# 2018 PROJECT

## Cyber-Attack Detection and Information Security for Industry 4.0

## PROGRESS REPORT

November 2020

University of Engineering and Technology
Vietnam National University, Hanoi

NANYANG TECHNOLOGICAL UNIVERSITY
SINGAPORE

UTS
UNIVERSITY OF TECHNOLOGY, SYDNEY

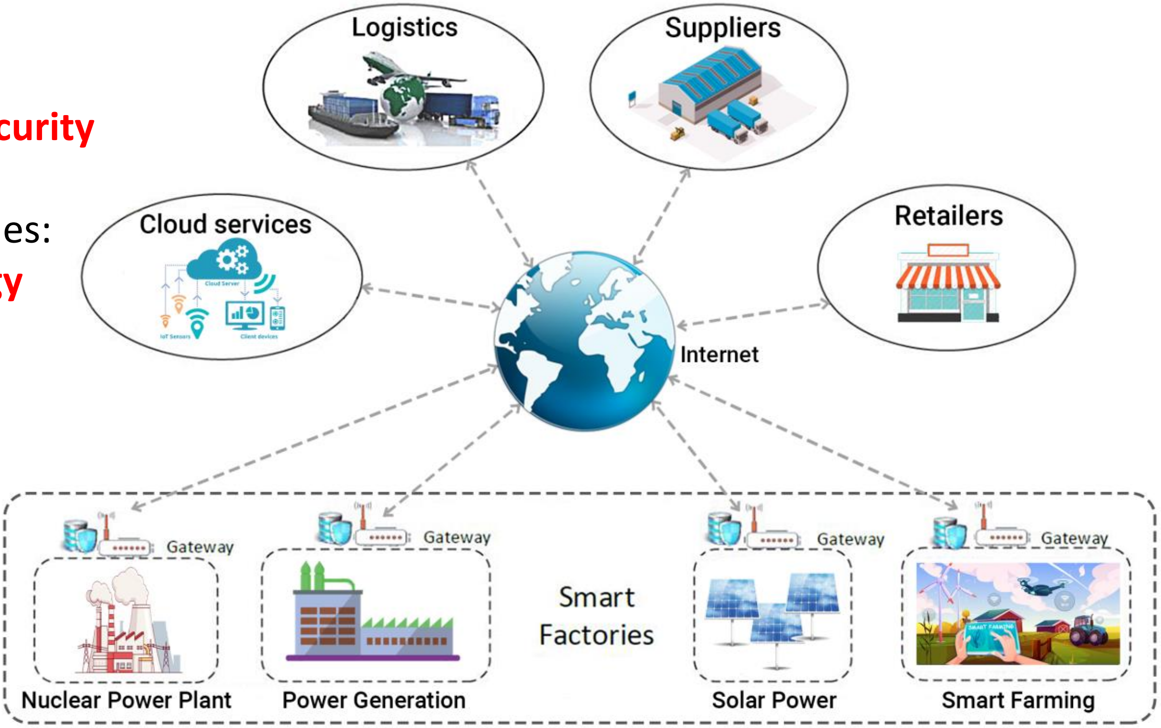
# Project: Cyber-Attack Detection and Information Security for Industry 4.0

## Context - Industry 4.0

- a main driver for the development of smart cities
- a vision of smart factories built with intelligent cyber-physical systems
- breakthrough achievements in many sectors (healthcare, food, and agriculture, …)
- when connected to the cyber world, **cybersecurity risks** become a key concern due to open systems with IP addresses

## Objectives

To provide tools to **enhance cybersecurity** in Industry 4.0 by applying several recently-developed smart technologies: **deep learning**, **blockchain technology** and **physical-layer security**



## Speaker: Nguyen Linh Trung

VNU University of Engineering and Technology, Hanoi, Vietnam

# Project information: Targets & Tasks

**Targets:**

1. A method to detect cyber-security threats in Industry 4.0 through using advanced deep learning algorithms
2. A framework to protect data from cyber-attacks using blockchain technology
3. Solutions to enhance security at the physical interface of information transmission using physical-layer security technology
4. A sustainable research collaboration network in the ASEAN region, in Australia and worldwide, for developing human resource in Vietnam that is able to develop effective cyber-security solutions

**Tasks**: 6  scientific tasks (Tasks 1 to 6), 1 technological task (Task 7), 1 networking task (Task 8)

# Project information: Members, etc.

- **Project members:**
  1. VNU-UET (Vietnam): Assoc. Prof. Nguyen Linh Trung (leader)
  2. VNU-UET (Vietnam): Assoc. Prof. Nguyen Viet Ha
  3. NTU (Singapore): Prof. Dusit Niyato
  4. UTS (Australia): Prof. Eryk Dutkiewicz
  5. UTS (Australia): Dr. Diep Nguyen
  6. UTS (Australia): Dr. Hoang Dinh
  7. VNU-UET (Vietnam): Dr. Tran Thi Thuy Quynh (9/2019)
  8. VNU-UET (Vietnam): Dr. Ta Duc Tuyen (9/2019)
  9. VNU-UET (Vietnam): M.Sc. Tran Viet Khoa (PhD student, 9/2019)
  10. VNU-UET (Vietnam): M.Sc. Bui Minh Tuan (PhD student, 9/2019)

- **Project duration**: 7/2018 – 6/2021 (36 months)

- **Project budget**: NICT: 110k

# Project Activities & Results: Scientific - Task 1 (UET, UTS)

## Task 1: Analyze and identify potential cyber-security risks in Industry 4.0

❖ 2019: Literature study of cyber-security vulnerabilities and potential risks of manufacturing systems in Industry 4.0.

