart cities.

Broader Impacts

- ASEAN countries are among nations affected heavily on cybersecurity attacks, especially on IoT related systems where the hardware security is the essential issue. Therefore, our research will lead to the widespread use of more secure IoT devices in smart cities as expected that the IoT will yield up to $11.1 trillion in economic value a year by 2025, and interestingly, 40 percent of which could be from developing economies.
- This project is to raise awareness amongst policy makers, business and industries, people in ASEAN on secure IoT systems as a management tool and possible roles in tackling the problems of ICT, business, transportation, industry and others.
- The research results will be submitted as research papers for academic peer-review journals as well as research papers to for regional and global conferences to share project results. This will contribute significantly to IoT and hardware security research areas.

Methods

- Based on a deep and comprehensive survey on the hardware security issues in IoT systems and current research issues, existing solutions in this topic, we will clarify the risks, detailed requirements for implementing these hardware security solutions.
- Propose the innovative and new solutions to improve hardware security in IoT systems.
- DL techniques will also be exploited and utilized in the evaluation of PUF designs, anti-SCA attack and hardware Trojan detection solutions.
- FPGA based prototypes are used to preliminarily evaluate the performance and parameters of the proposed designs. Then, several ASIC design techniques will be employed to implement the proposed designs.

Proposed Content

- **WP (Work package 1)**: Management and logistics.
- **WP2**: Survey and subsystem development.
- **WP3**: Prototype development and proof-of-concept experiment.
- **WP4**: Demonstration, application development and technology transfer.

Plan for Connected Projects

- Collaboration between different partners to share the knowledge and experience in this emerging and exciting field;
- Promote the developed technologies to academia, industry, and practical applications in different countries:
  - Prof. Van-Phuc Hoang, Dr. Quang-Kien Trinh, Dr. Thi-Nga Dao, Dr. Van-Trung Nguyen and others from LQDTU, Vietnam
  - Dr. Takeshi Takahashi and his colleagues from NICT, Japan
  - Prof. Kazuo Sakiyama & Prof. Cong-Kha Pham from UEC, Japan
  - Prof. Massimo Alioto, NUS, Singapore
  - Prof. Máire O’Neill and Dr. Chongyan Gu from QUB, UK

Conclusions

- Hardware oriented security is becoming essential for IoT network in smart cities.
- The development of Artificial Intelligence (AI) provides efficient tools for hardware security evaluation.
- The proposal will be performed with collaboration of leading experts from ASEAN countries, Japan and EU.