2018 PROJECT

Cyber-Attack Detection and Information Security for Industry 4.0

PROGRESS REPORT

November 2021

VNU University of Engineering and Technology

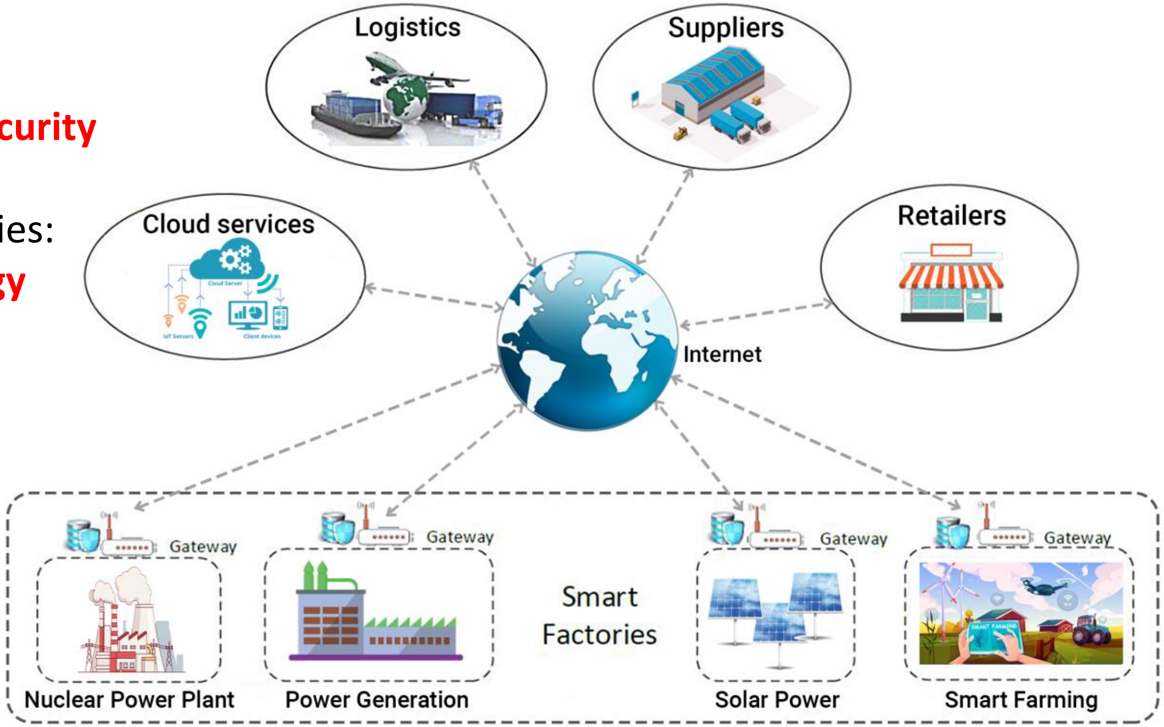
Project: Cyber-Attack Detection and Information Security for Industry 4.0

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

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 resources in Vietnam that is able to develop effective cyber-security solutions

Project information: Members, etc.

- ❖ **Project members:**
  1. VNU-UET (Vietnam): Prof. Nguyen Linh Trung (leader)
  2. VNU-UET (Vietnam): 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 (Ph.D. student, 9/2019)
  10. VNU-UET (Vietnam): M.Sc. Bui Minh Tuan (Ph.D. student, 9/2019)

- ❖ **Project duration**: 7/2018 – 6/2021 (36 months) – Extended to July 2022.

- ❖ **Project budget**: NICT: 110k; Actual expenses: 41.5k

Project Activities: Overall

1. **Scientific development**
    - ❖ Task 1: Analyze and identify potential cyber-security risks in Industry 4.0
    - ❖ Task 2: Develop an innovative risk assessment model to quantify the risks in Industry 4.0
    - ❖ Task 3: Implement an online web reference ranking the risks in Industry 4.0
    - ❖ Task 4: Develop and implement an innovative method to detect and isolate cyber-security attacks using deep learning
    - ❖ Task 5: Develop an unprecedented data securing method using blockchain technology
    - ❖ Task 6: Develop receiver-based friendly jamming and collaborative beamforming methods to safeguard sensors/actuators
2. **Technological Development & Experiments**
    - ❖ Task 7: Implement and evaluate the performance of the proposed blockchain application on a real testbed
3. **Networking**
    - ❖ Task 8: Annual Workshops and Exhibitions on Cyber-Security

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

Task 1: Analyze and identify potential cyber-security risks in Industry 4.0 (I4)

