Special Issue

Security and Privacy in AI-Powered Systems

Message from the Guest Editors

This Special Issue seeks to explore innovative solutions for enhancing the security and privacy of AI-powered systems. Topics of interest include security vulnerabilities, privacy-preserving AI techniques, adversarial machine learning defenses, secure deployment practices, and legal or ethical considerations. We aim to enhance interdisciplinary discussions that address both technical and societal dimensions, contributing to the development of robust, privacy-aware AI systems. Key topics of interest include, but are not limited to, the following:

- Security vulnerabilities in AI algorithms and models;
- Privacy-preserving techniques in AI-powered data analytics;
- Secure and trustworthy AI model deployment;
- Adversarial machine learning and defenses;
- Ethical and legal considerations in AI security and privacy;
- Real-world case studies of securing AI-powered applications.

Guest Editors

Dr. Bo Liu

School of Computer Science, University of Technology Sydney, Sydney, NSW 2007, Australia

Prof. Dr. Tianqing Zhu

Faculty of Data Science, City University of Macau, Macau 999078, China

Deadline for manuscript submissions

20 June 2026

Future Internet

an Open Access Journal by MDPI

Impact Factor 3.6
CiteScore 8.3

mdpi.com/si/222973

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

mdpi.com/journal/futureinternet

MDPI

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)