Special Issue

Privacy and Security in Machine Learning

Message from the Guest Editors

Machine learning is clearly a research area that will continue creating real-world impacts, as computing power becomes increasingly more readily available. Security and privacy considerations, however, are vital, in particular since machine learning algorithms are often perceived as magical black boxes, in which the inner workings are not easily made transparent. Important topics that warrant new research are, among others:

- The right to be forgotten. How much of the "original" personal data is embedded in trained neural networks? Can we delete this data without retraining? How can we measure the anonymity/pseudonymity of training data embedded in a trained network?
- How easy is it to attack training sets and trained networks? If ML is used for real-world applications such as autonomous driving, successful attacks may have huge impact.

We look forward to receiving research papers that address, not only the aforementioned examples, but also any excellent research that investigates privacy and security aspects in ML in depth.

Guest Editors

Prof. Dr. Edgar Weippl
SBA Research, University of Vienna, 1040 Vienna, Austria

Prof. Dr. Francesco Buccafurri
Department of Information Engineering, Infrastructures and Sustainable Energy (DIIES), University Mediterranea of Reggio Calabria, 89122 Reggio Calabria, Italy

Deadline for manuscript submissions

closed (31 October 2018)

Machine Learning and Knowledge Extraction

an Open Access Journal by MDPI

Impact Factor 4.0
CiteScore 6.3

mdpi.com/si/13566

Machine Learning and Knowledge Extraction
MDPI, Grosspeteranlage 5
4052 Basel, Switzerland
Tel: +41 61 683 77 34
make@mdpi.com

mdpi.com/journal/make

Machine Learning and Knowledge Extraction

an Open Access Journal by MDPI

Impact Factor 4.0
CiteScore 6.3

mdpi.com/journal/make

MDPI

About the Journal

Message from the Editor-in-Chief

Editor-in-Chief

Prof. Dr. Andreas Holzinger
1. Human-Centered AI Lab, Institute of Forest Engineering, Department of Forest and Soil Sciences, University of Natural Resources and Life Sciences, 1190 Vienna, Austria
2. xAI Lab, Alberta Machine Intelligence Institute, University of Alberta, Edmonton, AB T5J 3B1, Canada

Author Benefits

High Visibility:

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

Rapid Publication:

manuscripts are peer-reviewed and a first decision is provided to authors approximately 20.8 days after submission; acceptance to publication is undertaken in 4.6 days (median values for papers published in this journal in the second half of 2024).

Journal Rank:

JCR - Q2 (Computer Science, Artificial Intelligence) / CiteScore - Q1 (Engineering (miscellaneous))