- ✓ Analyze interactions between Operation Technology (OT) and Information Technology (IT)
- ✓ Main vulnerabilities and risks in manufacturing in I4 [1]

❖ 2020: Survey main vulnerabilities and risks in Vietnam

- ✓ Studied the influences of threats on manufacturing in details
- ✓ The cyber attack case studies in Vietnam
- ✓ Impacts of Covid 19 on cyber security [1]

| Types | Vulnerabilities and exposures | Consequences |
|---|---|---|
| IT Network Threats | - Software used to operate the hardware may no longer be supported, maintained, and updated<br>- Unsupported operating systems | - Old malware families as Downad (aka Conficker), WannaCry (WCry), andGamarue (Andromeda) are in manufacturing environments |
| | - Autorun (autorun.inf) in USB or infected removable devices | The propagation of virus or worms |
| | - Targeted campaigns and opportunistic hacking incidents | - Espionage or information exfiltration<br>- Isolated manufacturing networks are not entirely safe from internet worms |
| OT Network Threats | - ICS Vulnerabilities: human-machine interfaces (HMIs), Programmable logic controllers (PLCs), and SCADA, e.g. Stuxnet (Iran), ESET (Slovakia), … | - Destroy factories<br>- Destroy infrastructure |
| Intellectual property | - Malicious computer-aided design files<br>- Word documents that may have been kept in old, isolated machines or archived in data storages | - Industrial espionage |

| Industry sectors | Types of attack | Case's Consequences |
|---|---|---|
| Transportation (airport system), | Advanced and persistent threat, (APT)<br>Deface | - The VIP membership databases of national carrier Vietnam Airlines was also stolen and leaked online, and roughly 411,000 passengers had also been exposed (Jul, 2016) |
| Financial/Banks | - Ransomware and malware | - A customer of Vietcombank, lost more than 22.000 USD via Internet Banking transaction, Aug 2016<br>- Ransomware cost Vietnamese users about VND15 trillion or more than $600 million (BKAV 2017) |
| Website, computer | - Malware | Damage caused by computer viruses to Vietnamese users reached a record of VND 14,900 billion, equivalent to US $642 million |

*[1] Analyze and identify potential cyber-security risks in Industry 4.0, AVITECH Technical report, 2020*

# Project Activities & Results: Scientific - Task 2 (UET, UTS)

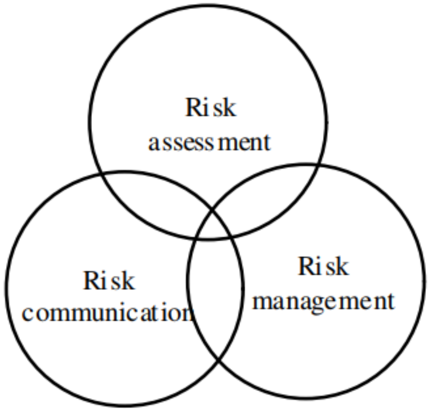
Task 2: Develop an innovative risk assessment model which can efficiently quantify cyber-security risks for Industry 4.0

