Received: 6 January 2020 | Accepted: 3 February 2020 | Published on: 4 March 2020
DOI: 10.1002/spe.2813

EDITORIAL

WILEY

Software tools and techniques for fog and edge computing

The Internet of Things (IoT) paradigm promises to make "things" such as physical objects with sensing capabilities and/or attached with tags, mobile objects such as smartphones and vehicles, consumer electronic devices, and home appliances such as fridge, television, health care devices, as part of the Internet environment. In cloud-centric IoT applications, the sensor data from these "things" is extracted, accumulated, and processed at the public/private clouds, leading to significant latencies. To satisfy the ever increasing demand for cloud computing resources from emerging applications such as IoT, academics and industry experts are now advocating for going from large-centralized cloud computing infrastructures to micro data centers located at the edge of the network. These micro data centers are often closer to a user (geographically and in access latency) compared to the centralized cloud data center. The aim of utilizing such edge resources is to off load computation that would have "traditionally" been carried out at the cloud data center to a resource that is closer to a user or edge devices. This vision also acknowledges the variation in network latency from an end-user to cloud data center. While the network around a data center is often high capacity and speed, that near the user device may have variable properties (in terms of resilience, bandwidth, latency, etc.). Referred to as "fog/edge computing," this paradigm is expected to improve the agility of cloud service deployments in addition to bringing computing resources closer to end-users. The emergence of computing paradigms such as edge and fog computing supports the data analysis near the data sources for a wide range of applications. Edge computing is the middle layer between users and cloud data centers, and it plays an important role in the IoT use cases where applications required near real-time actions. The intermediate edge layer provides limited computing and storage resources, which consists of network gateways and micro data centers. Edge computing application orchestration is capable of big data processing and can be installed in heterogeneous hardware configurations. Due to the large-scale deployment and device heterogeneity, edge computing infrastructure designing and implementation are challenging, including model analysis, system integration, protocol designing, energy, and security modeling. In addition, since edge data centers are installed in network gateways with open network configuration, they are prone to several network threats, less trustworthy, and easy to compromise. On the one hand, the development of fog and edge clouds includes dedicated facilities, operating system, network, and middleware techniques to build and operate such micro data centers that host virtualized computing resources. On the other hand, the use of fog and edge clouds requires extension to current programming models and proposes new abstractions that will allow developers to design new applications that take benefit from such massively distributed systems. The use of this approach also opens up other challenges in security and privacy (as a user now needs to "trust" every micro data center they interact with), support for resource management for mobile users who transfer session from one micro data center to another, and support for "embedding" such micro data centers into devices (eg, cars, buildings, etc).

The objective of this special issue is to disseminate original contributions and research findings concerning the challenges and changes (both evolutionary and disruptive) in edge and fog computing. It provides cutting-edge research from both academia and industry, with emphasis on current developments and future directions in security and privacy issues of emerging fog computing. The call for special issues received a number of submissions. Each paper was reviewed by at least three reviewers and went through at least two rounds of reviews. After a two-phase peer review process, we have accepted 14 high-quality papers related to the aforementioned areas of interest. The accepted papers focus on recent solutions by developing novel research ideas around edge and fog computing for several applications, such as health care, smart city, urban pollution monitoring, etc. The brief contributions of these papers are discussed in the following section.

The first paper titled "*Abnormal visual event detection based on multi-instance learning and autoregressive integrated moving average model in edge-based Smart City surveillance*" by Xu et al proposes an abnormal event detection approach based on multi-instance learning and autoregressive integrated moving average model for video surveillance of crowded scenes in urban public places. It utilizes an unsupervised method for abnormal event detection by combining multi-instance visual feature selection and the autoregressive integrated moving average model. This approach has thoroughly experimented, and the experimental results demonstrate the efficiency of the proposed approach by achieving better abnormal event detection performance for a crowded scene of urban public places with an edge environment.

The second paper titled "*User allocation-aware edge cloud placement in mobile edge computing*" by Guo et al studies the edge cloud placement problem, which is to place the edge clouds at the candidate locations and allocate the mobile users to the edge clouds. Further, it formulates as a multi-objective optimization problem with the objective to balance the workload between edge clouds and minimize the service communication delay of mobile users. The experiment results show the performance of the proposed approach in terms of workload balance and communication delay for validation.

