Journal of Reliable Intelligent Environments (2024) 10:1
https://doi.org/10.1007/s40860-024-00219-x

EDITORIAL

Editorial

Antonio Coronato[2] · Juan C. Augusto[1]

Published online: 26 February 2024

This first issue of the tenth volume of the Journal of Reliable Intelligent Environments brings six articles in various technical areas.

Blockchain-based collaborative business process data sharing and access control, by Xiaoxiao Sun, Yijie Wei, and Hujun Shen, proposes an innovative framework to manage large-scale data storage and reliable access control in blockchain-based collaborative business process executions with multiple Internet of Things (IoT) devices and participants.

Handling uncertainty in self-adaptive systems: an ontology-based reinforcement learning model, by Saeedeh Ghanadbashi, Zahra Safavifar, Farshad Taebi, and Fatemeh Golpayegani, faces the problem of uncertainty in self-adaptive systems that may results in inconsistent decisions and unexpected system behavior. Authors proposed a hybrid approach that improves the classic Reinforcement Learning based methods with domain otologies to handle rare events.

Two-stage RFID approach for localizing objects in smart homes based on gradient boosted decision trees with under- and over-sampling, by Shadi Abudalfa, and Kevin Bouchard, presents an approach to localize objects within a smart home based on a double localization mechanism. The first stage detects the main area (room) where the object is located. Then, the second one determines the exact position within the identified area.

Cluster head selection and malicious node detection using large-scale energy-aware trust optimization algorithm for HWSN, by Rahul Das, and Mona Dwivedi, focuses on Hierarchical Wireless Sensor Networks (HWSN). The specific problems faced are cluster head selection and malicious node detection. To this aim, authors proposed a large-scale energy-aware trust optimization algorithm. In particular, a harmonic search genetic algorithm is initially used to select the Cluster Head based on energy, trust, distance, and density. Then, malicious nodes are detected using an energy-aware intra- and inter-cluster trust estimation model.

Formal verification for security and attacks in IoT physical layer, by Zinah Hussein Toman, Lazhar Hamel, Sarah Hussein Toman, Mohamed Graiet, and Dalton Cézane Gomes Valadares, proposes an Event-B proof-based formal model for the verification of security characteristics of the IoT physical layer. The model is built incrementally using a refining method during design and verification, and consists of three formally conceived levels.

MSDN-IoT multicast group communication in IoT based on software-defined networking, by Youssef Baddi, Anass Sebbar, Karim Zkik, Yassin Maleh, Faysal Bensalah, and Mohammed Boulmalf, defines a novel multicast software-defined network called MSDN-IoT, which is based on a hierarchical shared multicast tree and a flexible set of SDN controller modules, like group management for dynamic multicast services.

We hope these articles stimulate the community to produce further improvements in these areas.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

✉ Antonio Coronato
a.coronato@unifortunato.eu

Juan C. Augusto
j.augusto@mdx.ac.uk

[1] Research Group on Development of Intelligent Environments
Department of Computer Science, Middlesex University,
London, UK

[2] Universitá Giustino Fortunato, Benevento, Italy