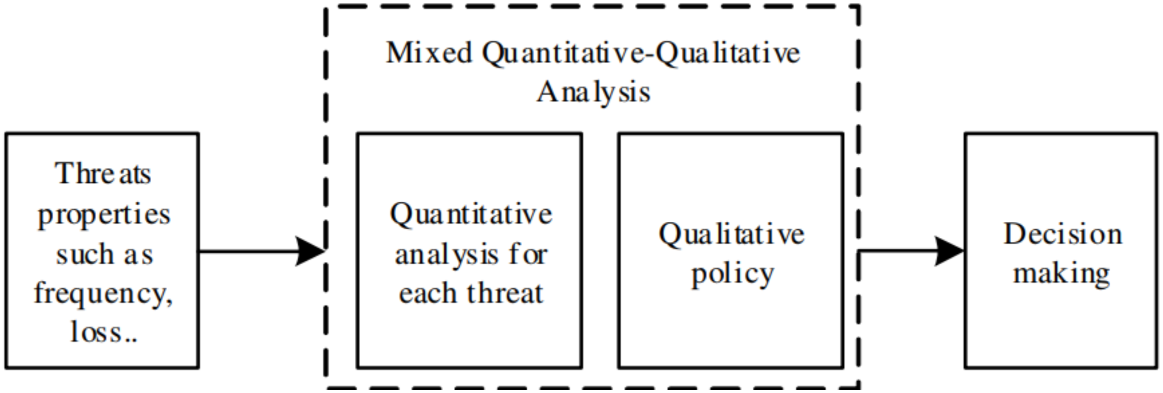
❖Activity

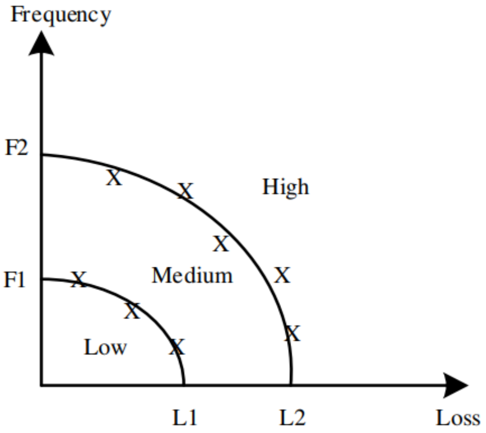
✓ 2020: Preliminarily overviewed the quantitative and qualitative risk analyses and risk assessment model.

❖Result

✓ Proposed the use of an appropriate risk assessment model to classify the risks in cybersecurity of I4 [1].




Threats properties such as frequency, loss..
Mixed Quantitative-Qualitative Analysis
Quantitative analysis for each threat
Qualitative policy
Decision making



[1] Risk models for the security of Industry 4.0 systems, AVITECH Technical report, 2020

# Project Activities & Results: Scientific - Task 4 (UET, UTS)

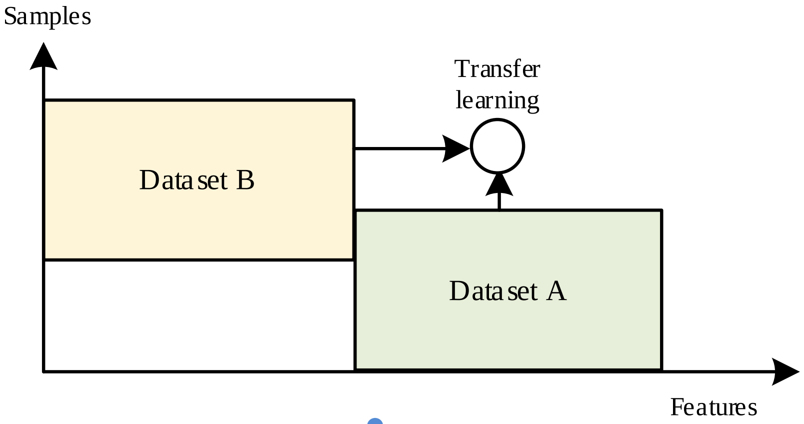
## Task 4: Develop and implement an innovative method to detect and isolate cyber-security attacks using deep learning

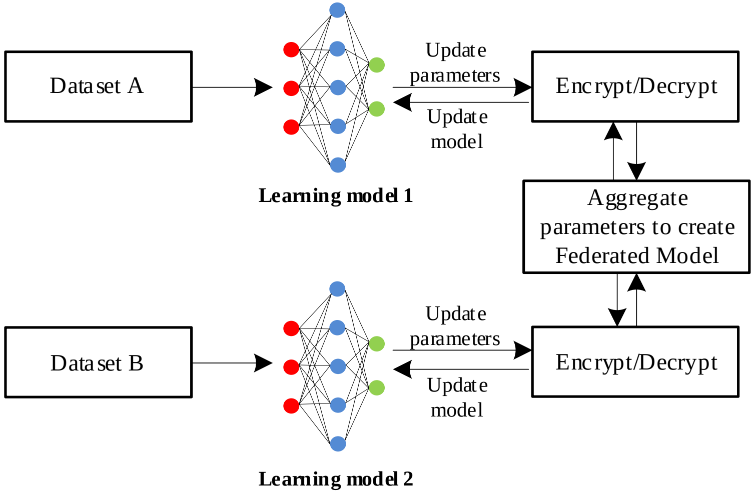
❖ 2019: Proposed collaborative learning-based cyberattack detection model to identify attack in distributed environment of Industry 4.0 by learning data which have the same properties [1].

❖ 2020: set-up collaboration with Cybersecurity Lab at NICT on machine learning for cybersecurity

❖2020: Applied federated transfer learning to the above developed cyberattack detection model [2].

- ✓ The revised model can identify attack in distributed environment of Industry 4.0 by learning from datasets which have different properties.
- ✓ The revised model was tested with NSL-KDD cybersecurity dataset and produced good results.





