Special Issue

Advances in Secure AI: Technology and Applications

Message from the Guest Editors

Artificial intelligence (AI) is a technology that enables us to identify solutions to complex problems using relatively simple learning mechanisms in a data-driven fashion. Due to the recent success and advances in AI techniques such as computer vision and natural language processing, many intelligent services integrate AI, especially in mission-critical applications dealing with complex systems such as autonomous vehicles, environmental monitoring, and cybersecurity. However, we still do not understand the complete characteristics of AI models and learning techniques; therefore, it has become an urgent call for both theoreticians and partitioners to investigate robust, timely, explainable, and trustworthy AI to avoid unforeseen malfunction of AI-based services. This Special Issue aims to address the latest advances in the techniques and applications of secure AI. Potential topics include but are not limited to the following:

- Adversarial attack and defense techniques;
- AI model stealing attack and defense techniques;
- Data poisoning (AI backdoor/trojan) attack, detection, and defense;
- Explainable AI (XAI) techniques and applications;

Guest Editors

Dr. Sangkyun Lee
School of Cybersecurity, Korea University, Seoul 02841, Republic of Korea

Prof. Dr. Yunheung Paek
Department of Electrical and Computer Engineering, Seoul National University, Seoul 08826, Korea

Deadline for manuscript submissions

closed (30 November 2022)

Applied Sciences

an Open Access Journal by MDPI

Impact Factor 2.5
CiteScore 6.1

mdpi.com/si/123436

Applied Sciences
Editorial Office
MDPI, Grosspeteranlage 5
4052 Basel, Switzerland
Tel: +41 61 683 77 34
applsci@mdpi.com

mdpi.com/journal/applsci

Applied Sciences

an Open Access Journal by MDPI

Impact Factor 2.5
CiteScore 6.1

mdpi.com/journal/applsci

MDPI

About the Journal

Message from the Editor-in-Chief

As the world of science becomes ever more specialized, researchers may lose themselves in the deep forest of the ever increasing number of subfields being created. This open access journal *Applied Sciences* has been started to link these subfields, so researchers can cut through the forest and see the surrounding, or quite distant fields and subfields to help develop his/her own research even further with the aid of this multi-dimensional network.

Editor-in-Chief

Prof. Dr. Giulio Nicola Cerullo
Dipartimento di Fisica, Politecnico di Milano, Piazza L. da Vinci 32, 20133 Milano, Italy

Author Benefits

Open Access:

free for readers, with article processing charges (APC) paid by authors or their institutions.

High Visibility:

indexed within Scopus, SCIE (Web of Science), Ei Compendex, Inspec, Embase, CAPlus / SciFinder, and other databases.

Journal Rank:

JCR - Q2 (Engineering, Multidisciplinary) / CiteScore - Q1 (Fluid Flow and Transfer Processes)