Journal of Cybersecurity and Privacy

MDPI

Message from the Editor-in-Chief

Computing and communication technologies are at the heart of societal advancements in transportation, production and manufacturing, logistics, healthcare, utility, recreation, social, and many other domains. While these advancements offer profound benefits, they also pose new security and privacy challenges that can undermine these advancements. It is possible now for adversaries to exist anywhere and at any time in the data life cycle. Adversaries might attempt traditional attacks intended to subvert the confidentiality, integrity, and availability of these new cyber systems and, while such threats can lead to privacy, data, and economic damage, they can also lead to physical damage to the world around us and directly affect our personal well-being. New developments in the science and engineering of cybersecurity are needed in order to provide the tools that are necessary to protect our society and the investments we have made across a variety of domains. Further, collaboration between technology, policy, legality, and economics is needed in order to arrive at the best solutions to mitigate the emergence and impact of cybersecurity threats before they occur.

Editor-in-Chief
Prof. Dr. Danda B. Rawat

Aims

The *Journal of Cybersecurity and Privacy* (ISSN 2624-800X) is an open access journal of scientific research on all technical areas of cybersecurity. Our aim is to provide an advanced forum for displaying information, computer and network security, cryptography, cyber–physical system security, digital forensics, etc. The *Journal of Cybersecurity and Privacy* publishes articles, reviews, systematic reviews, communications, and viewpoints as well as Special Issues on particular subjects.

The aim of the *Journal of Cybersecurity and Privacy* is to encourage scientists to publish their experimental and theoretical results in as much detail as possible. Therefore, the journal has no restrictions regarding the length of papers. Full experimental details should be provided so that the results can be reproduced. In addition, electronic files or software regarding the full details of the calculation and experimental procedure as well as the source codes can be submitted as supplementary material.

Scope

- Machine Learning in Security
- Artificial Intelligence Security
- Big Data Security and Privacy
- Cloud Security
- Digital and Information Forensics
- Quantum Security
- Cyber–Physical System Security
- Network and Mobile Security
- IoT Security
- Security Risk and Engineering
- Management, Policies, and Human Factors in Security
- Privacy and Cyber Threat
- Anomymity and Privacy
- Cryptography and Cryptology
- Authetication and Access Control
- Biometrics

Author Benefits

Open Access

Unlimited and free access for readers

No Copyright Constraints

Retain copyright of your work and free use of your article

Thorough Rigorous Peer-Review

No Space Constraints, No Extra Space or Color Charges

No restriction on the maximum length of the papers, number of figures or colors

Rapid Publication

A first decision is provided to authors approximately 23.5 days after submission; acceptance to publication is undertaken in 9.8 days (median values for papers published in this journal in the second half of 2023)

MDPI is a member of

MDPI