Special Issue

Security and Privacy in Artificial Intelligence Systems

Message from the Guest Editors

Artificial Intelligence (AI) has become the core engine driving innovation across diverse domains, including autonomous vehicles, healthcare, finance, and next-generation communication systems. However, the rapid deployment of AI introduces new vectors of security and privacy risks: adversarial attacks against models, data poisoning, model inversion, backdoor threats, and privacy leakage from training data. These vulnerabilities not only compromise system integrity but also raise ethical and regulatory concerns for trustworthy AI adoption. This Special Issue will explore cutting-edge research on security and privacy in AI systems, covering theoretical foundations, algorithmic advances, and practical applications. By focusing on both attack and defense perspectives, as well as privacy-preserving AI frameworks, this Special Issue will provide a comprehensive view of how to build resilient and trustworthy AI ecosystems. Its scope is well aligned with that of *Electronics*, emphasizing digital technologies, system reliability, and user protection.

Guest Editors

Dr. Yangfei Lin

School of Informatics and Engineering, University of Electro-Communications, Tokyo 1828585, Japan

Dr. Qiong Chang

Department of Computer Science, Science Tokyo, Tokyo 152-8550, Japan

Deadline for manuscript submissions

15 May 2026

Electronics

an Open Access Journal by MDPI

Impact Factor 2.6
CiteScore 6.1

mdpi.com/si/258372

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

mdpi.com/journal/electronics

Electronics

an Open Access Journal by MDPI

Impact Factor 2.6
CiteScore 6.1

mdpi.com/journal/electronics

About the Journal

Message from the Editor-in-Chief

Electronics is a multidisciplinary journal designed to appeal to a diverse audience of research scientists, practitioners, and developers in academia and industry. The journal is devoted to fast publication of latest technological breakthroughs, cutting-edge developments, and timely reviews of current and emerging technologies related to the broad field of electronics. Experimental and theoretical results are published as regular peer-reviewed articles or as articles within Special Issues guestedited by leading experts in selected topics of interest.

Editor-in-Chief

Prof. Dr. Flavio Canavero
Department of Electronics and Telecommunications, Politecnico di Torino, 10129 Torino, Italy

Author Benefits

High Visibility:

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

Journal Rank:

JCR - Q2 (Engineering, Electrical and Electronic) / CiteScore - Q1 (Electrical and Electronic Engineering)

Rapid Publication:

manuscripts are peer-reviewed and a first decision is provided to authors approximately 16.8 days after submission; acceptance to publication is undertaken in 2.4 days (median values for papers published in this journal in the first half of 2025).

MDPI