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

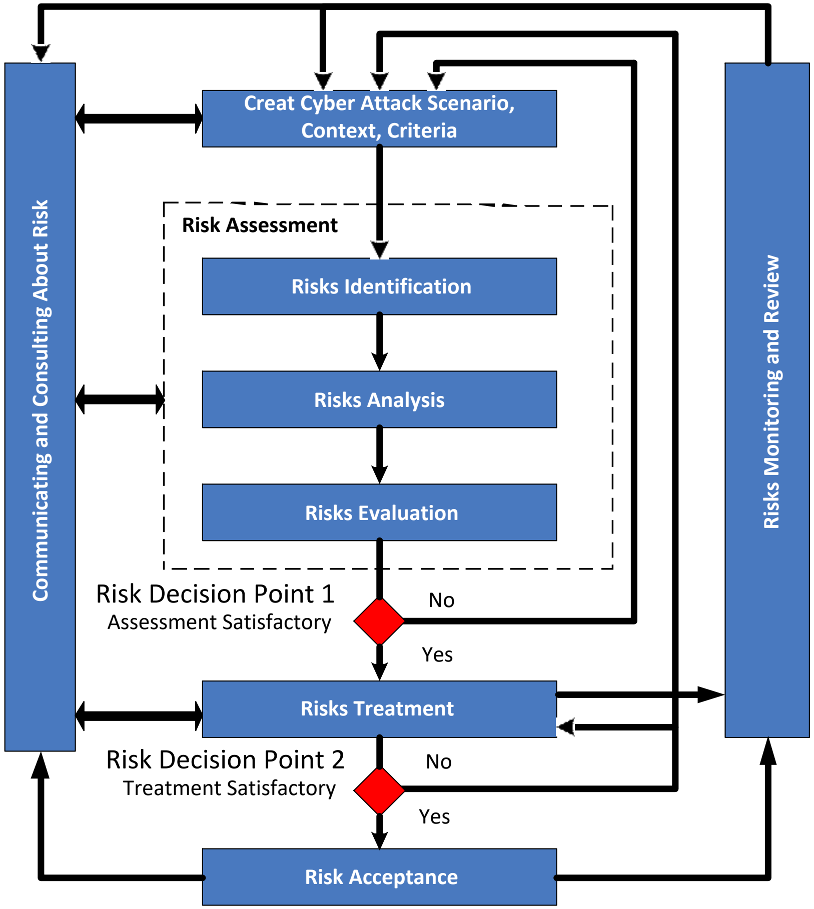
❖ 2020: Surveyed main vulnerabilities and risks in Vietnam

❖ 2021: Surveyed cybersecurity risk assessment and management standards widely used

✓ NIST SP 800-30 and ISO IEC, focusing on operational systems in Industry 4.0

✓ Standards applied in Vietnam: Vietnam National Standard 10295:2014, ISO/IEC 27001:2009, ISO/IEC 27005:2011

❖ 2022: To survey cybersecurity risk assessment and management standards for Industrial IoT systems.



Information security risk management process from ISO/IEC 27005

[1] Analyze and identify potential cyber-security risks in Industry 4.0, *Technical reports*, 2020 & 2021

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

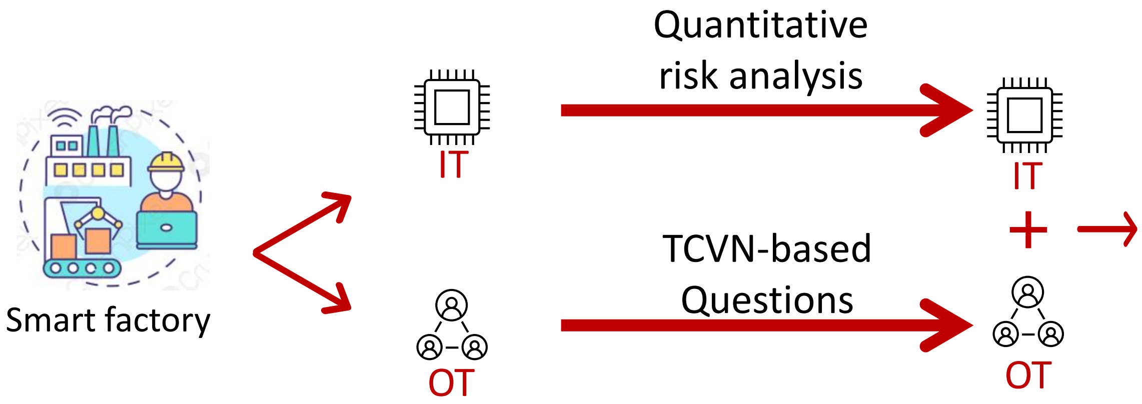
Task 2: Develop an innovative risk assessment model which can efficiently quantify cyber-security risks for Industry 4.0

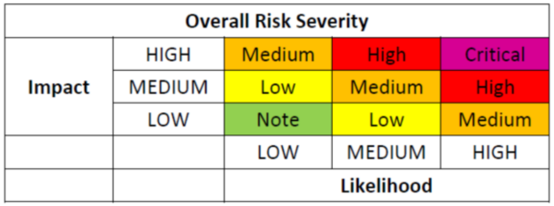
❖ 2019 & 2020: Overviewed the quantitative and qualitative risk analysis and risk assessment model [1].

