machine learning & knowledge extraction

an Open Access Journal by MDPI

IMPACT FACTOR 6.0

CITESCORE 9.9

Privacy and Security in Machine Learning

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)

Message from the Guest Editors

Dear Colleagues,

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.

Prof. Dr. Edgar Weippl
Prof. Dr. Francesco Buccafurri
Guest Editors

mdpi.com/si/13566

Special Issue

machine learning & knowledge extraction

IMPACT FACTOR 6.0

CITESCORE 9.9

an Open Access Journal by MDPI

Editor-in-Chief

Prof. Dr. Andreas Holzinger

1. Human-Centered AI Lab, Institute of Forest Engineering, Department of Ecosystem Management, Climate and Biodiversity, BOKU University, Vienna, Austria
2. Institute of Human-Centered Computing, Faculty of Computer Science and Biomedical Engineering, Graz University of Technology, Graz, Austria
3. xAI Lab, Alberta Machine Intelligence Institute, University of Alberta, Edmonton, AB, Canada

Message from the Editor-in-Chief

Machine learning deals with understanding intelligence to design algorithms that can learn from data, gain knowledge from experience and improve their learning behaviour over time. The challenge is to extract relevant structural and/or temporal patterns ("knowledge") from data, which is often hidden in high dimensional spaces, thus not accessible to humans. Many application domains, e.g., smart health, smart factory, etc. affect our daily life, e.g., recommender systems, speech recognition, autonomous driving, etc. The grand challenge is to understand the context in the real-world under uncertainty. Probabilistic inference can be of great help here as the inverse probability allows to learn from data, to infer unknowns, and to make predictions to support decision making.

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), dblp, and other databases.
Rapid Publication: manuscripts are peer-reviewed and a first decision is provided to authors approximately 27 days after submission; acceptance to publication is undertaken in 4.4 days (median values for papers published in this journal in the second half of 2025).

Contact Us

Machine Learning and Knowledge Extraction Editorial Office
MDPI, Grosspeteranlage 5
4052 Basel, Switzerland

Tel: +41 61 683 77 34
www.mdpi.com

mdpi.com/journal/make
make@mdpi.com
𝕏@MAKE_MDPI