Editorial: New developments in cloud and IoT

Muhammad Younas [a], Irfan Awan [b], George Ghinea [c], Tor-Morten Grønli [d]

[a] School of Engineering, Computing and Mathematics, Oxford Brookes University, Oxford, OX33 1HX, United Kingdom
[b] Department of Electrical Engineering and Computer Science, University of Bradford, Bradford, BD7 1DP, United Kingdom
[c] Department of Computer Science, Brunel University London, Uxbridge, UB8 3PH, United Kingdom
[d] Westerdals-Oslo School of Arts, Communication and Technology, Faculty of Technology, Mobile Technology Lab, Oslo, Norway

a b s t r a c t

Cloud computing and Internet of Things (IoT) provide new paradigms for the development of distributed, heterogeneous and complex systems which are characterised by requirements such as large scale storage space, large volume of data, high end compute processing power, and interoperable networks and communication protocols. Such systems contain a set of smart (physical) devices of IoT which are interconnected and controlled through (software) services using cloud infrastructure. Thus the convergence of cloud with the IoT has the potential to provide new levels of services in various sectors including businesses, education, science and research, public sector and governmental organizations. This editorial presents the work of the papers accepted for the special issue on 'new developments in cloud and IoT'.

1. Introduction

Cloud computing and IoT are different technologies. But after a number of years of inception, cloud and IoT have started to converge and to develop complementary relationships [1,2]. For instance, IoT generates a large volume of (big) data that put huge strain on IoT networks and devices. Cloud can be used to store and process IoT generated data in order to improve the overall efficiency of IoT applications. However, in order to fully realise the benefits of cloud and IoT many research challenges still need to be addressed. These include, data communication and processing, security, privacy and other quality of service attributes of cloud and IoT systems [3].

This special issue on ''New developments in cloud and IoT'' aims to foster the dissemination of high quality research with new ideas and developments in the areas of IoT and cloud services. The special issues was organized to receive papers from open call as well as extended papers from the IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud-2016) and the International Conference on Open and Big Data (OBD-2016), IEEE CS-TCI, which were held in Vienna, Austria, during 22–24 August 2016.

The conferences were attended by a large number of participants from different countries across the world. The call for papers for this special issue attracted 48 papers from open call as well as from authors of the above conferences. All the submitted papers were reviewed by multiple reviewers and they went through multiple rounds of review. Based on the review, 9 papers were accepted for this special issue.

E-mail addresses: m.younas@brookes.ac.uk (M. Younas), i.u.awan@bradford.ac.uk (I. Awan), george.ghinea@brunel.ac.uk (G. Ghinea), tmg@westerdals.no (T.-M. Grønli).

2. New developments in cloud and IoT

The papers accepted for this special issue present interesting and timely research work in the areas of security, access control, quality of service in hybrid cloud, mobile cloud, social networks and workflows, and data classification in IoT. The work presented in each of the paper is summarized as follows.

The paper by Belyaev et al. [4] provides a valuable insight into the access control and security issues in component-oriented application services. The authors contend that modern server operating systems enable the deployment of concurrent application services on a single server instance which has become common in data centres and cloud-based service provisioning. It is beneficial to the service providers to deploy large number of services on a single server instance thereby reducing the total cost of ownership. However, the challenge is to regulate access control of application services to system resources and sharing of data between application services. In order to address this challenge, this paper develops a Linux Policy Machine (LPM) framework which unlike existing kernel-level solutions, provides access control facilities for various service components running in isolated environments. It also proposes policy classes in order to manage policies related to accessing system and application level resources. Various experiments are carried out in order to demonstrate how regulated inter-component communication can take place through tuple spaces.

Chifor et al. [5] investigate into the security issues of IoT-enabled smart home devices and their interaction with cloud-based services. IoT devices generally require an existing infrastructure (such as operating system, etc.) which is commonly out of the control of a device's user. The authors propose a security authorization scheme for IoT-based smart home devices which are

connected using untrusted cloud services. The proposed scheme enables such devices to use cloud system in order to relay input commands to user's smart phone for authorization. The main benefits of this scheme are that it is user-centric and it provides better security in an untrusted IoT and cloud environment.

Hybrid cloud is a combination of public and private clouds. Depending on the level of privacy and security of applications, hybrid cloud generally outsources non-critical applications to public clouds. The paper by Labba et al. [6] develops a Multi Agent System (MAS) framework for hybrid clouds in order to optimise computing and data transfer costs when applications are outsourced to public clouds. The framework exploits the extended version of the Fiduccia-Mattheyses (E-FM) algorithm. It is evaluated using a number of simulation experiments in order to estimate and evaluate the overall outsourcing and deployment costs of applications in hybrid clouds.