❖ 2021: Studied the risk assessment methods, identified their pros and cons to find the appropriate method for Industry 4.0 [1]

- ✓ Studied the risk assessment methods widely applied to identifying the risks in Industry 4.0: OWASP, CVSS, Risk Scanning.
- ✓ Studied the architecture of smart factory systems and IoT ecosystems to find the weight of different layers in systems

❖ 2022: To propose a method of risk assessment, able to identify the risks in both IT and OT systems of a smart factory.





Overall Risk Severity				
Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Note	Low	Medium
		LOW	MEDIUM	HIGH
			Likelihood	

[1] Risk models for the security of Industry 4.0 systems , *Technical reports*, 2020 & 2021

Project Activities & Results: Scientific - Task 3 (UET)

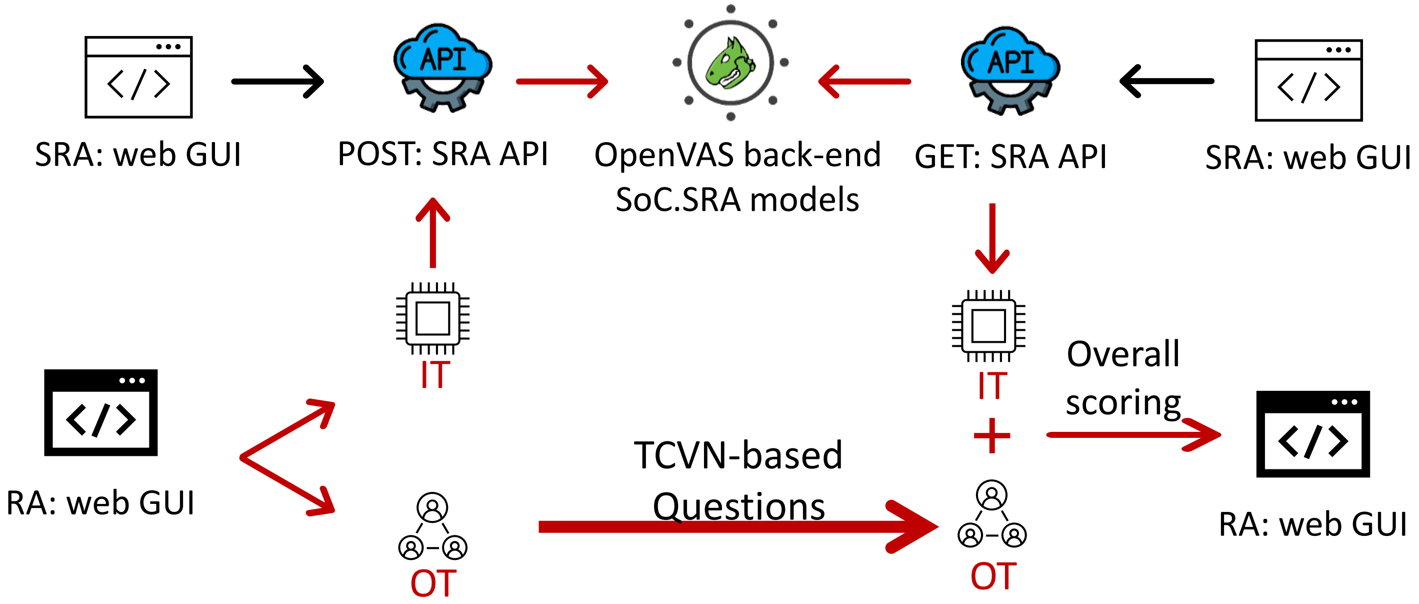
Task 3: Implement an online web reference service listing and ranking the risks in Industry 4.0

❖ 2019 and 2020: not started.

❖ 2021: Studied web programming for creating the target website and connect API to open-source risk assessment method

- ✓ Built the design flow of the website
- ✓ Connected the website to open-source methods

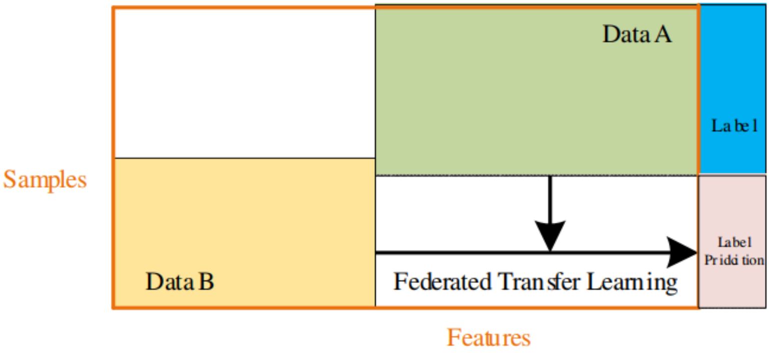
❖ 2022: To complete the website based on the proposed method in Task 2, for identifying the risks of both IT and OT of a smart factory.



