Special Issue

Security and Privacy in AI: Human Interaction, Awareness and Protection

Message from the Guest Editors

With the rapid rise of AI in sectors like healthcare, finance, education, and governance, ensuring the security and privacy of these systems is more important than ever, especially in areas involving human interaction. This Special Issue focuses on human-centric approaches to AI security, aiming to enhance user trust and protect personal data. We welcome original research and review articles on both technical solutions and awareness-based strategies. Topics include:

- Adversarial threat defense in AI systems
- Privacy-aware machine learning and data handling
- Human-in-the-loop security approaches
- AI privacy education and awareness
- Explainable and interpretable AI (XAI)
- Trust frameworks for human–AI collaboration
- Real-world case studies

Help us shape a secure and trustworthy AI future. Submit your work today!

Guest Editors

Dr. Xuechao Yang

Dr. Chenhao Xu

Dr. Jack Li

Prof. Dr. Xun Yi

Deadline for manuscript submissions

30 November 2025

Applied Sciences

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)