*[1] Collaborative learning model for cyberattack detection systems in IoT Industry 4.0, WCNC 2020*

*[2] Transfer learning model for cyberattack detection, AVITECH Technical report, 2020*

# Project Activities & Results: Scientific - Task 5 (UET, NTU, UTS)

## Task 5: Develop an unprecedented data securing method using blockchain technology

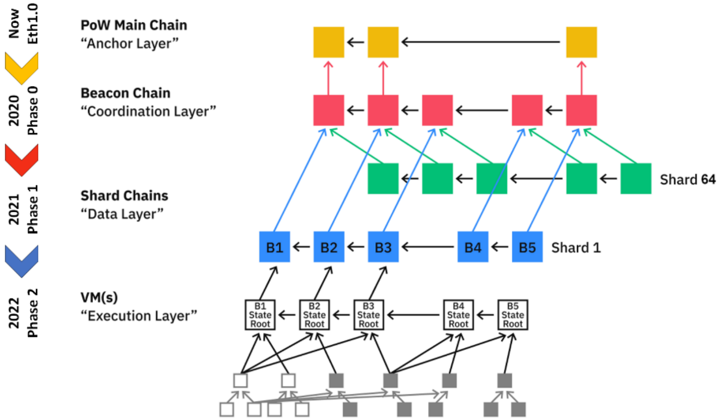
❖ 2019: Overviewed the development of decentralized consensus mechanisms and mining strategy management in blockchain networks [1].

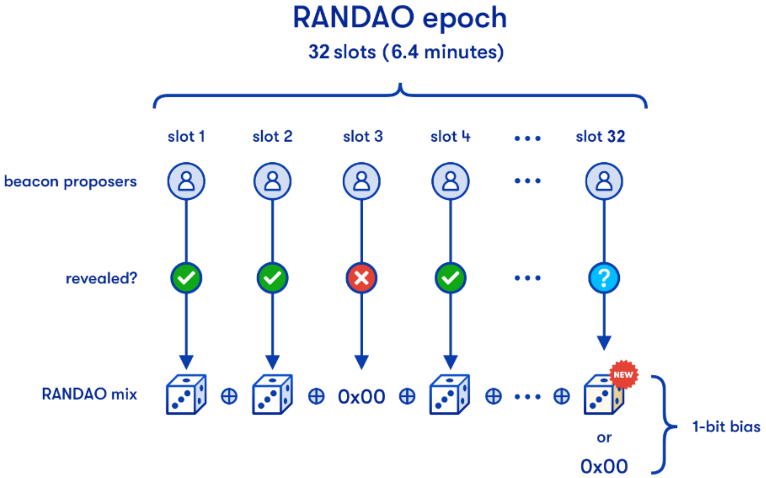
❖ 2020: Reviewed the migration of PoW in Ethereum 1.0 to PoS in Ethereum 2.0 [2]

✓ Joined Prysmatic Labs community and deployed a private Ethereum 2.0 network at phase 0.

✓ Compared performance between Ethereum 1.0 and 2.0 in terms of CPU and Power consumptions

✓ Determined of drawback of RANDAO protocol is Last-Revealer Attacks in Beacon Chain Randomness





[1] *Proof-of-stake consensus mechanisms for future blockchain networks, IEEE Access, 2019*

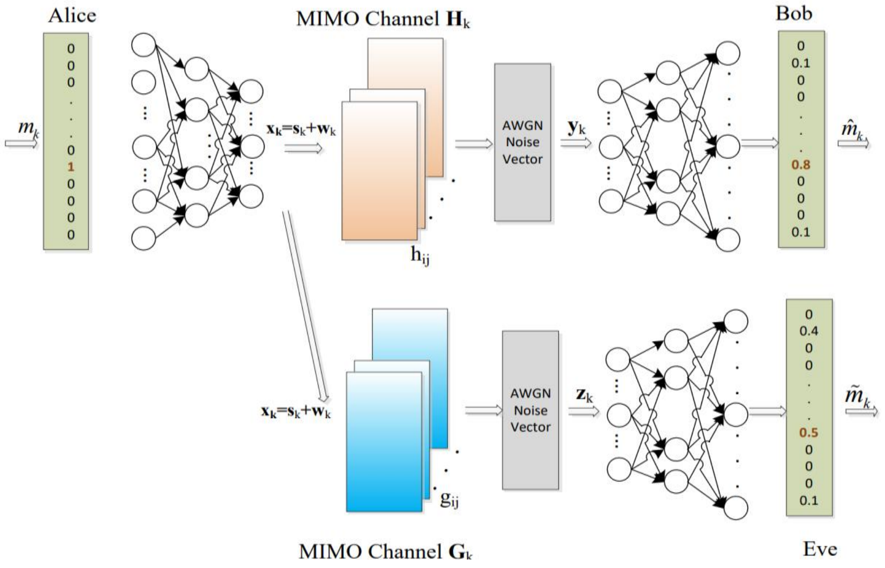
[2] *Data security using blockchain technology, AVITECH Technical report, 2020*

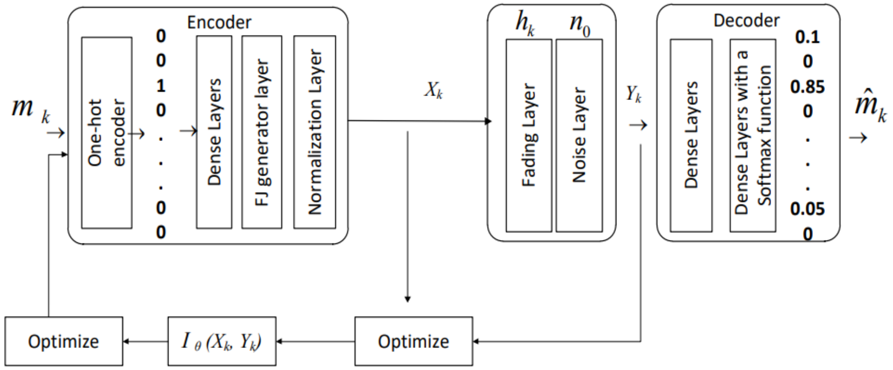
# Project Activities & Results: Scientific - Task 6 (UET, UTS)