The third paper titled "*A secure fog-based platform for SCADA-based IoT critical infrastructure*" by Baker et al contributes a novel security "toolbox" to reinforce the integrity, security, and privacy of SCADA-based IoT critical infrastructure at the fog layer. The toolbox incorporates a key feature, that is, a cryptographic-based access approach to the cloud services using identity-based cryptography and signature schemes at the fog layer. This paper also presents the implementation details of a prototype for our proposed secure fog-based platform and provides performance evaluation results to demonstrate the appropriateness of the proposed platform in a real-world scenario. The results from the experiments demonstrate a superior performance of the secure fog-based platform, which is around 2.8 seconds when adding five virtual machines (VMs), 3.2 seconds when adding 10 VMs, and 112 seconds when adding 1000 VMs, compared to the multilevel user access control platform.

The fourth paper titled "*Developing applications in large scale, dynamic fog computing: A case study*" by Giang et al presents a case study in building fog computing applications using an open-source platform distributed node-RED. It shows how applications can be decomposed and deployed to a geographically distributed infrastructure using distributed node-RED, and how existing software components can be adapted and reused to participate in fog applications. This case study is implemented in a lab-based fog infrastructure and simulated for large-scale evaluation.

The fifth paper titled "*An osmotic computing infrastructure for urban pollution monitoring*" by Longo et al focuses on the design and development of a middleware that integrates data coming from mobile and IoT devices specifically deployed in urban contexts using the osmotic computing paradigm. Moreover, a component of the osmotic membrane has been developed in this paper for security management.

The sixth paper titled "*Characterizing application scheduling on edge, fog, and cloud computing resources*" by Varshney and Simmhan offers a taxonomy of concepts essential for specifying and solving the problem of scheduling applications on edge, fog, and cloud computing resources. The proposed model is divided into multiple steps, initially characterized by the resource capabilities and limitations of these infrastructures and offers a taxonomy of application models, quality-of-service constraints and goals, and scheduling techniques based on a literature review, followed by tabulated key research prototypes and papers using this taxonomy. It also highlights gaps in the literature and open problems remain.

The seventh paper titled "*Cloud-aided online electroencephalography (EEG) classification system for brain healthcare: A case study of depression evaluation with a lightweight CNN*" by Ke et al presents the design of an online EEG classification system aided by cloud centering on a lightweight convolutional neural network (CNN). The system incrementally trains the CNN on cloud and enables hot deployment of the trained classifier without the need to restart the gateway to adapt to the users' needs. The classifier maintains a high convolutional layer to gain the ability of processing high-dimensional EEG segments. Finally, the model is experimented to validate the contribution.

The eighth paper titled "*SEWMS: An Edge-based Smart Wearable Maintenance System in Communication Network*" by Rui et al proposes a dynamic context-aware information push algorithm (DCAIP) by focusing on the current low level in information, complicated scenes, and various information on on-site maintenance. It also presents a smart wearable maintenance system (SEWMS), an edge computing-assisted IoT platform for the real-time guidance of technical experts and systems for on-site maintenance personnel, aiming to improve the efficiency and quality of on-site maintenance.

The ninth paper titled "*A crosswalk pedestrian recognition system by using deep learning and zebra-crossing recognition techniques*" by Dow et al investigates a real-time pedestrian recognition system that ensures high accuracy by using a deep learning classifier and zebra-crossing recognition techniques. The proposed system was designed to improve pedestrian safety and reduce accidents at intersections. Environmental feature vectors were first used to detect zebra crossings and to determine crossing areas. An adaptive mapping technique was then used to map the pedestrian waiting area based on the crossing area. A dual-camera mechanism was used to maintain detection accuracy and improve system fault tolerance. Finally, the you-only-look-once model was used to recognize pedestrians at intersections.

The 10th paper titled "*Intelligent sentiment analysis approach using edge computing-based deep learning technique*" by Sankar et al studies machine learning algorithms to extract the best features from the training review dataset. Then, the selected features are fed into the CNN and other fully connected layers for further processing. This work has also employed a pretrained sentiment analysis model over an Android application framework to classify reviews on a smartphone without the need for any cloud or server-side application programming interface.

