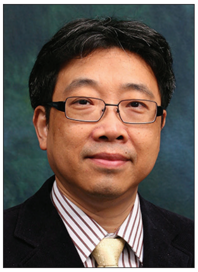
HUMAN-DRIVEN EDGE COMPUTING AND COMMUNICATION: PART 2


Jiannong Cao


Aniello Castiglione


Giovanni Motta


Florin Pop


Yanjiang Yang


Wanlei Zhou

The new challenge addressed by the Human-Driven Edge Computing and Communication Feature Topic is how to put users in the loop so that they can retake control of their information. The massive proliferation of personal computing devices is opening new human-centered designs that blur the boundaries between man and machine. In addition, edge services are also used to exchange the data collected and processed within the context of the IoT towards external services and/or to visualize them through traditional browser by the users. Now, the frontier for the research on the data management is related to the so-called edge computation and communication, consisting of an architecture of one or more collaborative multitude(s) of computing nodes that are placed between the sensor networks and the cloud-based services. Such a mediating level is responsible for carrying out a substantial amount of data storage and processing to reduce the retrieval time and have more control over the data with respect to cloud-based services, and to consume less resources and energy to reduce the workload.

The interdependencies among those three different levels of storage and computing within an IoT solution are complex, and determining at which level data should be collocated and elaborated is a demanding challenge that is not simple to handle. Such a complex situation is further exacerbated if we consider achieving quality of service goals such as reliability, availability, security, mobility, and energy efficiency, without compromising the correct behavior of the system and the service duration of the devices' batteries.

The analysis of human activity and their interactions with physical and digital artefacts will also be extremely useful for closing the control loop of adaptive distributed systems. This may open a new research playground for distributed systems that adapt to user behaviors in different contexts, moving more and more to the network edge through devices such as fifth generation (5G) mobile networks or 5G wireless systems. The second aspect of the frontier of the current research is therefore related to the application of challenging networking solutions to support fog communication and computation in the Internet of Things.

This is the second part of this Feature Topic. We received a total of 51 submissions co-authored by people belonging to institutions spread around the world. The submissions went through a rigorous review process, and the result was the acceptance of 15 contributions that have been split up into more than one issue. The first eight papers were included in November 2017 issue, while six more are included in this issue.

The first contribution, co-authored by Sarros *et al.*, is "Connecting the Edges: A Universal, Mobile-Centric. and Opportunistic Communications Architecture." The work introduces an information-centric model that enables the association of access to a desired content with the content itself, irrespective of the location where it is being held. The proposed system can pervasively operate in any networking environment and allows for the development of innovative applications.

The second article, co-authored by Liu *et al.*, is "A Survey on Access Control in Fog Computing," which provides a comprehensive survey on data access control in fog computing with the aim of highlighting security problems and challenges. The main contribution of the article is represented by the state of the art on access control schemes in fog computing.

A wearable plantar bio-feature extractor constructed via commercial pressure sensors and the Raspberry PI platform is presented in the article co-authored by Zhou *et al.*, "I Walk, Therefore I Am: Continuous User Authentication with Plantar Biometrics." The authors propose a model that applies machine-learning-based techniques to derive a user's plantar bio-features as authentication tokens in the system.

In the fourth article, "Securing the Human-Driven Post-Quantum Internet of Things with Lattice-Based Cryptography," co-authored by Liu *et al.*, the authors focus on the implementation aspects of lattice-based cryptography for resource-constrained IoT devices, and practical suggestions to choose appropriate implementation techniques. Several research challenges for securing the post-quantum IoT are highlighted in the article.

Bhuiyan *et al.*, in their article "PrivacyProtector: Privacy-Protected Patient Data Collection in IoT-Based Healthcare Systems," introduce the challenges of privacy protected data collection for IoT medical devices, which are more vulnerable to numerous security threats and attacks than other network devices. The authors propose a practical framework called PrivacyProtector, a novel patient privacy protected data collection method with the objective to prevent different types of attacks. They introduce the idea of secret sharing and share repairing (in case of data loss or compromise) for patient data privacy.

In the last and sixth article, "Deep Learning: The Frontier for Distributed Attack Detection in Fog-to-Things Computing," Diro and Chilamkurti present a novel distributed deep learning scheme of cyber-attack detection in fog-to-things computing. The authors experimentally show that deep models are superior to shallow models in detection accuracy, handling distributions, and scalability.

This Feature Topic would have not have been possible without the ongoing efforts of many individuals. First of all, the Guest Editors owe gratitude to all the contributing authors and to the efforts of the reviewers. Our special thanks go to Osman Gebizlioglu, the previous Editor-in-Chief of *IEEE Communications Magazine*, for his support and advisce. We sincerely appreciate the efforts of the highly knowledgeable editorial team of *IEEE Communications Magazine*.

BIOGRAPHIES

JIANNONG CAO [M'93, SM'05, F'15] (csjcao@comp.polyu.edu.hk) received his M.Sc. and Ph.D. degrees in computer science from Washington State University. He is currently a Chair Professor with the Department of Computing at Hong Kong Polytechnic University. He is also the director of the Internet and Mobile Computing Lab in the department and the director of the university's Research Facility in Big Data Analytics. His research interests include parallel and distributed computing, mobile computing, and big data analytics.

ANIELLO CASTIGLIONE [S'04, M'08] (castiglione@ieee.org) has a Ph.D. in computer science from the University of Salerno, Italy. He is an adjunct professor at the University of Salerno and at the University of Naples ''Federico II,'' Italy. He is the Managing Editor of two international journals and has served as a Guest Editor of several Special Issues in many high-ranked journals. His research interests include security and privacy on communication networks, information forensics and Security, and applied cryptography.

GIOVANNI MOTTA [S'97, M'05, SM'11] (giovannimotta@google.com) received his Laurea in informatica in 1996 (Summa Cum Laude) from the University of Salerno and a Ph.D. in computer science from Brandeis University in 2002. He is currently with Google (Terra Bella), where he works on high resolution satellite imagery and analytics. His main interests are in the fields of data compression, coding, and algorithms. He has been granted 13 patents, and published two books and more than 50 peer-reviewed papers in journals and conferences.

FLORIN POP (florinpop@ieee.org), a professor, received his Ph.D. in computer science at the University Politehnica of Bucharest in 2008. His main research interests are large-scale distributed systems, big data, cloud and edge computing, adaptive methods, multi-criteria optimization methods, prediction methods, self-organizing systems, and performance evaluation using modeling and simulation. He is a reviewer and Guest Editor for several journals. He is a scientific researcher at the National Institute for Research and Development in Informatics, Bucharest.

YANJIANG YANG (yang.yanjiang@huawei.com) is currently a senior researcher at Shield Lab, Huawei, Singapore. Prior to that, he was with the Institute for Infocomm Research, Singapore, as a research scientist between 2008 and 2015. His research spans a wide spectrum of information security such as applied cryptography, trusted computing, multimedia security, and cloud security; his main current research interest is IoT security, especially connected car security.

WANLEI ZHOU [M'92, SM'09] (wanlei.zhou@deakin.edu.au) received his B.Eng. and M.Eng. degrees from Harbin Institute of Technology, China, in 1982 and 1984, respectively, and his Ph.D. degree from the Australian National University, Canberra, in 1991. He is currently the Alfred Deakin Professor, Chair of Information Technology, and Associate Dean of the Faculty of Science, Engineering and Built Environments, Deakin University, Melbourne, Australia. His research interests include distributed systems, network security, bioinformatics, and e-learning.