## Task 6: Develop receiver-based friendly jamming and collaborative beamforming methods to safeguard sensors/actuators

- 2019: Studied how to combine auto-encoder and friendly jamming (AE-FJ) for PLS, propose AE-FJ scheme for MISO wire tap channel, and MINE-based FJ scheme for MISO wire tap channel [1]

- 2020: Exploited the generalization capability of neural networks to develop the robust MIMO FJ scheme with imperfect channel [2]
  - ✓ Developed a new security scheme in which the secrecy optimization in which compact q-bit representation of the CSI is available at the transmitter instead of the perfect CSI
  - ✓ Proposed MINE-based FJ scheme for MIMO wire tap channel without CSI
  - ✓ Proposed AE-FJ scheme for MIMO wire tap channel





*[1] Autoencoder based Friendly Jamming, WCNC 2020*

*[2] Learning based friendly Jamming with imperfect CSI for security in MIMO wiretap channel, AVITECH Technical report, 2020*

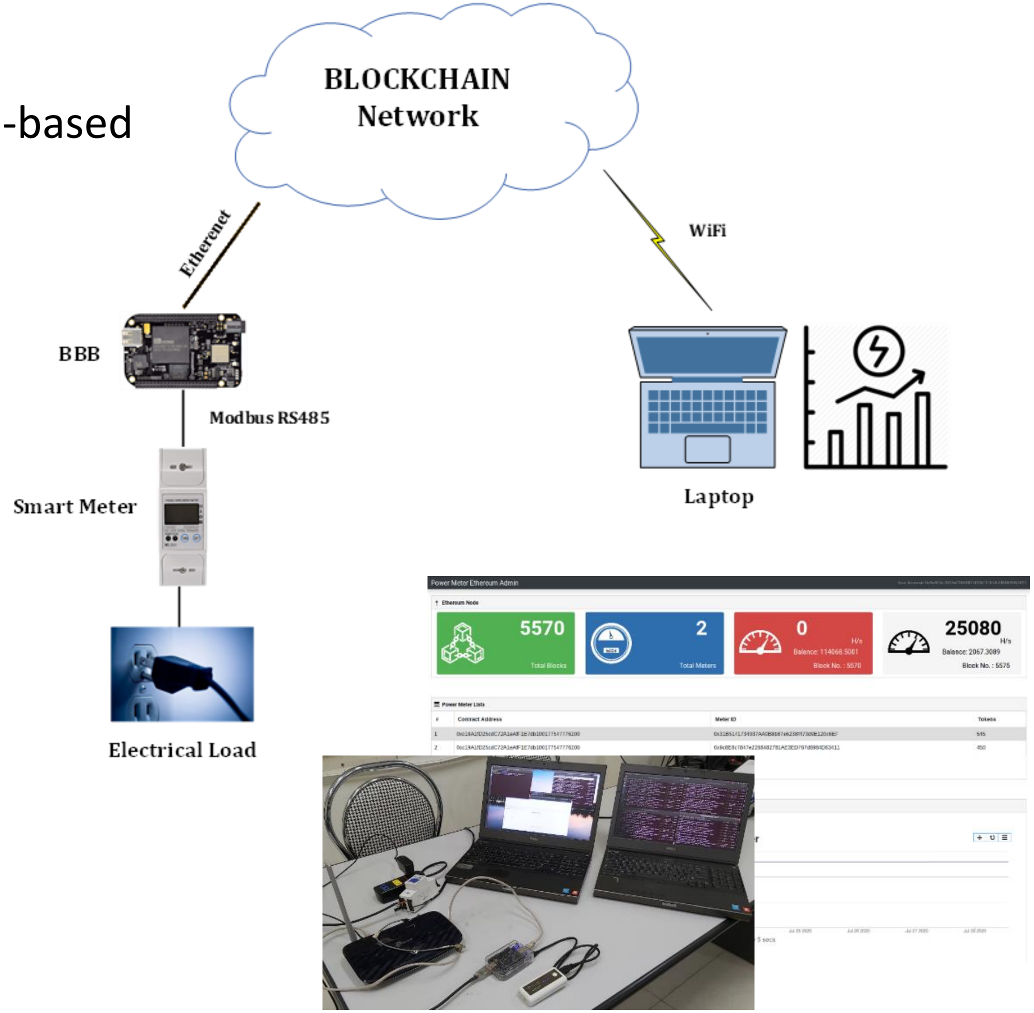
# Project Activities & Results: Technological - Task 7 (UET, NTU, UTS)

## Task 7: Implement and evaluate performance of the proposed blockchain application on a real testbed

❖ 2019: Studied the design of a blockchain-based testbed for smart grids, smart factories

