SPECIAL ISSUE on Advancements in Machine Learning for Cybersecurity and Privacy: Algorithms, Models, and Applications

GUEST EDITORS

Gulshan Kumar, Shaheed Bhagat Singh State University, Ferozepur (Punjab) India

Krishan Kumar, Punjab University, Chandigarh, India

Subhash Chander, Malout Institute of Management and Information Technology, Malout (Punjab) India

Munish Kumar, Maharaja Ranjit Singh Punjab Technical University, Bathinda (Punjab) India

DESCRIPTION

This special issue in **Open Computer Science (IF 2022: 1.5)** focuses on Advancements in Machine Learning for Cybersecurity and Privacy.

The objective of this special issue is to showcase the latest advancements in machine learning techniques, algorithms, models, and applications that address the challenges of ensuring cyber security and privacy in the digital age.

The intersection of machine learning, cyber security, and privacy is a critical area of research in today's digital landscape. By providing a dedicated platform to share and discuss advancements in this field, this special issue will foster collaboration, facilitate knowledge exchange, and inspire further research in the domains of machine learning, cyber security, and privacy.

We believe that this special issue will attract a wide range of submissions from researchers and practitioners across the globe, enabling a comprehensive exploration of the advancements in machine learning for cyber security and privacy. The publication of this special issue in Open Computer Science will not only enhance the journal's reputation but also contribute significantly to the scientific community.

The scope of this special issue includes, but is not limited to, the following topics:

- Novel machine learning algorithms for threat detection and anomaly detection.
- Privacy preserving machine learning techniques and models.
- Machine learning approaches for secure authentication and access control.
- Adversarial machine learning and countermeasures.
- Machine learning applications in securing Internet of Things (IoT) devices and networks.
- Deep learning models for malware detection and analysis.
- Machine learning for data protection and secure communication.

Authors are requested to submit their full revised papers complying the general scope of the journal. The submitted papers will undergo the standard peer-review process before they can be accepted. Notification of acceptance will be communicated as we progress with the review process.

HOW TO SUBMIT

Before submission authors should carefully read the Instruction for Authors, available online.

Manuscripts can be written in TeX, LaTeX (strongly recommended) - the journal's LATEX template. Please note that we do not accept papers in Plain TEX format. Text files can be also submitted as standard DOCUMENT (.DOC) which is acceptable if the submission in LATEX is not possible. **For an initial submission, the authors are strongly advised to upload their entire manuscript, including tables and figures, as a single PDF file.**

All submissions to the Special Issue must be made electronically via online submission system Editorial Manager: http://www.editorialmanager.com/opencs/

All manuscripts will undergo the standard peer-review process (single blind, at least two independent reviewers). **When entering your submission via online submission system please choose the option "SI: Advancements in Machine Learning for Cybersecurity and Privacy".**
Submission of a manuscript implies that the work described has not been published before and it is not under consideration for publication anywhere else.

The deadline for submissions is November 30, 2023 but individual papers will be reviewed and published online on an ongoing basis.

Contributors to the Special Issue will benefit from:

- Critical peer-review
- no space constraints
- quick online publication upon completing the publishing process (**continuous publication model**)
- better visibility due to **Open Access** – free, unrestricted and permanent access to all the content
- **liberal policies on copyrights** (authors retain copyrights) and on self-archiving (no embargo periods)
- promotion of published papers to readers and citers
- **long-term preservation** – content archiving with Portico

We are looking forward to your submission!

In case of any questions please contact Editorial Office (opencomputerscience@degruyter.com)