The 11th paper titled "*Pipeline provenance for cloud-based big data analytics*" by Wang et al proposes a solution, named LogProv toward realizing the functionalities for big data provenance, which needs to renovate data pipelines or some of big data software infrastructure to generate structured logs for pipeline events, and then stores data and logs separately in cloud space. The LogProv is implemented and deployed in Nectar Cloud, associated with Apache Pig, Hadoop ecosystem, and adopted Elasticsearch to provide query service.

The 12th paper titled "*Socially aware microcloud service overlay optimization in community networks*" by Apolónia et al presents a model, named Select in Community Networks (SELECTinCN), which enhances the overlay creation for pub/sub systems over peer-to-peer (P2P) networks. Moreover, SELECTinCN includes social information based on cooperation within CNs by exploiting the social aspects of the community of practice. The model organizes the peers in a ring topology and provides an adaptive P2P connection establishment algorithm, where each peer identifies the number of connections needed based on the social structure and user availability.

The 13th paper titled "*DewSim: A trace-driven toolkit for simulating mobile device clusters in Dew computing environments*" by Hirsch et al models and develops a trace-based toolkit built on modular software artifacts to speed up research in resource management techniques in Dew environments. A trace-driven methodology is adopted to assure the practical value of simulated scenarios. The toolkit comprises a device profiler application for Android to capture generic battery and central processing unit traces from real devices, a profile mixer to create user interaction baseline traces through generic ones, and an extensible engine to simulate the execution of workloads configurable via text files.

The 14th paper titled "*How to Place Your Apps in the Fog-State of the Art and Open Challenges*" Borgi et al review the existing methodologies to solve the application placement problem in the fog, while pursuing three main objectives. First, it offers a comprehensive overview of the currently employed algorithms, on the availability of open-source prototypes, and on the size of test use cases. Second, it classifies the literature based on the application and fog infrastructure characteristics that are captured by available models, with a focus on the considered constraints and the optimized metrics. Finally, it identifies some open challenges in application placement in the fog.

The 15th paper titled '*SELFNET 5G mobile edge computing infrastructure: Design and prototyping*' by Chirivella-Perez *et al*. presented the design and prototype implementation of the fifth-generation (5G) mobile edge infrastructure based on a mobile edge computing paradigm. This mobile edge infrastructure SELFNET is an amlganmation of cloud computing, software-defined networking, and network function virtualization to end up with a portable 5G infrastructure testbed which enabled the realistic execution and testing.

Finally, in the last paper titled '*SDN/NFV security framework for fog-to-things computing infrastructure*' by Krishnan *et al*. proposed DTARS which is a System for Distributed Threat Analytics and Response for an Edge/Fog and SDN integrated architecture. In this system, the detection scheme runs at the data plane wherein a coarse-grained behavioral, anti-spoofing, flow monitoring and fine-grained traffic multi-feature entropy-based algorithms are deployed. The proposed framework has been developed for defense applications on malware testbed.

We hope that the research contributions and findings in this special issue would benefit the readers in terms of enhancing their knowledge and encouraging them to work on various aspects of edge and fog computing.

ACKNOWLEDGEMENTS

We express our sincere thanks to the editor-in-chief for allowing us to organize this special issue. The editorial office staffs are excellent and thanks for their support. We are also thankful to all the authors who made this special issue possible, and to the reviewers for their thoughtful contributions.

Rajiv Ranjan[1]
Massimo Villari[2]
Haiying Shen[3]
Omer Rana[4]
Rajkumar Buyya[5]

[1]*School of Computing, Newcastle University, Newcastle upon Tyne, UK*
[2]*Department of MIFT, University of Messina, Messina, Italy*
[3]*Department of Electrical and Computer Engineering, University of Virginia, Charlottesville, Virginia*
[4]*School of Computer Science and Informatics, Cardiff University, Cardiff, UK*
[5]*School of Computing and Information Systems, University of Melbourne, Parkville, Australia*

Correspondence
Rajiv Ranjan, School of Computing, Newcastle University, Newcastle upon Tyne, UK.
Email: rranjans@gmail.com