❖ 2020: Built several system models to implement the testbed for smart grids [1]:

- ✓ Studied cyberattacks to blockchain network (Ethereum 1.0)
- ✓ Implemented two versions of the testbed, on: Public and Private Ethereum networks
- ✓ Verified the resistance of the blockchain testbed against two types of cyberattacks: DDoS & 51% attacks



| # | Contract Address | Meter ID | Tokens |
|---|---|---|---|
| 1 | 0xc19A1fD25cdC72A1eAfF1E7db100177547776200 | 0x3185141734037AA0B8b87e6238f73d9E120c6EF | 545 |
| 2 | 0xc19A1fD25cdC72A1eAfF1E7db100177547776200 | 0x9c8E8c7847e2288482781AE3ED787d8984D63411 | 450 |

*[1] Implementation a blockchain based testbed for smart grids, AVITECH Technical report, 2020*

# Project Activities & Results: Networking - Task 8 (UET, NTU, UTS)

## Task 8: Annual Workshops and Exhibitions on Cyber-Security

❖ 2019:

✓ Organized IVO Workshop on cybersecurity in Industry 4.0, Hanoi, Vietnam, March 2019

✓ Organized special session on cybersecurity in Industry 4.0 within the 19th International Symposium on Communication and Information Technologies, Ho Chi Minh city, Vietnam, September 2019

❖ 2020:

✓ Researcher exchange (Nguyen Linh Trung, project leader), at Cybersecurity Laboratory at the NICT, 1 month (12/2019 – 1/2020)

✓ Plan for a researcher exchange (Mr. Tran Viet Khoa), at the Cybersecurity Laboratory at the NICT, 3 months (9-12/2020), to conduct research collaboration in machine learning for cyberattack detection: could not implement due to COVID

# Publications

❖ Conference Papers:

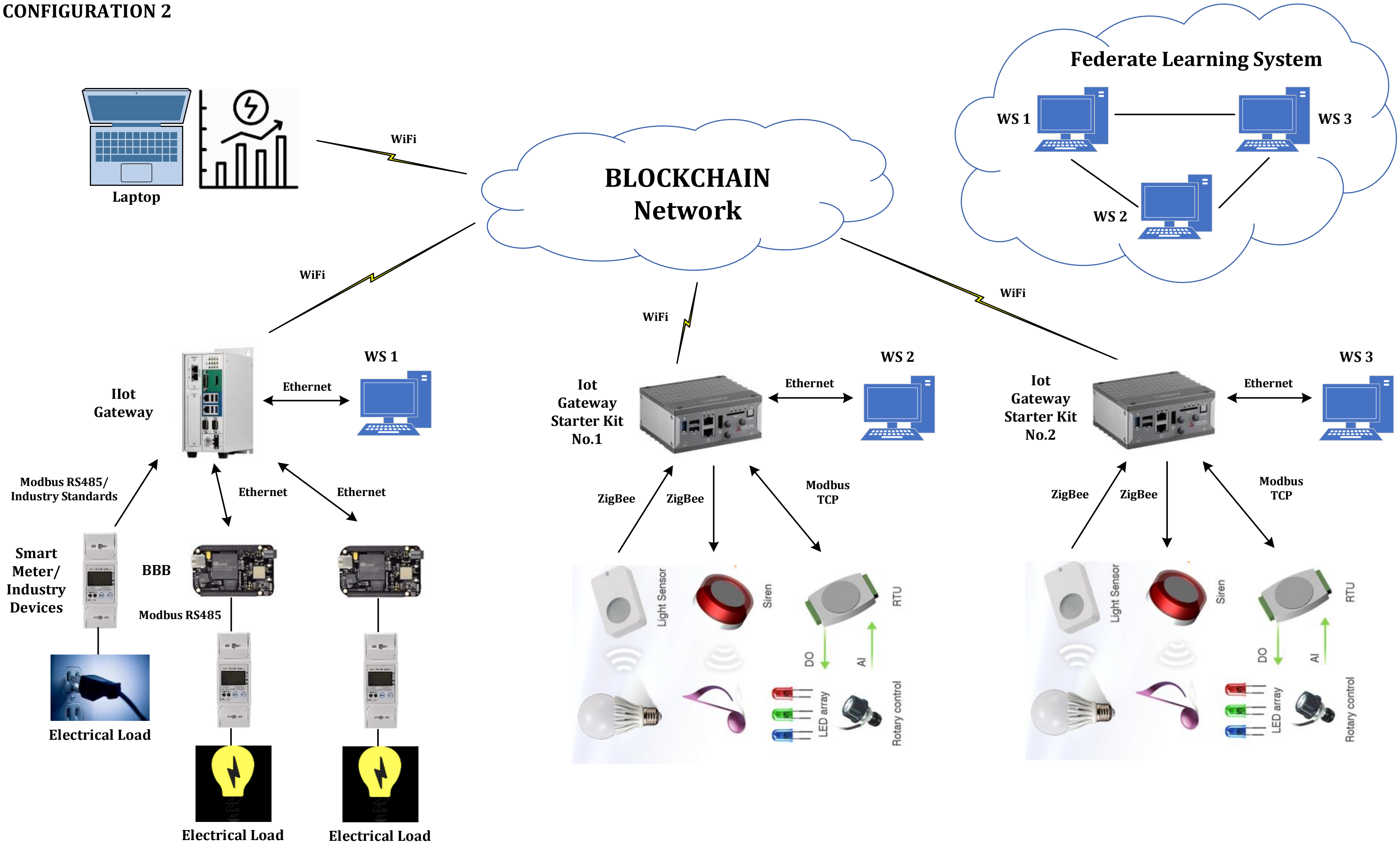
| No: | Paper title: | Author names | Affiliation | Conference name | date | venue |
|---|---|---|---|---|---|---|
| 1 | Network Coding with Multimedia Transmission: A Software-Defined-Radio based Implementation [Task 6] | TTT Quynh,<br>TV Khoa,<br>LV Nguyen,<br>NL Trung | VNU-UET | International Conference on Recent Advances in Signal Processing, Telecommunications and Computing | March 2019 | Hanoi, Vietnam |
| 2 | Collaborative Learning Model for Cyberattack Detection Systems in IoT Industry 4.0 [Task 4] | TV Khoa,<br>YM Saputra,<br>DT Hoang,<br>NL Trung,<br>DN Nguyen,<br>NV Ha,<br>E Dutkiewicz | VNU-UET, UTS | IEEE Wireless Communications and Networking Conference | May 2020 | Seoul, South Korea |
| 3 | Autoencoder based Friendly Jamming [Task 6] | BM Tuan,<br>TD Tuyen,<br>NL Trung,<br>NV Ha | VNU-UET | IEEE Wireless Communications and Networking Conference | May 2020 | Seoul, South Korea |

