2018 PROJECT

Cyber-Attack Detection and Information Security for Industry 4.0

FINAL REPORT

November 2022

ĐẠI HỌC CÔNG NGHỆ

UTS
UNIVERSITY OF TECHNOLOGY, SYDNEY

NANYANG TECHNOLOGICAL UNIVERSITY
SINGAPORE

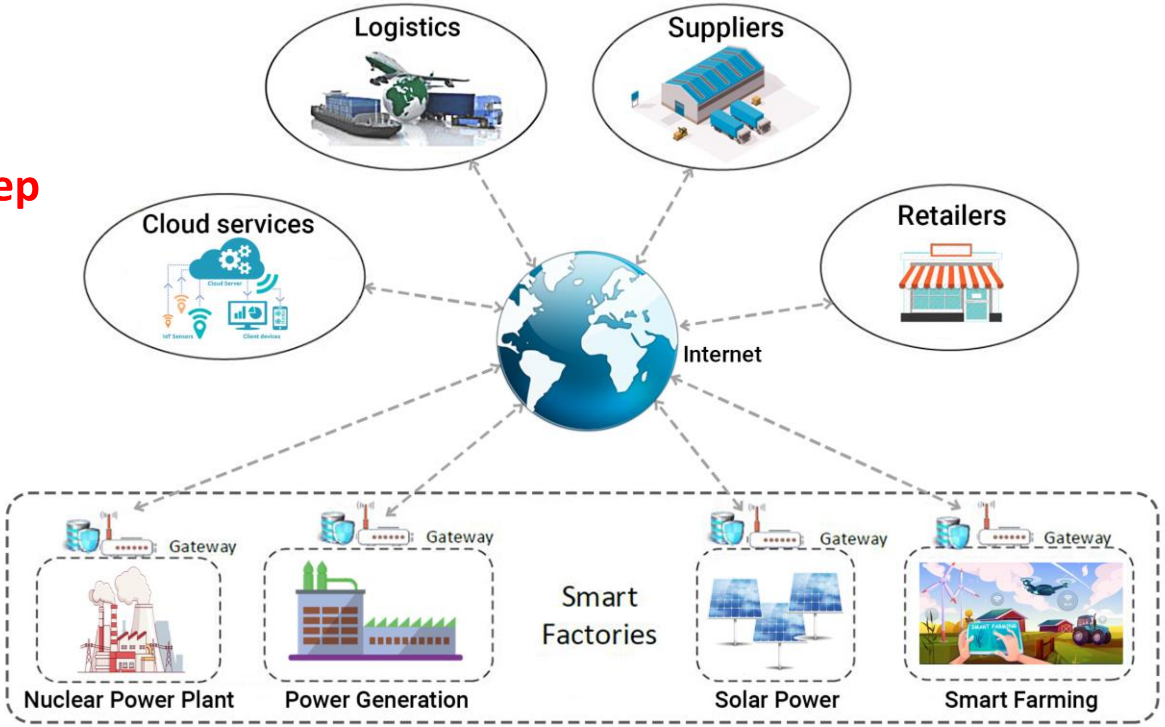
Project: Cyber-Attack Detection and Information Security for Industry 4.0

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 associate member:**

1. VNU-UET (Vietnam): Do Hai Son (M.Sc. Student)

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

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

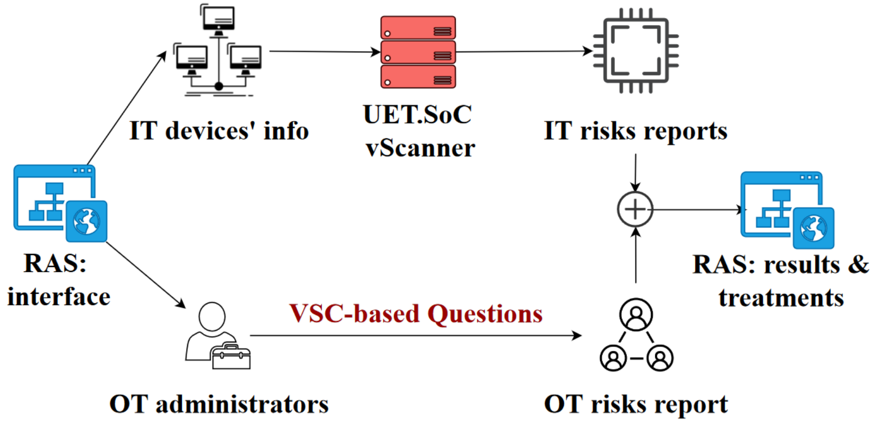
Project Activities & Results: Scientific - Tasks 1, 2, 3 (UET)

