Topical Collection

Intelligent Security and Privacy Approaches against Cyber Threats

Message from the Collection Editor

As many organizations have moved to work from home, cyber attackers have expanded their advanced persistent threats (APT), such as phishing, spear-phishing and zero-day attacks, to exploit vulnerabilities of home networks. It is urgent to develop well-designed privacy security approaches, algorithms, protocols, standards and policies for safeguarding home and organization networks against new cyber threats. Topics of interest include but are not limited to: - Intelligent security practices and model-based AI against COVID-19 threats; - Privacy-enabled human factor models against COVID-19 cyberattacks; - AI-based Intrusion Detection Systems for discovering COVID-19 cyberattacks; - AI-based cognitive models against COVID-19 cyberattacks; - Privacy-driven human analytical behaviours in home networks; - Privacy-preserving algorithms and approaches for protecting data of home networks; - Secure Big Data analytics to analyze heterogeneous IoT and home elements;

Collection Editor

Dr. Nour Moustafa

School of Engineering and Information Technology, University of New South Wales at ADFA, Canberra, ACT 2612, Australia

Journal of Cybersecurity and Privacy

mdpi.com/si/49399

mdpi.com/journal/
jcp

MDPI

About the Journal

Message from the Editor-in-Chief

Editor-in-Chief

Prof. Dr. Danda B. Rawat
Department of Electrical Engineering and Computer Science, Howard
University, Washington, DC 20059, USA

Author Benefits

High Visibility:

indexed within ESCI (Web of Science), Scopus, EBSCO, and other databases.

Rapid Publication:

manuscripts are peer-reviewed and a first decision is provided to authors approximately 24.4 days after submission; acceptance to publication is undertaken in 4.6 days (median values for papers published in this journal in the first half of 2025).

Journal Rank:

CiteScore - Q1 (Computer Science (miscellaneous))