Security and Safety

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

Submission deadline– 30th September 2026

OPEN ACCESS

Call for Papers

Special Issue on

Security and Safety in Embodied Intelligence

Guest Editors:

- **Qiang Wei**, National Digital Switching System Engineering & Technological R&D Center, China
- **Yunhao Liu**, Tsinghua University, China
- **Lina Yao**, University of New South Wales, Australia

Science Press | edp sciences

Call for Papers

sands.edpsciences.org

Call for Papers

Special Issue on

Security and Safety in Embodied Intelligence

Background

As a key bridge connecting artificial intelligence and the physical world, embodied intelligence, by virtue of the real-time interaction, dynamic learning, and autonomous decision-making capabilities of intelligent agents with the environment, is rapidly penetrating into various scenarios such as industrial production, service industries, and family life. The application of embodied intelligence technology has greatly improved production efficiency and life convenience. However, as the coupling between embodied intelligence systems and the physical world becomes increasingly close, their security issues have become more prominent. Such systems integrate hardware components such as sensors, processors, and actuators, as well as software modules such as perception algorithms, decision models, and control programs. In complex and dynamic environments, security vulnerabilities in any link may trigger a chain reaction. Different from the pure software environment, embodied intelligence needs to achieve a closed-loop security of "perception-decision-execution" in an open and dynamic environment, and its security threats are characterized by cross-modal, cross-level, and cross-domain features. On the one hand, in human-computer interaction scenarios, if the physical actions of intelligent agents are deviated or out of control, they may directly cause serious physical harm to humans. This requires embedding integrated security design in the whole life cycle of the system, forming a full-chain protection mechanism from hardware protection to algorithm constraints to prevent embodied intelligent agents such as robots from posing a threat to humans. On the other hand, humans may also use embodied intelligence systems through malicious manipulation, illegal access, and other means, making them tools that endanger public security or personal rights and interests. The security risks caused by such human factors further increase the complexity of protection. Furthermore, in order to build more reliable embodied intelligence systems, it is necessary to carry out research under the framework of integrated security.

Aims and Scope of the Special Issue

This special issue focuses on the development of integrated security of embodied intelligence, providing an opportunity for scientists, engineers, and practitioners to publish the latest theoretical and technological achievements, and encouraging the proposal of original ideas and new methods, such as algorithm security, data security, human-computer interaction security, alignment and security frameworks, *etc.*

This special issue covers (but not limited to) the following topics:

- Algorithm Security of Embodied Intelligence
- Sensing and Control Security of Embodied Intelligence
- Data Security of Embodied Intelligence
- Privacy Protection and Ethical Security of Embodied Intelligence
- Human-Computer Interaction Security in Cyber-Physical Fusion
- Vulnerability Mining of Embodied Intelligent Devices
- Anomaly Detection and Security Threat Discovery of Embodied Intelligence Systems
- Security Alignment and Integrated Security Framework of Embodied 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 Embodied 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 – 30 September 2026

Article Processing Charges - S&S is an Open Access journal and no APCs in 2025, APC is 1100 Euro in 2026.

Guest Editors

Qiang Wei, National Digital Switching System Engineering & Technological R&D Center, China, prof_weiqiang@163.com
Yunhao Liu, Tsinghua University, China, yunhao@tsinghua.edu.cn
Lina Yao, University of New South Wales, Australia, lina.yao@unsw.edu.au

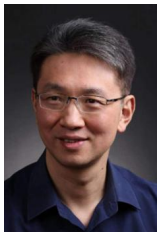
Contact

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

S&S Website

Guest Editor Biographies

Qiang Wei currently serves as a professor and doctoral supervisor at National Digital Switching System Engineering & Technological R&D Center, China, and specializes in software reverse analysis and industrial internet security. He has undertaken multiple research projects, including the National Key R&D Program and the National Natural Science Foundation of China.He is Awarded support from a national-level talent fund. He has published over 40 SCI-indexed papers in international security conferences such as CCS and USENIX, as well as in journals like TIFS and IoT. He serves on the editorial boards of international journals such as S&S. He has authored books including "Reverse Engineering and Vulnerability Analysis" and "Industrial Internet Security: Framework and Defense." He has received seven provincial and ministerial-level awards for scientific and technological progress, including first and second prizes. He now severs as an Associate Editor of *Security and Safety.*



