Special Issue

Security and Privacy in Artificial Intelligence: Technology, Applications, and Challenges

Message from the Guest Editors

Artificial intelligence (AI) technology is widely integrated into applications such as autonomous driving, healthcare, and language processing. Although AI technology, especially deep learning, holds tremendous promise, it faces significant security risks regarding adversarial robustness, model backdoors, fairness, and privacy. This Special Issue will consolidate research efforts to identify security and privacy challenges in AI systems, develop secure and robust AI algorithms and protocols, and create fairness- and copyright-preserving techniques. We invite prospective authors to submit original research contributions on topics including, but not limited to, the following:

- Adversarial Attacks and Defenses for AI;
- Backdoor Attacks and Defenses for AI;
- Data Poisoning Attacks and Defenses for AI;
- Jailbreak Attacks and Defenses for Large Models;
- The hallucination of Large Language Models;
- AIGC Detection and Attribution;
- Copyright Issues in AI;
- Privacy Issues in AI;
- Fairness Issues in AI;
- Model Interpretability and its Applications in AI Security.

Guest Editors

Dr. Yiming Li

Dr. Xiaojun Jia

Dr. Zhengyu Zhao

Deadline for manuscript submissions

closed (30 September 2025)

Applied Sciences

an Open Access Journal by MDPI

Impact Factor 2.5
CiteScore 5.5

mdpi.com/si/214643

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 5.5

mdpi.com/journal/applsci

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, CAPlus / SciFinder, and other databases.

Journal Rank:

JCR - Q2 (Engineering, Multidisciplinary) / CiteScore - Q1 (General Engineering)

MDPI