Call for Papers

ISA Transactions Special Issue on Security and Privacy of AI-based Automation Systems

Guest Editors: Professor Yang Xiang, Swinburne University of Technology, Australia and Professor Elisa Bertino, Purdue University, USA

I. AIMS AND SCOPES

Artificial Intelligence (AI) has recently been established as the key enabler in diverse technologies with many real-world applications such as self-driving cars, healthcare, energy, digital finance, cybersecurity, and advanced manufacturing. However, along with the rapid growth in AI systems and hardware in the last decade, there are emerging threats targeting AI systems, at both the software and hardware layers. Threats, such as adversarial examples and privacy inference attacks, will cause AI models to either malfunction or inadvertently compromise private and sensitive data. For example, in advanced manufacturing, imperfect AI models may lead to erroneous product condition monitoring systems, which may result in significant financial loss. It is therefore critical to identify the AI vulnerabilities and propose effective defense measures to protect AI models, systems and applications.

This special issue aims to advance the security of AI-based automation systems used in different domains and further promote research activities in utilizing AI in a secure and reliable way. The Special Issue seeks original theory- and application-driven studies to address the emerging security and privacy issues of AI models, systems and applications.

II. TOPICS OF INTEREST

In this special issue, we are calling for novel approaches related to AI security and privacy for both software and hardware within the subtopics listed herein. We solicit experimental, conceptual, and theoretical contributions on the following topics related to AI security and privacy. The topics include but are not limited to:

- AI based attacks and defenses
- Reliability and safety of AI models
- AI for enhancing security and privacy
- Adversarial attacks and mitigation
- Privacy issues in AI
- AI model stealing attacks and defenses
- AI Hardware Attacks
- Attacks on embedded AI
- Side-channel attacks on AI models
- Attacks and defenses on medical AI
- Zero-day attack and vulnerability detection using deep learning
- Advanced persistent threat (APT) detection in AI systems

III.SUBMISSION GUIDELINES

Authors should prepare their manuscripts according to the "Instructions for Authors" guidelines of "ISA Transactions" outlined at the journal website https://www.elsevier.com/journals/isa-transactions/0019-0578/guide-for-authors. All papers will undergo blind peer-review in accordance with the journal regular review procedure. Each

submission should clearly demonstrate evidence of benefits to society or large communities. Originality and impact on society, in combination with a media-related focus and innovative technical aspects of the proposed solutions will be the major evaluation criteria.

All manuscripts and any supplementary material should be submitted electronically through https://www.editorialmanager.com/isatrans/default.aspx. Only original and unpublished papers will be considered. Select article type "**SI: Security of AI-based Sys**" and nominate the managing editor as the Deputy Editor-in-Chief Professor Q.-G. Wang.

IV. IMPORTANT DATES

- Submission Deadline: 30 November 2022
- First Round Notification: 31 January 2023
- Revised Manuscript Due: 31 March 2023
- Notification of Acceptance: 30 April 2023
- Final Manuscript Due: 31 May 2023
- Anticipated Publication: 31 July 2023

V. GUEST EDITORS

Professor Yang Xiang, PhD, FIEEE
Dean of Digital Research
Swinburne University of Technology
Australia
Email: yxiang@swin.edu.au

Professor Elisa Bertino, PhD, FIEEE, FACM, FAAAS
Samuel D. Conte Professor of Computer Science
Director of Cyber Space Security Lab
Purdue University
United States of America
Email: bertino@purdue.edu