Research problem 1: Framework for Cyber Risk Assessment for Industry 4.0 and Recommendations for Vietnam

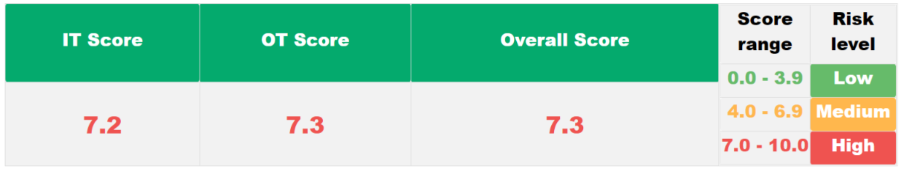
❖ We provided a brief review of methodologies and existing standards used for cyber risk assessment, primarily focusing on OT and recommendations for improving cyber risk assessment for information technology (IT) and operation technology (OT) systems in Industry 4.0 in Vietnam.

❖ We proposed a possible framework for Industrial IoT (IIoT) risk assessment in Vietnam. The proposed framework considers IT, OT, and IIoT system.

❖We built an experiment that simulates an IIoT network and compare with several existing frameworks. The results show that our method gives the same severity level as OWASP.



Proposed framework for RAS of IIoT.



IT Score	OT Score	Overall Score	Score range	Risk level
			0.0 - 3.9	Low
7.2	7.3	7.3	4.0 - 6.9	Medium
			7.0 - 10.0	High

Overall scoring risk assessment from our website.

[1] “A New Framework for Cyber Risk Assessment for Industry 4.0 and Recommendations for Vietnam”, *REV J. Electronics and Communications*, 2022. [under review]

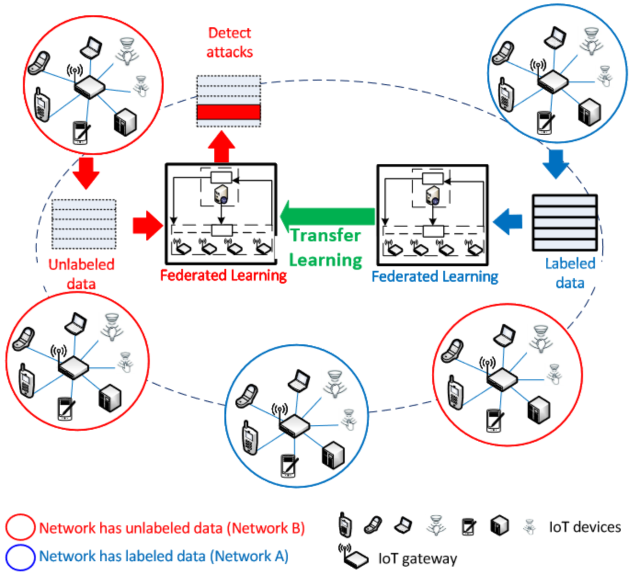
Project Activities & Results: Scientific - Task 4 (UET, UTS)

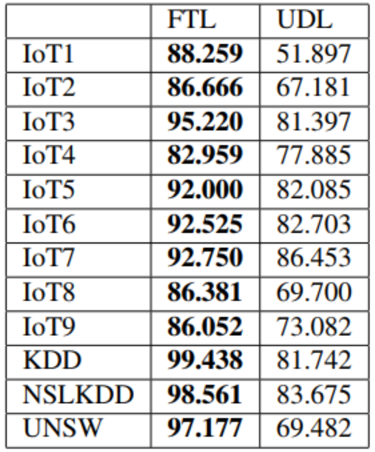
Research problem 2: Collaborative Learning Model for Cyberattack Detection Systems in IoT Networks

❖ We proposed a novel collaborative learning framework that can effectively detect cyberattacks in decentralized IoT systems, by combining the strengths of federated learning (FL) and transfer learning (TL).

❖ We proposed an effective transfer learning approach that can allow the deep learning model from the rich-data network to transfer useful knowledge to the low-data network even they have different features for cyberattack detection in IoT networks.