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

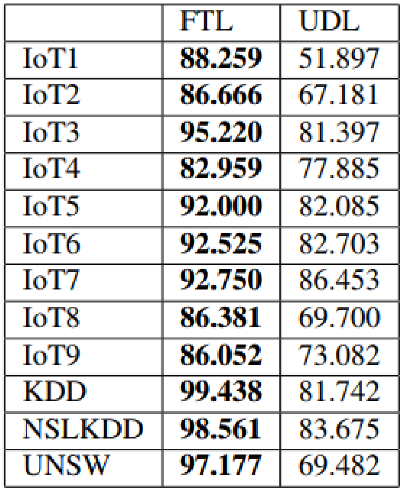
❖ 2019 & 2020: Proposed a novel collaborative learning-based cyberattack detection model, based on Federated Learning, to identify an attack in the distributed environment of Industry 4.0 by learning data that have the same properties, but with non-IoT datasets [1].



❖ 2021: Extended the above collaborative learning model, to combining both Federated Learning and Transfer Learning [2]:

✓ This model can identify an attack in a distributed environment of IoT networks from datasets that have different features, samples, or labels

✓ The model was run with Botnet-IoT KDD, NSL-KDD, UNSW dataset and demonstrated its advantage in comparison with unsupervised Deep Learning



	FTL	UDL
IoT1	**88.259**	51.897
IoT2	**86.666**	67.181
IoT3	**95.220**	81.397
IoT4	**82.959**	77.885
IoT5	**92.000**	82.085
IoT6	**92.525**	82.703
IoT7	**92.750**	86.453
IoT8	**86.381**	69.700
IoT9	**86.052**	73.082
KDD	**99.438**	81.742
NSLKDD	**98.561**	83.675
UNSW	**97.177**	69.482

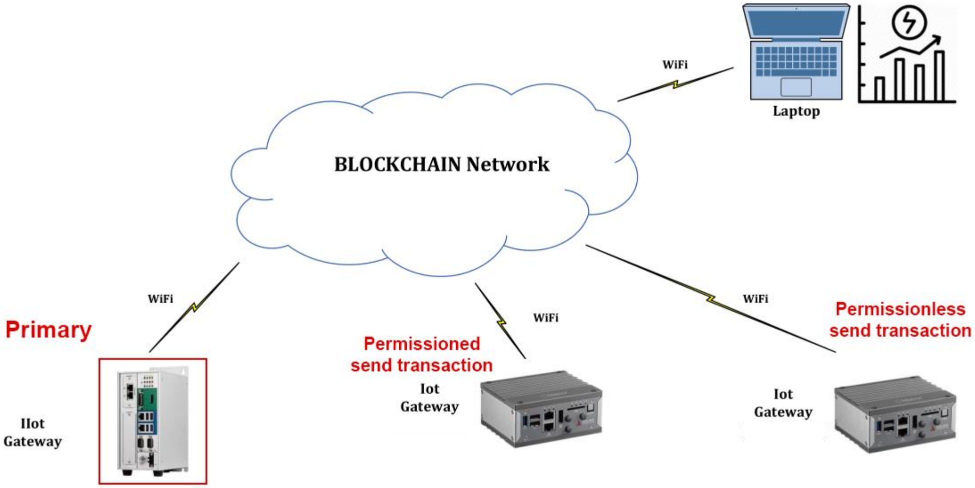
[1] "Collaborative Learning Model for Cyberattack Detection Systems in IoT Industry 4.0", *WCNC*, 2020.

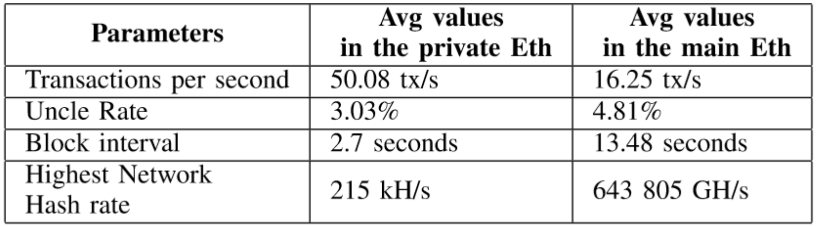
[2] "Deep Transfer Learning: A Novel Collaborative Learning Model for Cyberattack Detection Systems in IoT Networks", *IEEE Transactions on Cognitive Communications and Networking*, 2021 (to submit in December)

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

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

- 2020: Reviewed the migration of PoW in Ethereum 1.0 to PoS in Ethereum 2.0 [1]: computational power and Last-revealer attack.
- 2021: We proposed an effective framework to build a private Ethereum network for a smart grid [2].
  - ✓ A practical Ethereum-based smart grid is deployed with essential hardware at the home electrical system.
  - ✓ A smart contract for authentication in a securely multi-devices system is proposed.
  - ✓ A method to improve the efficiency of an Ethereum-based smart grid setup in practical work with the support of numerical experiments.





