applied sciences

IMPACT FACTOR 2.5

CITESCORE 5.5

an Open Access Journal by MDPI

Security and Privacy in Machine Learning and Artificial Intelligence (AI)

Guest Editors:

Dr. Tao Jiang

Dr. Yuling Chen

Prof. Dr. Yilei Wang

Prof. Dr. Huiyu Zhou

Deadline for manuscript submissions:
closed (20 June 2025)

Message from the Guest Editors

In the past decade, ML&AI techniques have been increasingly deployed for automated decisions in many critical applications, such as autonomous vehicles, cybersecurity and many more.However, the use of ML&AI in security- and privacy-sensitive domains, where adversaries may attempt to mislead or evade intelligent mechanisms, creates new frontiers for security research.On the one hand, ML&AI technologies, especially deep learning, have been repeatedly proven to suffer from trust and interpretability challenges in the face of various attacks. On the other hand, to overcome the efficiency and application limitation of simple data encryption solutions, new security, and privacy technologies are necessary to exploit. Therefore, how to ensure the security and privacy of the systems enabled by ML&AI techniques is becoming urgent and challenging.

ML&AI Theoretical topics:
- ML&AI interpretability
- Adversarial learning

Application topics:
- Evasion attacks and defenses
- AI-based detection techniques, e.g. intrusion detection, anomaly detection, fraud detection, malicious codes, network anomalous behaviors, etc.

applied sciences

IMPACT FACTOR 2.5

CITESCORE 5.5

an Open Access Journal by MDPI

Editor-in-Chief

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

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.

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 (General Engineering)

Contact Us

Applied Sciences Editorial Office
MDPI, Grosspeteranlage 5
4052 Basel, Switzerland

Tel: +41 61 683 77 34
www.mdpi.com

mdpi.com/journal/applsci
applsci@mdpi.com
𝕏@Applsci