IEEE TDSC Special Issue on AI/ML for Secure Computing

Artificial Intelligence (AI) and machine learning (including deep learning) have been widely studied in both academia and industry to achieve enhanced security and privacy of service computing (including cloud computing, Internet services, and Internet-of-Things). For instance, AI and machine learning algorithms can be deployed to detect sophisticated attacks, e.g., online abuse, which cannot be easily detected by traditional detection approaches like rule-based detection. It is important to investigate how they can be implemented to achieve a good trade-off between detection accuracy and learning cost. Meanwhile, AI and machine learning themselves are vulnerable to security and privacy concerns: for example, data used by them may leak sensitive information, thus compromising users' privacy. Thus, in some application scenarios, how to leverage the capability of AI and machine learning algorithms for enhanced secure service computing while protecting the user's privacy remains a challenging problem. Recent research has demonstrated the negative impact of other adversarial behavior: adversarial noise injected during the training phase ("poisoning") of AI and machine learning algorithms result in incorrect models; adversaries can construct "adversarial examples" that cause properly trained models to infer incorrect results. The security and robustness of AI and machine learning algorithms also have a strong impact on security and privacy of service computing.

The scope of this special issue is addressing the challenges of applying AI and machine learning algorithms to secure computing. In order to implement them in practice, a big obstacle for research is to have enhanced security while not impacting users' privacy.

In this special issue, we are seeking novel approaches and unpublished work related to AI and machine learning for enhanced security and privacy protection of service computing. In particular, we would like to focus on recent trends in adversarial machine learning, reinforcement learning, and privacy-preserving machine learning to improve the security. We solicit experimental, conceptual, and theoretical contributions on the following topics related to AI and machine learning for enhanced security and privacy of service computing:

- Attacks on machine learning and defense
- Generative Adversarial Networks (GAN) for attacks and defenses
- Deep learning for enhanced security and privacy
- Enhanced security of service computing with reinforcement learning
- Adversarial machine learning for security and privacy of computing
- Adversarial examples: attacks and defenses
- Robust learning for enhanced security and privacy in service computing
- Learning for malware analysis and detection
- Learning for anomaly and intrusion detection
- Learning for critical infrastructure security
- Learning for cryptanalysis
- Learning for spam detection
- Learning for secure online social networks

Important Dates

- Manuscript Submission Deadline: October 1, 2019
- First Round of Reviews: December 15, 2019
- Revised Papers Due: January 31, 2019
- Final Notification: March 31, 2020
- Final Manuscript Due: April 15, 2020

Submission Guidelines

Papers submitted to this special issue for possible publication must be original and must not be under consideration for publication in any other journal or conference. TDSC requires meaningful technical novelty in submissions that extend previously published conference papers. Extension beyond the conference version(s) is not simply a matter of length. Thus, expanded motivation, expanded discussion of related work, variants of previously reported algorithms, incremental additional experiments/simulations, may provide additional length but will fall below the line for proceeding with review. Submissions must be directly submitted via the IEEE TDSC submission web site at https://mc.manuscriptcentral.com/tdsc-cs.

Guest Editors

- N. Asokan, Aalto University, Finland, asokan@acm.org
- Pan Hui, University of Helsinki, Finland & Hong Kong University of Science and Technology, Hong Kong, panhui@cse.ust.hk
- Qi Li, Tsinghua University, China, qi.li@sz.tsinghua.edu.cn
- Ravi Sandhu, The University of Texas at San Antonio, ravi.sandhu@utsa.edu