Parameters	Avg values in the private Eth	Avg values in the main Eth
Transactions per second	50.08 tx/s	16.25 tx/s
Uncle Rate	3.03%	4.81%
Block interval	2.7 seconds	13.48 seconds
Highest Network Hash rate	215 kH/s	643 805 GH/s

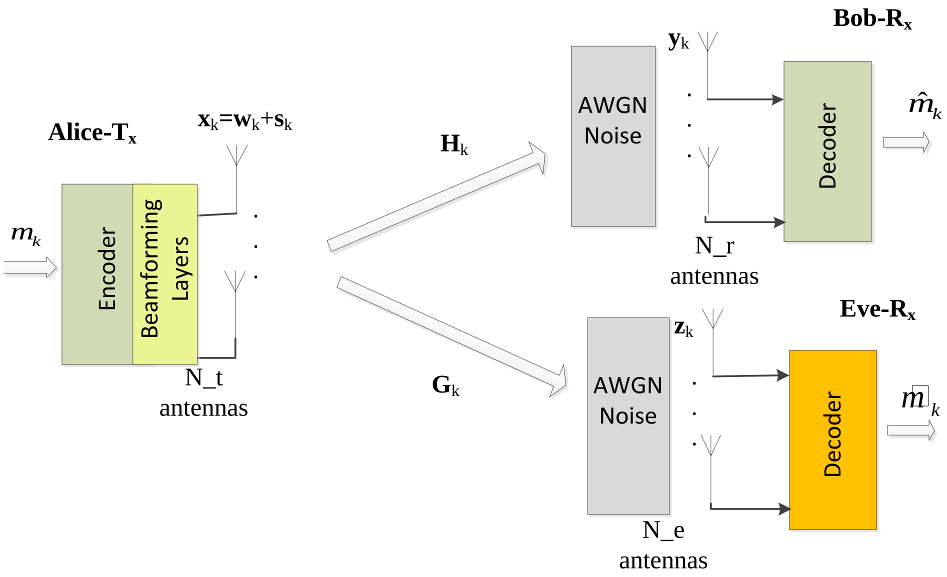
Improve Performance of a Private Ethereum Network: Verification on the Real System

[1] Data Securing Method using Blockchain Technology: From Ethereum 1.0 to Ethereum 2.0, *Technical report*, 2020

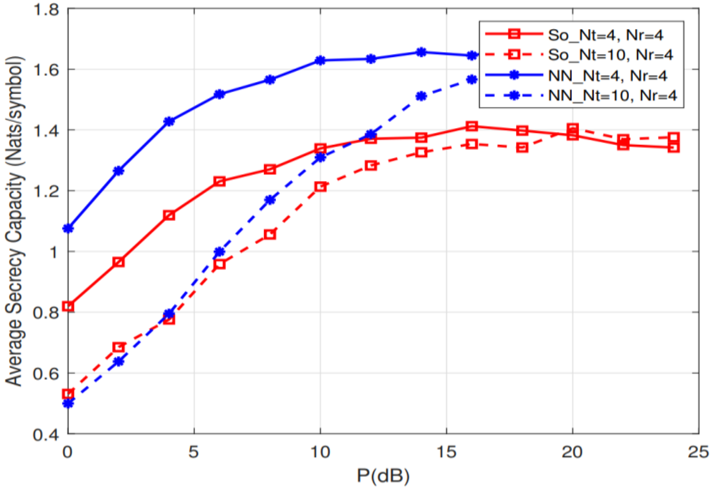
[2] An effective framework of private Ethereum blockchain network for smart grid. *ATC 2021*, Vietnam

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

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



- 2020: Exploited the generalization capability of neural networks to develop the robust FJ scheme with imperfect channel [1].
- 2021: Embedded Deep Learning based beamforming into Autoencoder and MINE-based Friendly Jamming method to maximize secrecy capacity on MIMO wiretap channel when only imperfect CSI is available at transmitter [2].
  - ✓ Better secrecy capacity compared to the conventional method regarding CSI error at the transmitter
  - ✓ Lower complexity (floating-point operations/ FLOPs) of the proposed method compared to conventional methods



Secrecy rate versus transmit power.

