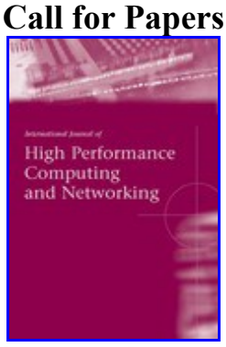
INDERSCIENCE PUBLISHERS
Linking academia, business and industry through research

Call for Papers



Int. J. of High Performance Computing and Networking

CSS 2018: Special Issue on: "Smart Monitoring and Protection of Data-Intensive Cyber-Physical Critical Infrastructures"

Guest Editors:
Dr. Raffaele Pizzolante, University of Salerno, Italy
Prof. Florin Pop, University Politehnica of Bucharest, Romania
Prof. Massimo Ficco, University of Campania Luigi Vanvitelli, Italy
Prof. Marek Ogiela, AGH University of Science and Technology, Poland

Today even more research efforts are being aimed at the monitoring and protection of data-intensive cyber-physical critical infrastructures, e.g. critical civil or military infrastructures, such as transport systems, water treatment facilities, power plants, electricity grids, oil and gas refineries. Security of such critical infrastructures is of paramount importance, since its failure can have important social and economic consequences.

However, this seems to go in the opposite direction with respect to devices used within such infrastructures, e.g. Internet of Things (IoT) devices. Indeed, such devices, which enable the interconnection of sensors and controllers, typically have constrained hardware and software characteristics, which impose several limitations on the security facilities to be used. Such completely heterogeneous devices exchange large amounts of data, sometimes for short periods. Thus, the problem of efficient and intelligent monitoring of such infrastructures arises.

This special issue invites original research and review articles that will bring the emerging area of data-intensive cyber-physical critical infrastructures monitoring to the attention of the academic and industrial research community. We invite the submission of papers introducing novel algorithms, techniques, software architectures and hardware technologies that support the advancement of the state of the art concerning the reliable and effective processing of information concerning the cyber-physical world.

The issue will carry revised and substantially extended versions of selected papers presented at the 10th International Symposium on Cyberspace Safety and Security (CSS 2018), but we are also inviting other experts to submit articles for this call.

Subject Coverage

Suitable topics include, but are not limited, to the following:

- Mobile data analysis, management and processing for cyber-physical critical infrastructures
- Information fusion for mobile data for cyber-physical critical infrastructures
- New techniques in smart data for cyber-physical critical infrastructures
- Machine learning algorithms over big data for cyber-physical critical infrastructures
- Deep learning models, architectures and algorithms for big data for cyber-physical critical infrastructures
- Brain-inspired representations learning of big data for cyber-physical critical infrastructures
- Edge/cloud computing for big data and smart data for cyber-physical critical infrastructures
- Applications of fuzzy set theory, rough set theory and soft set theory in smart data for cyber-physical critical infrastructures
- Security, privacy and trust in big data and smart data for cyber-physical critical infrastructures
- Streaming data learning algorithms for cyber-physical critical infrastructures
- Intelligent decision-making systems for big data and smart data in cyber-physical critical infrastructures
- Prediction methods for big data and smart data applications in cyber-physical critical infrastructures
- Evolutionary computing in big data in cyber-physical critical infrastructures
- Swarm intelligence and big data for cyber-physical critical infrastructures
- Handling uncertainty and incompleteness in big data and smart data for cyber-physical critical infrastructures
- Open issues for smart data in cyber-physical critical infrastructures
- Models for risk identification and assessment in data-intensive cyber-physical critical infrastructures

Notes for Prospective Authors

Submitted papers should not have been previously published nor be currently under consideration for publication elsewhere. (N.B. Conference papers may only be submitted if the paper has been completely re-written and if appropriate written permissions have been obtained from any copyright holders of the original paper).

All papers are refereed through a peer review process.

All papers *must* be submitted online. To submit a paper, please read our Submitting articles page.

Important Dates

Manuscripts due by: *1 December, 2018*

Notification to authors: *1 February, 2019*

Final versions due by: *30 March, 2019*