International Journal of Network Security

(http://ijns.femto.com.tw/)

Special Issue (SI) on **Machine Learning/ Deep Learning for Cybersecurity Analytics**

Cybersecurity has become more and more important in recent years since 5th generation mobile networks and Internet of things are developing rapidly. The low latency and real-time transmission for networks bring a big challenge to the fields of intrusion detection, risk analytics and threat defense. Additionally, due to sophistication and scalability of the current network system, cybersecurity maintenance and hacker tracking conducted by traditional technologies may cause obvious problems of performance and accuracy. Some novel attacks or new variants of malicious behaviors are not efficiently detected by most existing defensive tools because these attacks or behaviors evade detection by using network traffic obfuscation, or even employ adversarial machine learning techniques for further exploitations. It is necessary to develop more robust detection, tracing and analysis models by leveraging machine learning, deep learning or advanced analytics approaches to enhance security in network. This special issue is aiming to draw attention to the latest research progress on machine learning-based or deep learning-based defensive and offensive techniques for cybersecurity analytics, and collect high-quality research studies on various applications of machine learning/ deep learning to cybersecurity.

Interesting topics include, but are not limited to:

- Vulnerability analysis of machine learning and deep learning models
- Cybersecurity in artificial intelligence
- Machine learning/ deep learning based intrusion detection and anomaly detection in network security
- Privacy preserving machine learning
- Machine learning/ deep learning for malware detection
- Machine learning/ deep learning for forensic analysis in cybersecurity
- Machine learning, deep learning and big data analytics for network management
- Adversarial machine learning
- Deep learning-based automated threat recognition
- Machine learning-based defense and response
- Generative adversarial network for cybersecurity

- Machine learning and deep learning for cloud security
- Machine learning and deep learning for IoT security

Manuscript Submission Information

Articles must be written in good English. Once a manuscript is accepted, the submitted article will be simultaneously reviewed and published elsewhere (except conference proceedings papers). All the submitted papers will go through the review process. The author should submit your Word or pdf file to the Guest editors via Email of wangch@mail.ncyu.edi.tw by the corresponding guest editor Prof. Chih-Hung Wang. The Email subject is asked to offer the name of submitting to SI: "**Machine Learning/ Deep Learning for Cybersecurity Analytics".**

Important dates

- Paper submission due: October 31, 2020
- First notification: January 31, 2021
- Revision submission: February 21, 2021
- Final decision: March 8, 2021

Guest Editors:

Prof. Chih-Hung Wang National Chiayi University, Taiwan wangch@mail.ncyu.edi.tw	Prof. Kouichi Sakurai Kyushu University, Japan sakurai@inf.kyushu-u.ac.jp
Prof. Kuo-Yu Tsai Feng Chia University, Taiwan kytsai@fcu.edu.tw	