algorithms

an Open Access Journal by MDPI

IMPACT FACTOR 1.8

CITESCORE 4.1

Commemorative Special Issue: Adversarial and Federated Machine Learning: State of the Art and New Perspectives

Guest Editor:

Prof. Dr. Theodore B. Trafalis
School of Industrial and Systems Engineering, The University of Oklahoma, Norman, OK 73019, USA

Deadline for manuscript submissions:
closed (15 December 2022)

Message from the Guest Editor

In 2022, we will be celebrating ten years of research on adversarial machine learning. In 2012, Battista Biggio and others demonstrated the first gradient-based attacks on machine learning models. More recently, federated learning (FL), a machine learning setting where many clients collaboratively train a model through a central server while keeping the training data decentralized, was developed. It can mitigate many of the systemic privacy risks and costs resulting from traditional, centralized machine learning. This area has received significant interest recently, both from research and applied perspectives. However, adversarial attacks pose a serious threat to the success of FL in real-world problems. Hence, advanced techniques in this area have attracted increasing attention from both machine learning and security communities and have become a hot research topic in recent years.

This Commemorative Special Issue welcomes the submission of papers based on original research about adversarial and federated machine learning. Historical reviews, as well as perspective analyses for the future in this field of research, will also be taken into consideration.

algorithms

IMPACT FACTOR 1.8

CITESCORE 4.1

an Open Access Journal by MDPI

Editor-in-Chief

Prof. Dr. Frank Werner
Faculty of Mathematics, Otto-von-Guericke-University, P.O. Box 4120, D-39016 Magdeburg, Germany

Message from the Editor-in-Chief

Algorithms are the very core of Computer Science. The whole area has been considered from quite different perspectives, having led to the development of many sub-communities: Complexity theory (limitations), approximation or parameterized algorithms (types of problems), geometric algorithms (subject area), metaheuristics, algorithm engineering, medical imaging (applications), indicates the range of perspectives. Our journal welcomes submissions written from any of these perspectives, so that it may become a forum for exchange of ideas between the corresponding scientific subcommunities.

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), Ei Compendex, and other databases.
Journal Rank: JCR - Q2 (*Computer Science, Theory and Methods*) / CiteScore - Q1 (Numerical Analysis)

Contact Us

Algorithms Editorial Office
MDPI, Grosspeteranlage 5
4052 Basel, Switzerland

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

mdpi.com/journal/algorithms
algorithms@mdpi.com
𝕏@Algorithms_MDPI