Security and Safety

Print ISSN 2097-2121
Online ISSN 2826-1275
CN 10-1841/TP

Submission deadline– 30th August 2024

OPEN ACCESS

Call for Papers

Special Issue on

Security and Safety in Artificial Intelligence

Guest Editors:

- **Hao Zhang**, Tongji University, China
- **Yu-Gang Jiang**, Fudan University, China
- **Claudio Melchiorri**, University of Bologna, Italy
- **Gerhard Rigoll**, Technical University of Munich, Germany

Science Press | edp sciences

Call for Papers

sands.edpsciences.org

Call for Papers

Special Issue on

Security and Safety in Artificial Intelligence

Background

The past few decades have witnessed the significant development of artificial intelligence, which would be widely used in critical infrastructure fields, such as rescue missions, environmental protection, and surveillance. Most recently, with the upgrading of computer hardware and software, artificial intelligence algorithms have been rapidly developed. However, the development of artificial intelligence technology is accompanied by vulnerabilities and threats, and the widespread application process is accompanied by many problems and incidents, which pose challenges to the industry, academia, and government. For this reason, security and safety in artificial intelligence is a critical and nonnegligible issue.

Aims and Scope of the Special Issue

Security and safety are important for artificial intelligence due to the complexity and infeasibility of related problems caused by uncertainty and external intrusion. Therefore, in order to obtain more complete artificial intelligence algorithms, it is necessary to study artificial intelligence under the context of security and safety issues. This special issue focuses on the development of security and safety in artificial intelligence. The key motivation behind this is to provide an opportunity for scientists, engineers, and practitioners to publish their latest theoretical and technical results, as well as to present original ideas and new approaches to AI in the context of security, such as offensive and defensive countermeasures, security detection, game optimization, data-driven security problems, *etc.*

The following is a non-exclusive list of topics relevant to the special issue:

- Attack modeling against artificial intelligence
- Attack detection for artificial intelligence
- Vulnerability analysis for artificial intelligence
- Data security and privacy for artificial intelligence
- Model-based and/or data-driven secure state estimation
- AI-based security algorithms and mechanisms
- AI-based security control
- Experimental evaluation for security and safety of artificial intelligence

Submissions

Authors should submit their manuscripts online directly at: https://sands.nestor-edp.org and choose, during submission, the special issue: **Security and Safety in Artificial Intelligence**. All relevant papers will be carefully considered and peer-reviewed by a distinguished team of international experts. The instructions for authors are detailed at: https://sands.edpsciences.org/author-information/instructions-for-authors.

Submission deadline – 30th August 2024

Article Processing Charges - S&S is an Open Access journal and no APCs in 2024.

Recommendation Editor - Jie Chen, Tongji University, chenjie206@tongji.edu.cn

Guest Editors

Hao Zhang, Tongji University, China, zhang_hao@tongji.edu.cn

Yu-Gang Jiang, Fudan University, China, ygj@fudan.edu.cn

Claudio Melchiorri, University of Bologna, Italy, claudio.melchiorri@unibo.it

Gerhard Rigoll, Technical University of Munich, Germany, rigoll@tum.de

Contact **Yuanyuan Liu**, *Security and Safety* Editorial Office, sands@edpsciences.org

Recommendation Editor Biography

Jie Chen is a professor at Tongji University, an academician of the CAE, IEEE Fellow and IFAC Fellow. His research fields include control science and engineering, intelligent unmanned system, complex system multi-index optimization and control, multi-agent collaborative control, *etc.* He is the director of the National Key Laboratory of "Autonomous Intelligent Unmanned System", director of the Basic Science Center of the National Natural Science Foundation of China, director of the Frontier Science Center of the Ministry of Education, director of the Shanghai Autonomous Intelligent Unmanned System Science Center. He is now the convener of the Control Science and Engineering Group of the Academic Degrees Committee of the State Council, the member of the Science and Technology Committee of the Ministry of Education and the director of the Special Committee, the vice chairman of the Chinese Association of Automation, the vice chairman of the Chinese Association of Artificial Intelligence, the vice president of the Chinese Association of Command and Control, the vice chairman of the Shanghai Expert Committee for Strategic Advisory on Artificial Intelligence, associate EiC of *Security and Safety* and the deputy chief editor and the editorial board of many academic journals.

Guest Editor Biographies

Hao Zhang is the Vice Dean of the School of Electronic and Information Engineering of Tongji University. She has published more than 190 papers in international journals and conferences, including 138 papers in SCI. She has published 9 papers in *Automatica*, an authoritative journal in the field of control, and 92 papers in IEEE Trans journals. 13 papers have been selected as highly cited papers in ESI, and she has been honored as one of the "100 most influential international academic papers in China". She received 7 provincial and ministerial awards and was the recipient of the Young Scientist Award of the Chinese Society of Automation; she presided over the 2019 National Natural Science Foundation of China Outstanding Youth Fund Project. She has been awarded the "Best Paper Award of IEEE International Conference on Information and Automation" twice. She is an associate editor/editorial board member of several international journals and co-chair/programming member of several international conferences such as WCICA, CCC, IEEE ICIA, etc. She is an editorial board member of *IEEE Intelligent Transportation Systems Magazine*, an editorial board member of *Security and Safety*, and an editorial board member of *Intelligence & Robotics*.

Yu-Gang Jiang is the Vice President of Fudan University, Chang Jiang Scholar Distinguished Professor, IEEE Fellow and IAPR Fellow. His research is focused on multimedia, computer vision, and robust & trustworthy AI. As the director of Shanghai Collaborative Innovation Center of Intelligent Visual Computing and Fudan Vision and Learning (FVL) Laboratory, he leads a group of researchers working on all aspects of robust & trustworthy visual analytics. He publishes extensively in top journals and conferences with over 20000 citations and an H-index of 80. His research outcomes have had major impacts on applications like mobile visual search/recognition and defect detection for high-speed railway infrastructures. His work has led to many awards, including the inaugural 2014 ACM China Rising Star Award, the 2015 ACM SIGMM Rising Star Award, and various awards from NSF China, MOE China, and Shanghai Government.

Claudio Melchiorri is an academician of the Italian Academy of Sciences, IEEE Fellow. He is a full professor at the Department of Electrical Engineering of the University of Bologna, head of the Department of Automation Engineering of the University of Bologna, and head of the Italian National Doctoral School in the field of automatic control. Professor Melchiorri is a senior member of the IEEE, a member of the IFAC Committee on Robotics, a member of the IFAC Technical Committee on Mechatronics, and a member of the IEEE Transactions on Robotics and Automation. He is currently a member of the editorial board of *Int. Journal of Robotics and Autonomous Systems*, *Control Engineering Practice*, and *the IFAC Journal on Mechatronics*. He has published more than 270 academic papers and 7 monographs.

Gerhard Rigoll is a professor at the Technical University of Munich and IEEE Fellow. His research interests are in the field of human-computer communication and multimedia information processing in the areas of multimodal interactive systems, speech and handwriting recognition, gesture recognition, face detection and recognition, action and emotion recognition, and interactive computer graphics. He has published over 550 papers in the field of pattern recognition and machine intelligence, covering the above application areas. He has served as an Associate Editor of *IEEE Transactions on Audio*, *Speech and Language Processing*, *the EURASIP Journal on Audio*, *Speech and Music Processing*, and *the EURASIP Journal on Image and Video Processing,* and on the Editorial Board of *the IEEE Signal Processing Society's Overview.* He has served as a reviewer for several scientific journals, as a session chair and program committee member for several international conferences, and as general chair of the 2008 annual DAGM-Symposium on Pattern Recognition.