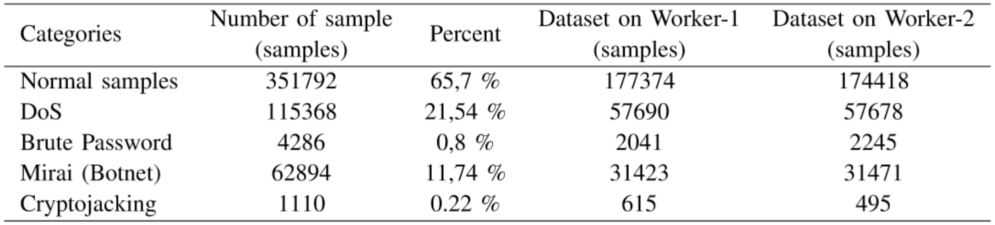
[1] Autoencoder based Friendly Jamming, *WCNC 2020* , Seoul, Korea

[2] Learning based Friendly Jamming with Imperfect CSI for Security in MIMO Wiretap Channel, *IEEE Transactions on Communications*, 2021 (to submit in December)

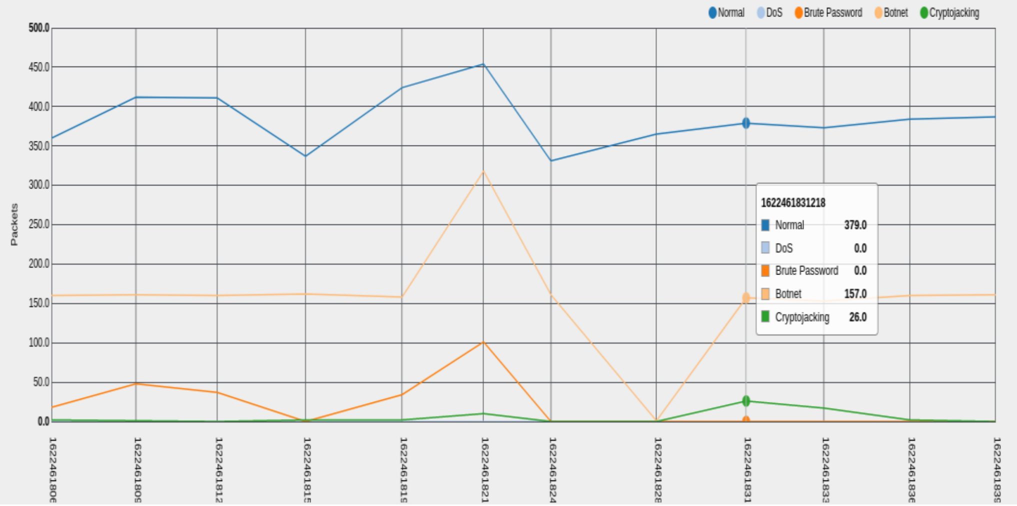
Project Activities & Results: Technological - Task 7 (UET, NTU, UTS)

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

- 2020: Built several system models to implement a testbed of blockchain for smart grid based on smart meter and beaglebone black [1].
- 2021: Built an Industrial IoT cyber-attack dataset and deployed a DL model into the IoT Gateways.
  - ✓ Sep 2021: Received 2 IoT Gateways and starter kits.
  - ✓ Deployed Industrial IoT cyber-attacks on our IoT network and extracted their properties in a dataset [1].
  - ✓ Implemented a collaborative learning-based deep belief network [2] to identify attacks on our collected dataset and monitor the results.
- 2022: To expand the system with the the full network (with 2 new IoT gateways and related devices) and test with various scenarios in the smart factory.



Categories	Number of sample (samples)	Percent	Dataset on Worker-1 (samples)	Dataset on Worker-2 (samples)
Normal samples	351792	65,7 %	177374	174418
DoS	115368	21,54 %	57690	57678
Brute Password	4286	0,8 %	2041	2245
Mirai (Botnet)	62894	11,74 %	31423	31471
Cryptojacking	1110	0.22 %	615	495



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

[2] Collaborative Learning Model for Cyberattack Detection Systems in IoT Industry 4.0, *WCNC 2020,* Seoul, Korea.

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, TV Khoa, LV Nguyen, 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, YM Saputra, DT Hoang, NL Trung, DN Nguyen, NV Ha, 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, TD Tuyen, NL Trung, NV Ha	VNU-UET	IEEE Wireless Communications and Networking Conference	May 2020	Seoul, South Korea
4	An effective framework of private ethereum blockchain networks for smart grid [Task 5]	DH Son, TTT Quynh, TV Khoa, HT Dinh, N Linh Trung, NV Ha, D Niyato, DN Nguyen, E Dutkiewicz	VNU-UET, UTS, NTU	2021 International Conference on Advanced Technologies for Communications (ATC) [Best student paper award]	Oct 2021	Ho Chi Minh, Vietnam

