Computing (2019) 101:725–727
https://doi.org/10.1007/s00607-019-00719-2

EDITORIAL

Special issue "Internet of Things (IoT)-based Services"

Fatos Xhafa[1]

Published online: 23 April 2019

Mathematics Subject Classification 68M11 · 68Uxx · 68M14

Introduction

Internet of Things (IoT) has become a major computing paradigm and the latest disruptive technology after the Cloud computing. The ability of IoT to connect with other systems and applications, from low to high level has prompted and promoted an unprecedented array of applications in all fields of human activity from science, engineering, business, health, leisure and everyday life, etc.

The technological development in IoT is going hand-by-hand with huge research efforts by an ever increasing community in a fascinating multidisciplinary field. In such research efforts, IoT-based services are deserving an important place due to the well-known Cloud "*everything-as-a-service*" paradigm.

This special issue is therefore devoted to latest research findings and developments in the IoT-based services and their application to a variety of domains. The special issue received 22 submissions, of which 14 submissions were pre-selected for potential publication and entered the review process. Finally, after reviewing process, 8 papers were accepted for publication in the issue.

The eight papers of the special issues are arranged as follows.

In the first paper [1] "*Multi-Access Edge Computing Aided Mobility for Privacy Protection in Internet of Things*" by Zhang et al., the authors consider Multi-Access Edge Computing (MEC) as an enabler for service development in 5G. They analyse opportunities brought by MEC to enhance IoT system's network privacy and propose a MEC enhanced Mobility Support System for IoT. Simulation results are presented to exemplify and sustain the claims.

Kayes et al. [2] in the second paper "*Critical Situation Management Utilizing IoT-Based Data Resources Through Dynamic Contextual Role Modeling and Activation*"

✉ Fatos Xhafa
fatos@cs.upc.edu

[1] Universitat Politècnica de Catalunya, Barcelona, Spain

deal with the provisioning of IoT services for critical situation management, where access to data and resources is usually restricted by means of their normal roles. The Role-Based Access Control (RBAC) and Context-Aware role-based Access Control (CAAC) frameworks are analysed. Then the authors present a formal approach to CAAC for dynamically specifying the contextual roles based on the relevant contextual conditions. An ontology-based approach which models the dynamic contextual roles and its associated access control policies is also introduced. The authors demonstrate the feasibility of the proposal by providing an experimental study on the performance of the approach.

The third paper [3] "*Improved Publicly Verifiable Group Sum Evaluation over Outsourced Data Streams in IoT Setting. Computing*" by Wang et al., research issues arising in the integration of the IoT and Cloud computing such as outsourced data stream collected by IoT devices. In this context, group sum evaluation over outsourced data stream collected by IoT devices is an essential building block in many stream applications. The authors emphasize the need to design a mechanism to verify the correctness of the group sum evaluation over the outsourced data streams, especially when the data streams are originated from multiple data sources. Existing schemes are analysed and two improved security schemes are presented.

Alshehri and Hussain [4] in the fourth paper "*A Fuzzy Security Protocol for Trust Management in the Internet of Things (Fuzzy-IoT)*" investigate ways of achieving a reliable and secure IoT connection and communication as essential for the proper working of the IoT network. The authors analyse as such a way building trusted communication among the things and the detection of attacks on the IoT trust system from malicious nodes. The proposed solution can firstly detect on-off attacks using the proposed fuzzy-logic based approach, and it can detect contradictory behaviour attacks and other malicious nodes. Then, a fuzzy logic-based approach to detect malicious nodes involved in bad service provisioning. Finally, to maintain the security of the IoT network, the proposal includes a secure messaging system that enables secure communication between nodes.

The fifth paper "*Detect and Correlate Information System Events Through Verbose Logging Messages Analysis*" by Amato et al. [5] approach detecting and tracking events from logging data as a critical element for security and system administrators. The authors aim to overcome existing limitations related to the verbosity and language-dependence of messages produced by many logging systems. A novel methodology is proposed to tackle this limitation by analysing event messages through a Natural Language Processing using semantic meta-data.

Khan et al. [6] in the sixth paper "*Efficient Routing for Corona based Underwater Wireless Sensor Networks*" study efficient routing protocols aiming to address imbalance energy consumption and the network performance degradation due to high data traffic at intermediate nodes. Several schemes are presented to distribute data traffic across the network nodes for efficient energy consumption. The efficiency of the proposed schemes against the baseline scheme is shown by extensive simulations.

The seventh paper "*Testing IoT Systems Using a Hybrid Simulation based Testing Approach*" by Bosmans et al. [7] brings an extensive overview of the challenges that arise when testing large IoT applications at the system level. A a novel hybrid simulation based testing approach is presented that is able to effectively facilitate interactions

among local entities (IoT devices or people) under synchronization between real-life and simulation environment and the scalability constraints of modern simulation techniques.

Finally, de Hoog et al. [8] in the last paper "*Towards a Distributed Real-Time Hybrid Simulator for Autonomous Vehicles. Computing*" present a real-time hybrid simulator that is capable of handling real and simulated vehicles simultaneously with full interaction, in real time. The experimental results effectively show the viability of this approach for validation of autonomous vehicles in a cost-efficient and safe manner.

Acknowledgements As I conclude this guest editorial preface, I would like to thank all the authors for their interesting contributions and reviewers for their timely feedback to authors. The help and support by the Editor-in-Chief, Prof. Schahram Dustdar, and the journal managerial team are highly appreciated.

References

1. Zhang P, Durresi M, Durresi A (2018) Multi-access edge computing aided mobility for privacy protection in internet of things. Computing. https://doi.org/10.1007/s00607-018-0639-0
2. Kayes ASM, Rahayu W, Dillon T (2018) Critical situation management utilizing IoT-based data resources through dynamic contextual role modeling and activation. Computing. https://doi.org/10.1007/s00607-018-0654-1
3. Wang XA, Liu Y, Sangaiah AK, Zhang J (2018) Improved publicly verifiable group sum evaluation over outsourced data streams in IoT setting. Computing. https://doi.org/10.1007/s00607-018-0641-6
4. Alshehri MD, Hussain FK (2018) A fuzzy security protocol for trust management in the internet of things (fuzzy-IoT). Computing. https://doi.org/10.1007/s00607-018-0685-7
5. Amato F, Cozzolino G, Mazzeo A, Moscato F (2018) Detect and correlate information system events through verbose logging messages analysis. Computing. https://doi.org/10.1007/s00607-018-0662-1
6. Khan ZA, Latif G, Sher A, Usman I, Ashraf M, Ilahi M, Javaid N (2019) Efficient routing for corona based underwater wireless sensor networks. Computing. https://doi.org/10.1007/s00607-018-0690-x
7. Bosmans S, Mercelis S, Denil J, Hellinckx P (2018) Testing IoT systems using a hybrid simulation based testing approach. Computing. https://doi.org/10.1007/s00607-018-0650-5
8. de Hoog J, Janssens A, Mercelis S, Hellinckx P (2018) Towards a distributed real-time hybrid simulator for autonomous vehicles. Computing. https://doi.org/10.1007/s00607-018-0649-y