❖ Journal Papers:

| No: | Paper title | Author | Affiliation | Journal | Publisher | Volume,Number, Pages |
|---|---|---|---|---|---|---|
| 1 | A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks [Tasks 5, 7] | W Wang, DT Hoang, P Hu, Z Xiong, D Niyato, P Wang, Y Wen, D Kim | NTU, UTS | IEEE Access | IEEE | vol. 7, pp. 22328-22370, 2019 |

# Societal Impact

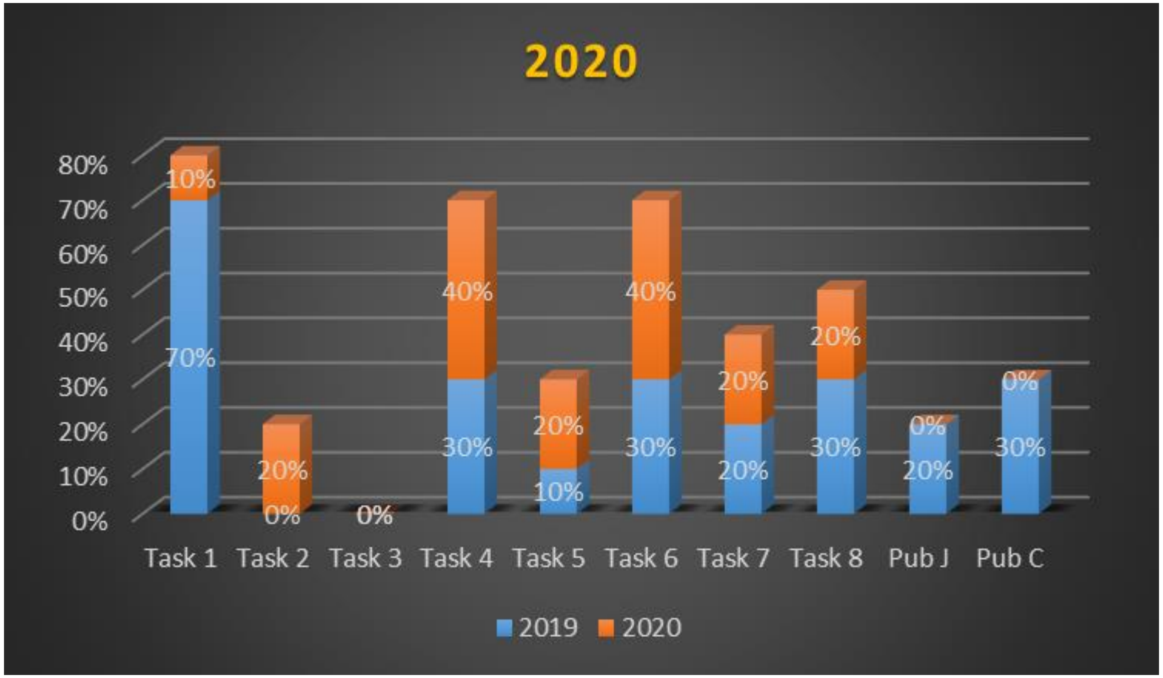
❖ Smart grid, Smart factory (SCADA): to implement