❖ 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

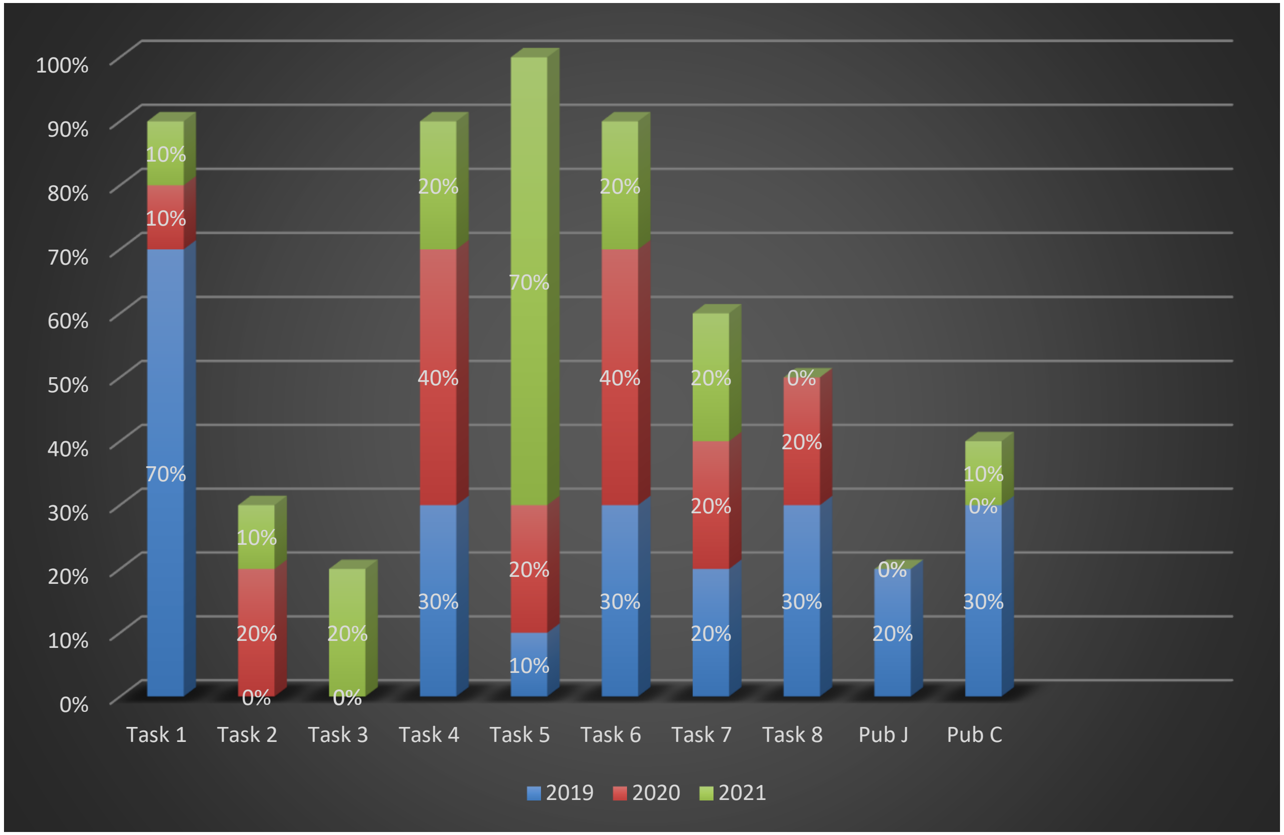
Project Activities: Budget

No.	Title	Period & venue	Yen	US$
1	2018 Forum Travel expense: 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 Travel expense: 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 Travel expense: Takeshi Takahashi, NICT	2019/3/26-28 Hanoi	¥104,500	$926.34
6	Registration for WCNC 2020	2020/5/25-28	¥35,158	$335
7	Equipment	2021/9/15 Hanoi	¥3,238,757	$30,860
Total NICT			¥4,419,677	$**41,415.91**

Future works in 2022

1. **Scientific development**
   - Task 1: Complete by aggregating and analyzing the advantages and disadvantages of exist cybersecurity risks assessments standards
   - Task 2: Complete to develop the methods to classify the risk for I4
   - Task 3: Complete to deploy the website to identify the risks for smart factory.
   - ~~Task 4: Completed applying the transfer learning model for cyberattack detection of IoT Network~~
     - ✓ Publication to be done.
   - ~~Task 5: Develop an unprecedented data securing method using blockchain technology~~
   - ~~Task 6: Show the capabilities of Deep learning based approaches to deal with channel estimation error to security communication~~.
     - ✓ Publication to be done.
2. **Technological Development & Experiments**
   - Task 7: Implement the completed testbed system for I4.
3. **Networking**
   - ~~Task 8: Annual Workshops and Exhibitions on Cyber-Security~~

