Special Issue

Adversarial Attacks and Mitigation Mechanisms in Large Language Models

Message from the Guest Editors

As large language models (LLMs) continue to revolutionize fields such as natural language processing, automated decision-making, and human–computer interaction, their security becomes increasingly critical. One of the emerging threats in this domain is adversarial attacks, where malicious actors manipulate input data to deceive models into making incorrect predictions or generating unintended outputs. This undermines the trust placed in LLMs and poses significant risks in applications in which safety, privacy, and reliability are paramount. This Special Issue aims to gather innovative research, methodologies, and datasets in the field of adversarial attacks and mitigation for large language models. We seek to explore both the theoretical foundations and practical implementations of securing LLMs against adversarial behavior, highlighting the intersection of AI security, model robustness, and real-world applications.

Guest Editors

Dr. Haitham Mahmoud

Dr. Nouh Elmitwally

Dr. Junaid Arshad

Prof. Dr. Sharad Mehrotra

Deadline for manuscript submissions

31 October 2025

Data

an Open Access Journal by MDPI

Impact Factor 2.0
CiteScore 5.0

mdpi.com/si/228407

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

mdpi.com/journal/data

Data

an Open Access Journal by MDPI

Impact Factor 2.0
CiteScore 5.0

mdpi.com/journal/data

About the Journal

Message from the Editor-in-Chief

Data is an open access journal that publishes scientific data in a reliable, citable, and accountable manner. Data grants the opportunity to formally share valuable data, for academic credit. It covers a wide range of disciplines in which data is generated so that published data is discoverable and available for wider re-use. The journal has highly accomplished scientists from a variety of disciplines on the editorial board. The publication emphasizes clarity, honesty, quality, and novelty and has a rigorous peer-review process. We strongly encourage you to share your data vision in Data.

Editor-in-Chief

Prof. Dr. Jamal Jokar Arsanjani
Geoinformatics and Earth Observation Research Group, Department of Planning, Aalborg University Copenhagen, A.C. Meyers Vænge 15, DK-2450 Copenhagen, Denmark

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, dblp, Inspec, RePEc, and other databases.

Journal Rank:

JCR - Q2 (Multidisciplinary Sciences) / CiteScore - Q2 (Information Systems and Management)

MDPI