Special Issue

Secure and Explainable AI: Enhancing Trust, Resilience, and Efficiency in Machine Learning Models

Message from the Guest Editor

This Special Issue focuses on advancing secure and explainable AI by addressing key challenges in adversarial robustness, AI security, and computationally efficient explainability. Topics of interest include but are not limited to the following:

- **Adversarial robustness in AI**: Detection and defense strategies against adversarial attacks.
- **Explainable AI (XAI) for security**: Interpretable models using SHAP, LIME, saliency maps, and decision tree surrogates for security applications.
- **Lightweight and efficient AI security**: Optimized security techniques for reducing computational overhead while maintaining robustness.
- **Privacy-preserving AI security**: Federated learning, homomorphic encryption, differential privacy, and secure multiparty computation for AI models.
- **Trustworthy AI in smart cities and healthcare**: Securing AI-driven traffic monitoring, surveillance, and medical diagnostics against adversarial threats.
- **Hybrid defense mechanisms**: Combining traditional cybersecurity techniques with AI-based threat detection for robust defenses.
- **Real-world case studies and applications**: Practical implementations of AI security and XAI in various domains.

Guest Editor

Dr. Sarfraz Brohi

Department of Computer Science and Creative Technologies,
University of the West of England (UWE), Bristol BS16 1QY, UK

Deadline for manuscript submissions

closed (15 October 2025)

Algorithms

an Open Access Journal by MDPI

Impact Factor 2.1
CiteScore 4.5

mdpi.com/si/235365

Algorithms
Editorial Office
MDPI, Grosspeteranlage 5
4052 Basel, Switzerland
Tel: +41 61 683 77 34
algorithms@mdpi.com

mdpi.com/journal/algorithms

MDPI

Algorithms

an Open Access Journal by MDPI

Impact Factor 2.1
CiteScore 4.5

mdpi.com/journal/algorithms

MDPI

About the Journal

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.

Editor-in-Chief

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

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)