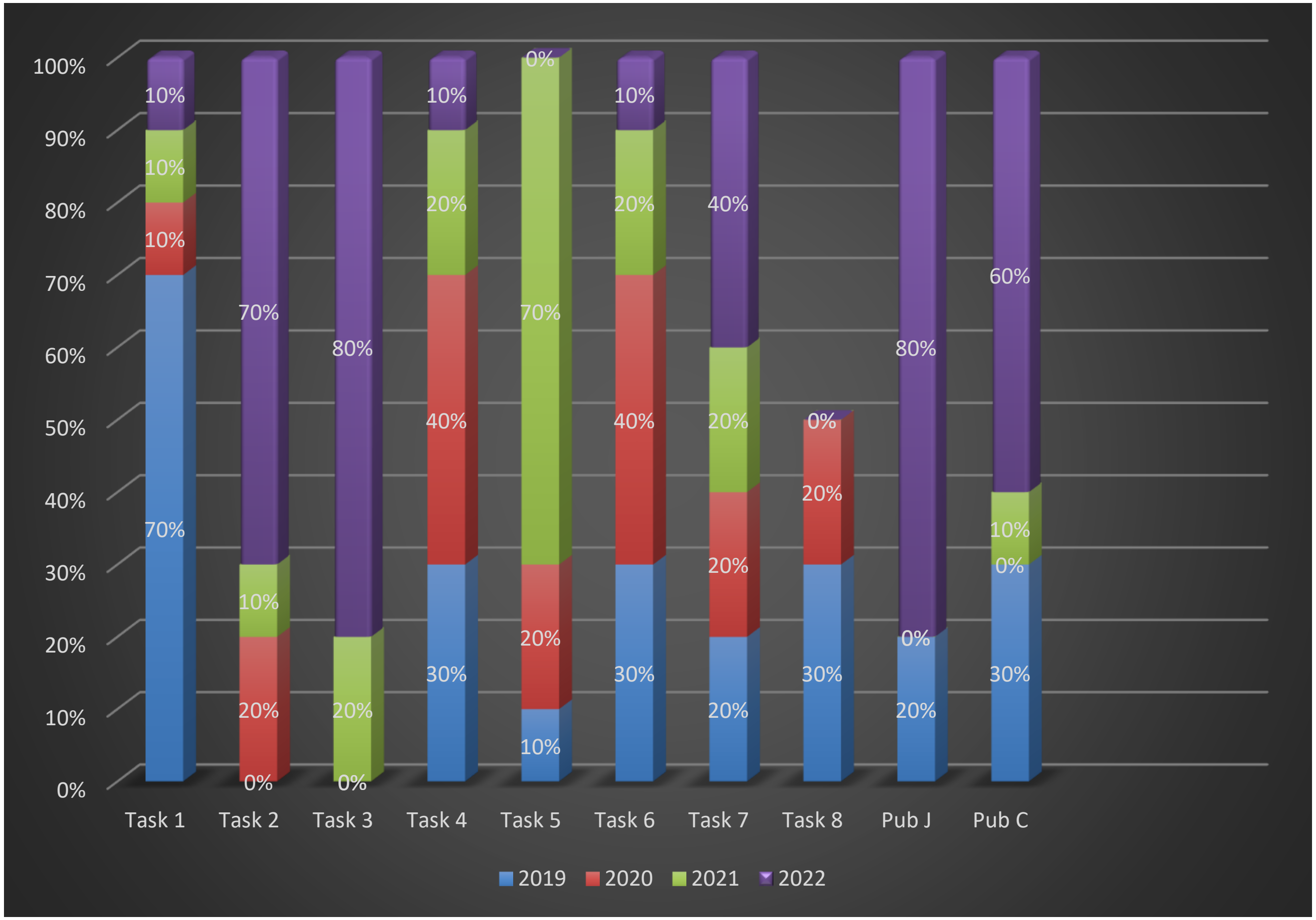
Conclusion: 2021



- ❖ Slow progress due to the outbreak of Covid-19
- ❖ Scientific: security solutions developed in detail
- ❖ Technological: basic design done
- ❖ Budget: equipment purchased (with big delay due to Covid); other plans could not be implemented (due to Covid)

Cyber-security in Industry 4.0, VNU (Vietnam), NTU (Singapore), UTS (Australia)

Future: 2022



- To complete the project
- Scientific: method and website for risk assessment to be completed
- Technological: to complete the main testbed (all equipment purchased)
- Publication: 2 main manuscripts to submit and revise

Thank you!

ĐẠI HỌC CÔNG NGHỆ

AVITECH
Advanced Institute of Engineering and Technology

VNU University of Engineering and Technology

NANYANG TECHNOLOGICAL UNIVERSITY
SINGAPORE

UTS
UNIVERSITY OF TECHNOLOGY, SYDNEY