Special Issue

Securing Artificial Intelligence Against Attacks

Message from the Guest Editors

AI has started to permeate many fields and industries with affordable and scalable services. This opens up new attack surfaces and attack vectors, using AI as both a tool for attacks, but also as a target. As currently prominent AI technologies like LLMs and DNNs lack explainability and thus also transparency. Many classical security approaches like penetration testing need to be adapted to this situation, translating the finding of a security-relevant error in an AI system into a fix is generally not possible for many currently employed algorithms. Complex systems like neural networks might increase the attack surface quite drastically, requiring special treatment not only from a technical perspective, but also from a risk management one. This Special Issue is dedicated to research results in the area of security for AI systems. It calls for cutting-edge contributions to fundamental theoretical research as well as its application in practice.

Guest Editors

Prof. Dr. Peter Kieseberg
Institute of IT Security Research, St. Pölten University of Applied Sciences, 3100 St. Pölten, Austria

Prof. Dr. Jungwoo Ryoo
College of Information Sciences and Technology (IST), Penn State University, State College, PA 16801, USA

Deadline for manuscript submissions

31 May 2026

Future Internet

an Open Access Journal by MDPI

Impact Factor 3.6
CiteScore 8.3

mdpi.com/si/241385

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

mdpi.com/journal/futureinternet

Future Internet

an Open Access Journal by MDPI

Impact Factor 3.6
CiteScore 8.3

mdpi.com/journal/futureinternet

About the Journal

Message from the Editor-in-Chief

Future Internet is a fast-growing journal devoted to rapid publications of the latest results in the general areas of computer networking/communications and information systems, with a focus on the Internet of Things, big data and augmented intelligence, smart systems (in terms of technologies, architectures, and applications), network virtualization, edge/fog computing, and cybersecurity. Both theoretical and experimental papers are welcome. Every year, *Future Internet* also features Special Issues dedicated to specific topics within the journal's scope.

Editor-in-Chief

Prof. Dr. Gianluigi Ferrari
Department of Engineering and Architecture, University of Parma, Parco Area delle Scienze, 181/A, 43124 Parma, Italy

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, Inspec, and other databases.

Journal Rank:

JCR - Q2 (Computer Science, Information Systems) / CiteScore - Q1 (Computer Networks and Communications)

MDPI