# Project Activities: Budget

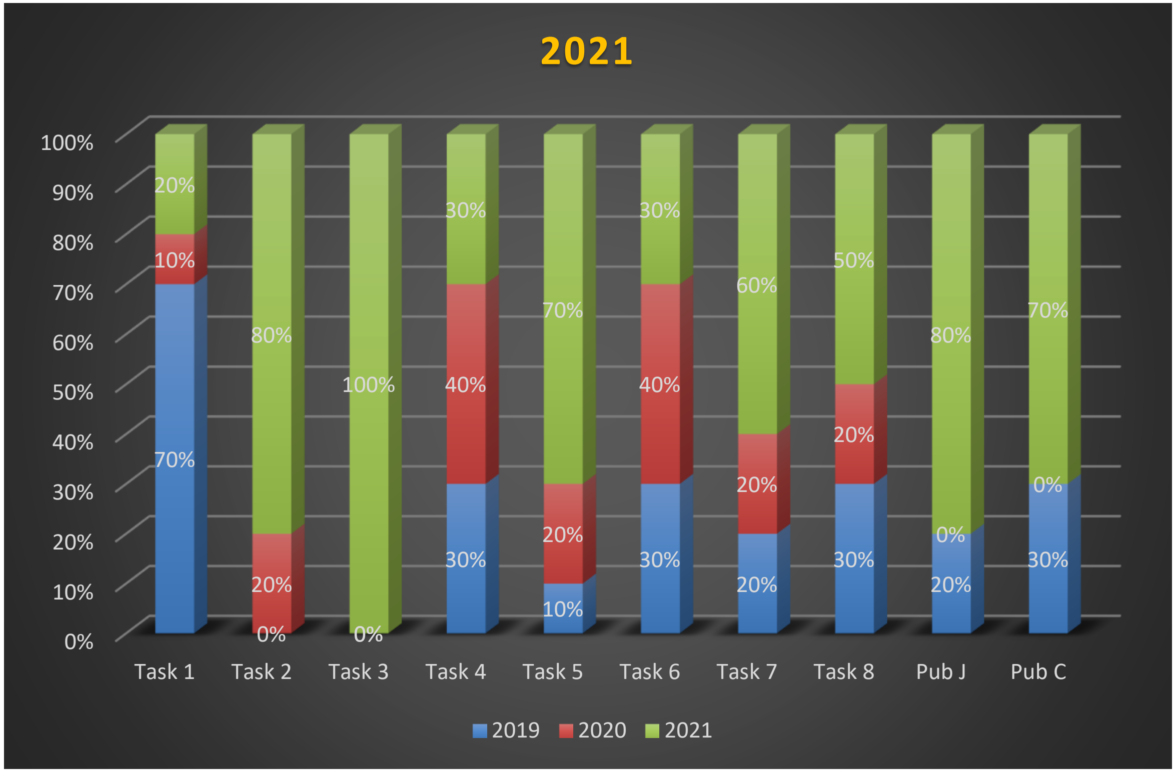
| No. | Title | Period & venue | Yen | USD |
|---|---|---|---|---|
| 1 | 2018 Forum (Nguyen Linh Trung, VNU-UET) | 2018/11/27-28, Jakarta | ¥91,347 | $820.90 |
| 2 | Kick-off meeting | 2018/12/14, Hanoi | ¥184,436 | $1,655.50 |
| 3 | Kick-off meeting (Dusit Niyato, NTU) | 2018/12/14, Hanoi | ¥96,500 | $871.17 |
| 4 | 1st IVO Wworkshop | 2019/3/26-28, Hanoi, Halong | ¥668,978 | $5,947.00 |
| 5 | 1st IVO Wworkshop (Takeshi Takahashi, NICT) | 2019/3/26-28, Hanoi | ¥104,500 | $926.34 |
| 6 | 2019 Forum (Nguyen Linh Trung, VNU-UET) | 2019/11/20-21, Manila | ¥99,065 | $899.96 |
| 7 | Research exchange (Nguyen Linh Trung, NICT) | 2019/12/15 – 2020/1/15 | ¥709,388 | $6,416.32 |
| 8 | Paper registration for WCNC 2020 | 2020/5/25-28 | ¥35,158 | $335 |
| 9 | Equipment (Testbed implementation) | purchase in progress | ¥3,238,757 | $30,860 |
| **Total** | | | ¥5,228,130 | $**48,732.19** |

# Conclusion: 2020



- ❖ General: Slow progress due to the outbreak of COVID-19
- ❖ Scientific: main tasks (4, 6) were in good progress, others were not
- ❖ Technological: preliminary studies have been done, waiting for the equipment (purchase in progress)
- ❖ Budget: plan for a 3-month research visit to NICT cannot be implemented due to COVID-19

# Future: 2021



- Scientific: Tasks 4, 6 are in good progress, almost ready for publication; Tasks 2, 3, 5 are slow, need more time to complete (extension)

- Technological: waiting for the equipment, need more time to complete (extension)

- Networking: unable to implement future planned activity: conference organization in Feb 2021, due to COVID

- Publication: unable to publish the planned book (as its contents come from the above planned conference); 3 more journal papers are expected

- Request: an extension of 6 months (until 12/2021).