Special Issue

Security and Privacy Evaluation of Machine Learning in Networks

Message from the Guest Editors

Machine learning algorithms have been playing an increasingly important role in many practical computing systems, such as auto-piloting, medicine diagnosis, spam detection, and person reidentification. Meanwhile, such machine learning algorithms are usually confronted with critical threats in an open and adversarial setting. These threats include evasion attack, backdoor attack, model stealth, data leakage and so on, which significantly affect the effectiveness and security of the machine learning systems.

This feature topic will benefit the research community towards identifying challenges and disseminating the latest methodologies and solutions regarding security and privacy evaluation issues in machine learning. The ultimate objective is to publish high-quality articles presenting open issues, delivering algorithms, protocols, frameworks, and solutions for security evaluation in machine learning.

Guest Editors

Dr. Xianmin Wang

Dr. Jing Li

Prof. Dr. Di Wu

Dr. Mingliang Zhou

Deadline for manuscript submissions

closed (15 December 2024)

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 guest-edited 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