frontiers | Frontiers in Physics

TYPE Editorial
PUBLISHED 15 August 2024
DOI 10.3389/fphy.2024.1464919

OPEN ACCESS

EDITED AND REVIEWED BY
Matjaž Perc,
University of Maribor, Slovenia

*CORRESPONDENCE
Yuanyuan Huang,
iyyhuang@hotmail.com

RECEIVED 15 July 2024
ACCEPTED 17 July 2024
PUBLISHED 15 August 2024

CITATION
Huang Y and Lu X (2024), Editorial: Security, governance, and challenges of the new generation of cyber-physical-social systems. *Front. Phys.* 12:1464919. doi: 10.3389/fphy.2024.1464919

Editorial: Security, governance, and challenges of the new generation of cyber-physical-social systems

Yuanyuan Huang[1]* and Xin Lu[2]

[1]Department of Network Engineering, Chengdu University of Information Technology, Chengdu, China, [2]School of Computer Science and Informatics, De Montfort University, Leicester, United Kingdom

KEYWORDS

cyber-physical-social systems (CPSS), internet of things-IoT, artificial intelligence-AI, big data, cyber-physical systems (CPS), advanced attacks, system security

Editorial on the Research Topic
Security, governance, and challenges of the new generation of cyber-physical-social systems

In recent years, the transformation of devices and systems into intelligent, interconnected entities has given rise to the concepts widely recognized as the Internet of Things (IoT) and cyber-physical systems (CPSs). The integration of social networks with CPSs leads to an innovative paradigm known as cyber-physical-social systems (CPSSs). CPSS, harmonizing the cyber, physical, and social spaces, constitutes the next evolution of intelligent systems. It is founded on the integration of embedded systems, computer networks, control theory, and sensor networks. A typical CPSS is comprised of sensors, controllers, actuators, and communication networks. Its salience lies in the seamless connection of physical devices to the Internet and social networks, thereby imbuing these devices with capabilities such as computation, communication, precise control, remote coordination, and autonomy. The applicability of CPSS spans diverse fields, including intelligent transportation systems, telemedicine, smart grid technology, aerospace, smart home appliances, environmental monitoring, intelligent buildings, defense systems, and weaponry. Thus, CPSS stands as a vital component of a nation's essential infrastructure.

CPSS exhibits a range of distinctive features, including the amalgamation of human and computer intelligence, the integration across various spatial domains, inherent network heterogeneity, and the incorporation of multi-source information. In the context of CPSS, data serves as a vital link, seamlessly connecting the three principal components: cyber systems, physical mechanisms, and social constructs. Information from physical and social systems is conveyed to the corresponding information system via network channels. Simultaneously, this information system reciprocates by supplying feedback to the physical and social domains through meticulous computation and informed decision-making processes. Nevertheless, the heterogeneous nature of CPSS, coupled with their reliance on confidential and sensitive data, and expansive deployment, makes them susceptible to an array of security threats. These threats span across the

cyber, physical, and social realms, presenting significant challenges related to privacy and trust.

This Research Topic is dedicated to presenting original research and insightful reviews, emphasizing innovations and enhancements in the domains of advanced attacks, system security, privacy, and trust technology in CPSS. Submissions focusing on detection and defense strategies employing artificial intelligence and big data are particularly encouraged. This includes a wide range of topics, including but not limited to, theoretical foundations, design methodologies, modeling techniques, configuration approaches, representational frameworks, data processing mechanisms, analytical methods, and their relevant applications within the context of CPSS.

Author contributions

YH: Writing–original draft, Writing–review and editing. XL: Writing–review and editing.

Funding

The author(s) declare that no financial support was received for the research, authorship, and/or publication of this article.

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note