Yunhao Liu serves as the Dean of the Global Innovation Exchange (GIX) at Tsinghua University, China. He is an Academician of the Chinese Academy of Sciences and a Fellow of both the Association for Computing Machinery (ACM) and the Institute of Electrical and Electronics Engineers (IEEE), and he has served as the Editor-in-Chief of ACM Transactions on Sensor Networks. Additionally, he is the Honorary Chair of the ACM China Council. His research focuses on a wide range of topics including the Internet of Things (IoT) and wireless sensor networks, indoor positioning and network diagnosis, RFID technology, supply chain and industrial internet systems, as well as distributed computing and cloud platforms. Professor Liu began his academic journey at Tsinghua University's Department of Automation from 1990 to 1995, where he earned his Bachelor's degree in Engineering. He then pursued studies at Beijing Foreign Studies University's Graduate School of Translation and Interpreting, graduating with a Master's degree in Literature in 1997. Later, from 2001 to 2004, he studied in the Department of Computer Science and Engineering at Michigan State University in the United States, where he obtained both his Master's and Doctoral degrees in Engineering. From 2004 to 2011, he held various academic and administrative roles at the Hong Kong University of Science and Technology, including Assistant Professor, Associate Professor, Ph.D. Supervisor, and Postgraduate Director. In 2011, he was appointed as a Cheung Kong Scholar Distinguished Professor at Tsinghua University under the Ministry of Education's prestigious talent program. He served as Dean of Tsinghua's School of Software from 2013 to 2017, and later from 2018 to 2020, he was the MSU Foundation Professor and Head of the Department of Computer Science and Engineering at Michigan State University in the U.S. Since August 2020, he has been serving as the founding Dean of the Global Innovation Exchange (GIX) at Tsinghua University, while also holding a professorship and supervising doctoral students in the Department of Automation. Throughout his distinguished career, Professor Liu has received numerous prestigious awards and honors. In 2007, he was awarded the Best Innovation and Research Award in Hong Kong. In 2010, he received the First Prize in Natural Sciences from the Ministry of Education. In 2011, he was honored with both the National Natural Science Award (Second Class) and the National Science Fund for Distinguished Young Scholars. In 2013, he received the ACM Presidential Award, one of the highest honors within the ACM. In 2014, his research team won the Best Paper Award at ACM MobiCom, one of the top conferences in mobile computing. In 2016, he was recognized by the China Computer Federation with the Youth Achievement Award from the IoT Committee. Most recently, in 2021, his students received the Best Student Paper Award at ACM SIGCOMM under his guidance. Professor Liu's contributions to academia span leadership, research, education, and international collaboration, making him a leading figure in computer science and innovation in China and globally. He now severs as an Associate Editor of *Security and Safety.*

Lina Yao is currently a Professor at University of New South Wales. Her research focuses on developing generalizable, explainable, and data-efficient algorithms in data mining, machine learning, and deep learning. She alsodesigns systems and user interfaces to advance human-machine interaction, with a particular emphasis on addressing key challenges such as robustness, trust, explainability, and resilience to strengthen human-autonomy collaboration. Her research interests span Few-Shot and Zero-Shot Learning, Deep Reinforcement Learning, Self-Supervised Learning, and Deep Generative Modeling, with broad applications across Recommender Systems, Computer Vision, Brain-Computer Interfaces, Intelligent Transportation Systems, and the Internet of Things. She has received multiple research awards, including ARC Future Fellowship, ARC Discovery Early Career Research Award and Inaugural Vice Chancellor's Women's Research Excellence Award from the University of Adelaide in 2015, Scientia Fellow from UNSW in 2019, Inaugural Women in AI Awards in 2021 and CORE Outstanding Research Contribution Award (formerly named after Chris Wallace) in 2023.