❖ We performed extensive experiments on recent real-world datasets including N-BaIoT, KDD, NSL-KDD, and UNSW to evaluate the performance of the proposed collaborative learning framework.





	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

[2] “Collaborative Learning Model for Cyberattack Detection Systems in IoT Industry 4.0”, *IEEE Wireless Communications and Networking Conference*, Seoul, Korea, 2020.

[3] “Deep Transfer Learning: A Novel Collaborative Learning Model for Cyberattack Detection Systems in IoT Networks”, *IEEE Internet of Things Journal*, 2022.

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

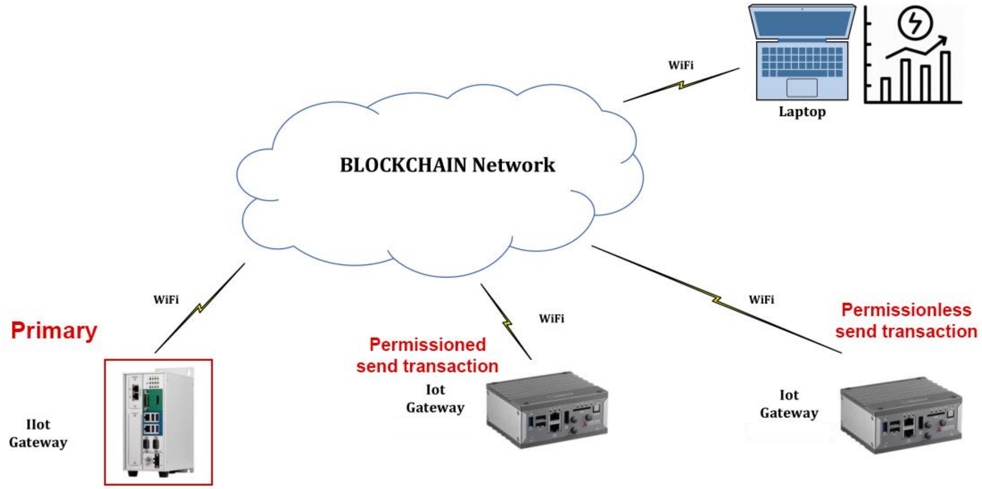
Research problem 3: Framework of Private Ethereum Blockchain Networks for Smart Grid

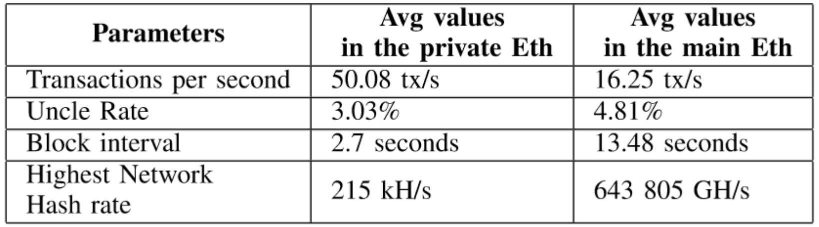
❖ We provided a survey on consensus mechanisms and mining strategy management in blockchain networks.

❖ We developed a practical Ethereum-based smart grid with essential hardware in a home electrical system.

❖ We proposed a smart contract for authentication in a securely multi-devices system.

❖ We 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 real System

[4] "A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks", *IEEE Access*, 2019.

[5] "An effective framework of private Ethereum blockchain networks for smart grid", *International Conference on Advanced Technologies for Communications, 2021*. [Best student paper award]

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

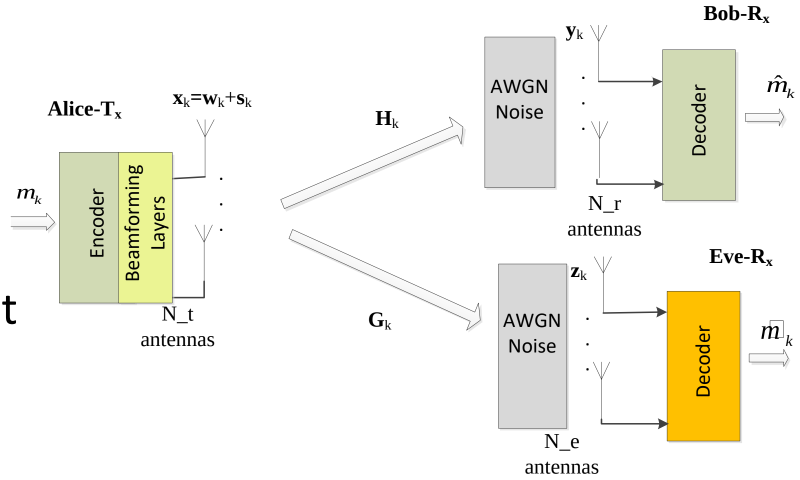
Research problem 4: Learning-based Friendly Jamming with Imperfect CSI for Security in MIMO Wiretap Channel