The paper by Al-Ayyoub et al. [7] investigates into service provisioning in cloud data centres by taking account of Quality of Service and the revenue generated by cloud service providers in situations where services are affected by unpredictable incidents such as power outages, network problems, security breaches, etc. This paper exploits mixed integer-linear programming (MILP) in order to develop a new model that routes service requests to appropriate data centre and manages incidents and abnormal circumstances. The objective is to maximize the net profit of a cloud service provider. The paper includes various experiments in order to evaluate the proposed model. The experiments show promising results with respect to quality of service, incident management and revenue generation by a cloud service provider.

Online social networks (OSNs) are used by millions of users across the globe. OSNs require high compute power, large data storages and efficient communication network technologies such as cloud, IoT and Internet. However, current OSNs face serious concerns such as information overload, single-point of failure and privacy issues. Liu et al. [8] propose to build a self-organized decentralized OSN (SDOSN) on the overlay network using an IoT infrastructure. SDOSN considers homophily features in order to define social relationships and user interests which are beneficial for efficient dissemination of information in OSNs. The paper also proposes a swarm intelligence search method that facilitates adaptive forwarding and effective service discovery. The proposed SDOSN is shown to provide better performance as compared to existing state of the art OSNs.

Antunes et al. [9] focus on the issue of data classification in IoT environment. The rationale given is that there exist billion of IoT devices which are used to generate, collect and share large volume of diversified data. However, this significantly complicates the process of managing data sources in IoT. The literature review reveals that there is no uniform way to represent, share, and understand IoT data which results in hindering the full realization of IoT potentials. The work presented in this paper identifies the limitations of current solutions. It describes the advantages of semantic approaches for context organization and extends an unsupervised model to learn word categories automatically. This is because full potential of IoT can be achieved when the devices work and learn together with minimal human intervention. The proposed solution is evaluated using Miller-Charles dataset and IoT semantic dataset. Experimental evaluation of the proposed technique yields promising results.

The paper by Hasham et al. [10] illustrates benefits (such as dynamic, on-demand and scalable provisioning of resources) that cloud computing provides for the execution of scientific workflows. Accordingly, it presents a framework that aims to reproduces Scientific Workflow Execution using Cloud-Aware Provenance (ReCAP). The framework also comprises mapping approaches which are used to capture cloud-aware provenance information and to help in re-provisioning the execution resources of similar configurations. The proposed framework is evaluated through a number of experiments in scientific domains such as astronomy and neuroscience. The experiments provide useful results and observations which include: the impact of different resource configurations on the workflow execution performance; capturing cloud information in various cloud usage scenarios but without causing performance overhead; and re-provisioning of cloud resources.

The rapid growth in IoT devices and mobile applications require a better computational resource paradigm that can provide good level of performance, security, and usability. Hasan et al. [11] presents a model, called Aura, which is claimed to be a highly localized IoT based cloud computing model that enables mobile clients to create ad hoc and flexible clouds using the IoT and other computing devices in the nearby vicinity. Aura is validated through a prototype application of MapReduce which runs on IoT devices using Contiki OS. Various experimental measurements were obtained from the prototype application. These were used in order to evaluate different performance metrics of Aura in comparison to traditional clouds and applications running natively on mobile phones. Aura is shown to provide better performance than existing solutions.

The paper by Zhou et al. [12] reports that cloud computing provides organizations with benefits of minimizing operational and administrative costs. But at the same time it results in high consumption of energy that could adversely affect its benefits. This paper aims to minimize energy consumption and to ensure the required level of QoS which is defined as a part of SLA (Service Level Agreement). In other words, energy consumption should be reduced such that it has minimal effects on SLA violation. Accordingly, the paper proposes two adaptive energy-aware algorithms for cloud datacentres —i.e., to maximize energy efficiency and to minimize SLA violation rate. The strategy employed in the proposed algorithms is to take into account application types, CPU and memory resources during the deployment of virtual machines (VMs). Evaluation is carried out using a number of PlanetLab VMs. Experimental results show that the proposed algorithms outperform existing energy-saving techniques in terms of (i) decreasing energy consumption, and (ii) minimizing SLA violation.

3. Summary

The papers published in this special issue have developed new models and techniques in order to further enhance research and development in the areas of cloud and IoT. More specifically, the papers focus on crucial issues such as security, access control, and quality of service in cloud and IoT. These topics have practical applications in cloud and IoT. Further, the papers also set useful directions for future research work.

References

[1] Alessio Botta, Walterde Donato, Valerio Persico, Antonio Pescap, Integration of cloud computing and Internet of Things: A survey, Future Gener. Comput. Syst. 56 (2016) 684–700.

[2] Christos Stergiou, Kostas E. Psannis, Byung-Gyu Kim, Brij Gupta, Secure integration of IoT and cloud computing, Future Gener. Comput. Syst. 78 (3) (2018) 964–975.

[3] Wei Li, Igor Santos, Flavia C. Delicato, Paulo F. Pires, