

## Special Issue

# Adversarial Machine Learning in Sensors: Attacks, Defenses and Outlooks

### Message from the Guest Editor

Machine learning has become a critical part of society, used in forecasting, autonomous vehicles, critical infrastructure, healthcare and even surveillance. However, machine learning algorithms are vulnerable to attacks during training and testing time, which can lead to their confidentiality, integrity, and availability being harmed. Although many defences have been proposed in the past, the issue remains largely unsolved, as even state-of-the-art defences can be evaded by attackers. In this Special Issue, we welcome any papers that explore or identify vulnerabilities in machine learning and papers which propose robust defences. Special attention will be given to papers which explore the issue of evadable defences and provide insights into how defences can create more resilient attackers.

### Guest Editor

Dr. Yisroel Mirsky

Software and Information Systems Engineering, Ben-Gurion University, Beer Sheba, Israel

### Deadline for manuscript submissions

closed (26 May 2023)



## Sensors

---

an Open Access Journal  
by MDPI

---

Impact Factor 3.5  
CiteScore 8.2  
Indexed in PubMed



[mdpi.com/si/149921](https://mdpi.com/si/149921)

*Sensors*  
Editorial Office  
MDPI, Grosspeteranlage 5  
4052 Basel, Switzerland  
Tel: +41 61 683 77 34  
[sensors@mdpi.com](mailto:sensors@mdpi.com)

[mdpi.com/journal/  
sensors](https://mdpi.com/journal/sensors)





# Sensors

---

an Open Access Journal  
by MDPI

---

Impact Factor 3.5  
CiteScore 8.2  
Indexed in PubMed



[mdpi.com/journal/  
sensors](https://mdpi.com/journal/sensors)



## About the Journal

### Message from the Editor-in-Chief

*Sensors* is a leading journal devoted to fast publication of the latest achievements of technological developments and scientific research in the huge area of physical, chemical and biochemical sensors, including remote sensing and sensor networks. Both experimental and theoretical papers are published, including all aspects of sensor design, technology, proof of concept and application. Sensors organizes Special Issues devoted to specific sensing areas and applications each year.

---

### Editor-in-Chief

Prof. Dr. Vittorio M. N. Passaro

Dipartimento di Ingegneria Elettrica e dell'Informazione (Department of Electrical and Information Engineering), Politecnico di Bari, Via Edoardo Orabona n. 4, 70125 Bari, Italy

---

### Author Benefits

#### Open Access:

free for readers, with article processing charges (APC) paid by authors or their institutions.

#### High Visibility:

indexed within Scopus, SCIE (Web of Science), PubMed, MEDLINE, PMC, Ei Compendex, Inspec, Astrophysics Data System, and other databases.

#### Journal Rank:

JCR - Q2 (Instruments and Instrumentation) / CiteScore - Q1 (Instrumentation)