Special Issue

Reliable and Secure AI Systems

Message from the Guest Editors

This Special Issue, “Reliable and Secure AI Systems”, aims to address these pressing concerns by compiling innovative research on AI robustness, adversarial machine learning, trustworthy AI, and security-aware AI deployment. Key topics of interest include, but are not limited to, adversarial machine learning including attacks and defenses, adversarial resilience in deep learning, secure federated learning, privacy-preserving AI, ethical AI frameworks, and formal verification techniques for AI systems. This Special Issue additionally seeks to explore novel attack and defense mechanisms against emerging AI threats and ways to make sure that AI systems remain transparent, explainable, and aligned with security best practices.

Guest Editors

Dr. Kassem Kallas
Dr. Reda Bellafqira
Dr. Kashif Ahmad

Deadline for manuscript submissions

31 August 2026

01010
01010
01010

Information

an Open Access Journal
by MDPI

Impact Factor 2.9
CiteScore 6.5

mdpi.com/si/250947

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

mdpi.com/journal/information

MDPI

01010
01010
01010

Information

an Open Access Journal
by MDPI

Impact Factor 2.9
CiteScore 6.5

mdpi.com/journal/information

About the Journal

Message from the Editor-in-Chief

The concept of *Information* is to disseminate scientific results achieved via experiments and theoretical results in depth. It is very important to enable researchers and practitioners to learn new technology and findings that enable development in the applied field.

Information is an online open access journal of information science and technology, data, knowledge and communication. It publishes reviews, regular research papers and short communications. We invite high quality work, and our review and publication processing is very efficient.

Editor-in-Chief

Prof. Dr. Willy Susilo
School of Computer Science and Software Engineering, University of Wollongong, Northfields Avenue, Wollongong, NSW 2522, Australia

Author Benefits

Open Access:

free for readers, with article processing charges (APC) paid by authors or their institutions.

High Visibility:

indexed within Scopus, ESCI (Web of Science), Ei Compendex, dblp, and other databases.

Journal Rank:

JCR - Q2 (Computer Science, Information Systems) / CiteScore - Q2 (Information Systems)