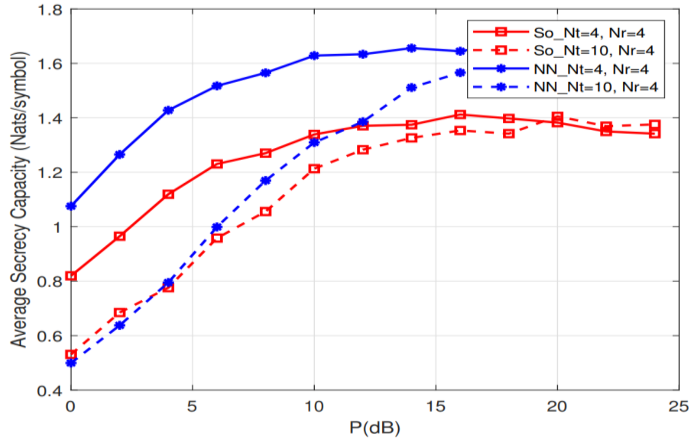
❖ We presented an SDR-based implementation of NC under the TWR model and two extended network models for multimedia transmission and cognitive radio, respectively.

❖ We leveraged the generalization features of neural networks to develop a MIMO friendly-jamming (FJ) scheme that is robust to imperfect channel state information (CSI) due to issues such as time varying channels or the limited number of pilots.

❖ We leveraged MFJ based on mutual information neural estimation (MINE) to demonstrate that it is possible to achieve a security performance comparable with the conventional FJ method without CSI.

❖ We also investigated the relationship between the MIMO secrecy optimization and detection tasks. In other words, maximizing secrecy rate and minimizing block/symbol error rate can be jointly optimized.





Secrecy rate versus transmit power.

[6] "Network Coding with Multimedia Transmission: A Software-Defined-Radio based Implementation", *Int'l Conf. Recent Advances in Signal Process., Telecom. and Comp.*, 2019, Vietnam.
[7] "Autoencoder based Friendly Jamming", *IEEE Wireless Communications and Networking Conference 2020*, Seoul, Korea.
[8] "Learning based Friendly Jamming with Imperfect CSI for Security in MIMO Wiretap Channel", *IEEE Transactions on Communications*, 2021 [under revision].

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

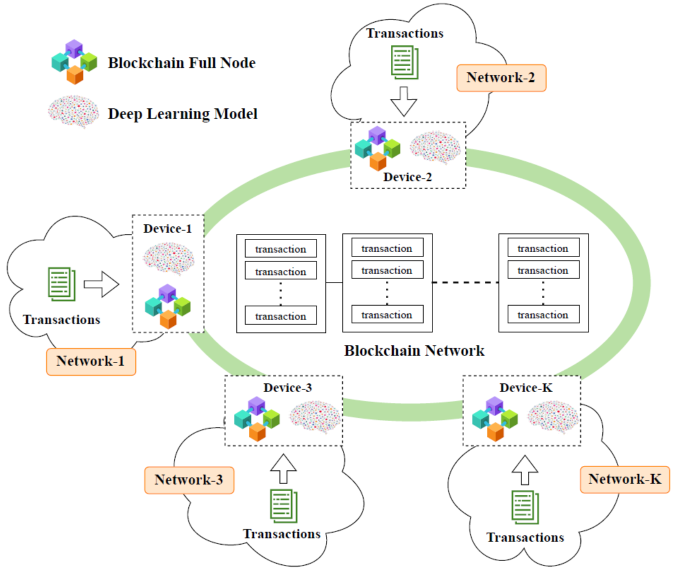
Research problem 5: Collaborative Learning for Cyberattack Detection in Blockchain Networks

