machine learning & knowledge extraction

an Open Access Journal by MDPI

IMPACT FACTOR 3.9

CITESCORE 8.5

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