Computing (2021) 103:1057–1059
https://doi.org/10.1007/s00607-021-00938-6

EDITORIAL

# Guest Editorial: QoS and security in software for wireless and mobile micro-services

Ahmed Mostefaoui[1] · Gabriele Gianini[2] · Ernesto Damiani[3,4] · Geyong Min[5]

Published online: 1 April 2021

## Introduction

Recent years have witnessed very remarkable technological advances in both hardware miniaturization (availability of enough powerful micro-devices at reasonable prices with communication capabilities) and associated software and service developments. Their target applications cover a broad spectrum of services, ranging from general public applications (health services, smart cities services, automotive services, etc.) to specialized applications (military, industrial, etc.). The development of such services and their deployment raise several open research challenges, among them Quality of service (QoS) and Security.

Quality of Service is intrinsically related to the requirements of the end users/applications. It can be declined under various metrics: technological metrics (throughput maximization, delay, and energy minimization, etc.) as well as user experience metrics (quality of data, completeness of the information, etc.). The recent developments have widened the perimeter of QoS to include new aspects and the corresponding metrics/constraints such as quality of the captured data, quality of the

✉ Ahmed Mostefaoui
ahmed.mostefaoui@univ-fcomte.fr

Gabriele Gianini
gabriele.gianini@unimi.it

Ernesto Damiani
ernesto.damiani@unimi.it

Geyong Min
g.min@exeter.ac.uk

[1] University of Burgundy Franche-Comte, Belfort, France

[2] Università degli Studi di Milano, Italy and EBTIC/Khalifa University of Science and Technology, Abu-Dhabi, UAE

[3] Research Centre on Cyber-Physical Systems (C2PS), Khalifa University of Science and Technology, Abu-Dhabi, UAE

[4] Università degli Studi di Milano, Milan, Italy

[5] University of Exeter, Exeter, UK

transmission, quality of the local processing due to intrinsic limitations (memory and computing), etc. This is a consequence of the used hardware, known to be more prone to failures, and of the development of the associated software, usually characterized by low-level abstraction (i.e., close to the hardware primitives for performance reasons). Another issue related to QoS is the increased importance of scalability for the proposed services, raised by the need of large scale deployment, as the expected number of devices used in an application may be of the order of thousands. Those new conditions call for a paradigm shift in terms of concepts and techniques handling QoS within micro-services.

Closely connected to QoS, the objectives related to privacy, security, and trust have become a significant challenge, mainly due to the extensive dissemination of these micro-services in our private lives, for instance in health monitoring, home control, e-payments, etc. Techniques addressing these issues aim at ensuring that the provided micro-services will protect the users' data and provide guarantees that no malicious device will affect the system decisions, under the additional constraints of granting a given QoS level.

A very important role in addressing the different issues of connected environments has been taken by Machine Learning techniques, and more recently by Deep Learning techniques.

## Special issue content

Acknowledging the central importance of QoS and security in micro-services, COMPUTING JOURNAL is running a special issue with a selection of papers addressing a number of key issues. This special issue has attracted numerous submissions (`18 submitted papers`), among which we have selected `8 papers` after a two-round reviewing process.

- The work presented by Mansour et al. focuses on querying connected environments such as smart buildings and smart cities: it proposes an Event Query Language for Connected Environments (EQL-CE)specifically designed to overcome some limitations of existing EQLs: the language uses operators that deal with spatial-temporal distributions, consider various data types and cope with the dynamical character of the connected environments.
- Siddiqui et al. tackle the issue of network intrusion detection by using ensembles of auto-encoders. The challenging aspect of this choice is that auto-encoders are very efficient but typically computationally expensive, whereas often the connected smart environments are resource constrained. To meet these constraints, they propose several and evaluate several approaches to reduce the ensemble complexity through adaptive de-activations of auto-encoders.
- The paper by Zroug et al. uses a formal approach based on Hierarchical Timed Colored Petri Nets to model and to evaluate the CSMA/CA MAC protocol in sensors networks. Differently from previous papers, the work covers also the quantitative verification of properties such as throughput, delivery ratio, delay and waiting time for ACK.

- Wang et al. propose a virtual network embedding algorithm based on Deep Reinforcement Learning, aiming at optimizing CPU, bandwidth, delay and security attributes of the substrate network.
- Benslimen et al. address the problem of attack prediction and of failure prediction by proposing a framework composed by various prediction agents, each agent consisting of a security predictor, a fault predictor and a generic anomaly detection model trained by reinforcement process.
- Martins et al. consider the challenge to provide Machine Learning capabilities to the resource-constrained environment of IoT: they propose a heuristic for adapting data prediction and data fusion techniques to pre-process data so as to avoid unnecessary communication between sensor devices and sinks.
- Fani Sani et al. focus, instead, on the study techniques for biased under-sampling of event logs in data rich environments: they show that is possible to considerably speed up the mining phase while at the same time preserving the quality of the results.
- Merzough at al. propose, investigate and evaluate a smart connected parking IoT solution based on image analysis. They implemented it using different classical and lightweight deep learning techniques (MobileNetV2, ResNet-50, YOLOv3, SSD-MobileNetV2, Tiny-YOLO, SqueezeDet): the system uses a periodic counting of empty spots in the parking lots, and an instantaneous driver notification through a lightweight MQTT mechanism.

**Acknowledgements** We would like to thank the Editor in Chief and the administrative stuff of the COMPUTING JOURNAL for their kind assistance and help.

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