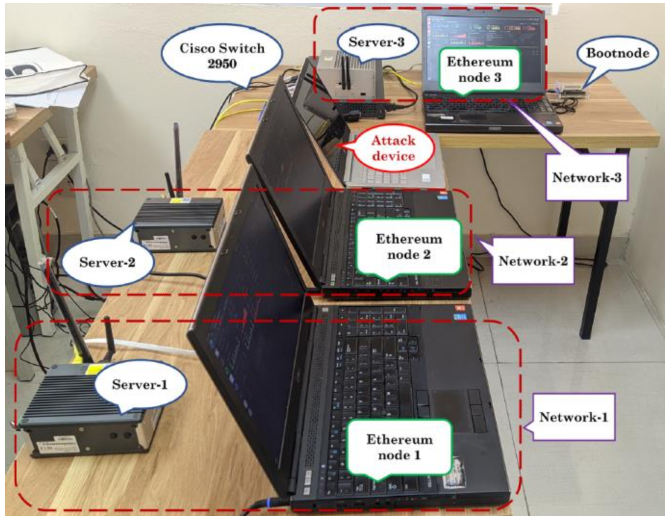
❖ We set up experiments in our laboratory to build a private blockchain network (BNaT) with the aims of not only obtaining real blockchain datasets, but also testing our proposed learning model in a real-time manner.

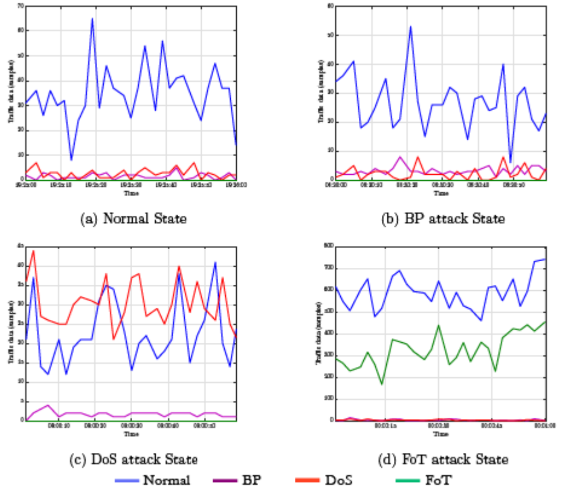
❖ We built an effective tool named Blockchain Intrusion Detection (BC-ID) to collect data in the blockchain network.

❖ We proposed a collaborative decentralized learning model to not only improve the accuracy of identifying attacks, but also effectively deploy in decentralized blockchain networks.

❖ We performed both intensive simulations and real-time experiments to evaluate our proposed framework.







(a) Normal State

(b) BP attack State

(c) DoS attack State

(d) FoT attack State

[9] “Collaborative Learning for Cyberattack Detection in Blockchain Networks”, *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 2022 [under review].

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

Publications

❖ 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
2	Deep transfer learning: A novel collaborative learning model for cyberattack detection systems in IoT networks [Task 4]	TV Khoa, DT Hoang, NL Trung, CT Nguyen, TTT Quynh, DN Nguyen, NV Ha, E Dutkiewicz	VNU, UTS	IEEE Internet of Things Journal	IEEE	Accepted, 2022
3	Collaborative Learning for Cyberattack Detection in Blockchain Networks [Task 7]	TV Khoa, DH Son, DT Hoang, NL Trung, TTT Quynh, DN Nguyen, NV Ha, E Dutkiewicz	VNU, UTS	IEEE Transactions on Systems, Man, and Cybernetics: Systems	IEEE	Submitted, 2022
4	A New Framework for Cyber Risk Assessment for Industry 4.0 and Recommendations for Vietnam [Task 1,2,3]	BM Tuan, TV Khoa, DH Son, NL Trung, TTT Quynh, NN Hoa, NV Ha	VNU, UTS	REV Journal on Electronics and Communications	REV	Submitted, 2022
5	Learning-based Friendly Jamming with Imperfect CSI for Security in MIMO Wiretap Channel [Task 6]	BM Tuan, NL Trung, DN Nguyen, M Krunz, NV Ha, DT Hoang, E Dutkiewicz	VNU, UTS	IEEE Transactions on Communications	IEEE	Submitted, 2021

Thank you!

ĐẠI HỌC CÔNG NGHỆ

UTS UNIVERSITY OF TECHNOLOGY, SYDNEY

NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE