



Security and Privacy for Artificial Intelligence: Opportunities and Challenges

Guest Editor:

Dr. Morteza Biglari-Abhari

Department of Electrical,
Computer, and Software
Engineering, The University of
Auckland, Auckland 1010, New
Zealand

Deadline for manuscript
submissions:

closed (15 February 2024)

Message from the Guest Editor

Dear Colleagues,

There has recently been a growing amount of interest in employing Artificial Intelligence (AI) in many applications, such as autonomous vehicles, industrial robotics, medical devices, and smart home systems, required to guarantee reliability, energy efficiency, time predictability, and high-level accuracy. As such applications process sensitive data and are connected to the Internet, security and privacy issues have become a critical concern. One important aspect of designing secure AI-based systems, especially on edge devices, is investigating the energy consumption overhead while achieving the required level of processing accuracy and performance.

The aim of this Special Issue is to collect high-quality submissions on research to avoid or mitigate the security vulnerabilities and achieve privacy preservation for AI applications considering the design at different levels of abstraction, from system-level design to micro-architecture level and hardware/software co-design. In addition, research outcomes to identify critical challenges and suggest further research opportunities are also welcome.

Dr. Morteza Biglari-Abhari
Guest Editor





information



an Open Access Journal by MDPI

Editor-in-Chief

Prof. Dr. Willy Susilo

School of Computer Science and
Software Engineering, University
of Wollongong, Northfields
Avenue, Wollongong, NSW 2522,
Australia

Message from the Editor-in-Chief

The concept of *Information* is to disseminate scientific results achieved via experiments and theoretical results in depth. It is very important to enable researchers and practitioners to learn new technology and findings that enable development in the applied field.

Information is an online open access journal of information science and technology, data, knowledge and communication. It publishes reviews, regular research papers and short communications. We invite high quality work, and our review and publication processing is very efficient.

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](#), and [other databases](#).

Journal Rank: CiteScore - Q2 (*Information Systems*)

Contact Us

Information Editorial Office
MDPI, St. Alban-Anlage 66
4052 Basel, Switzerland

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

mdpi.com/journal/information
information@mdpi.com
[X@InformationMDPI](#)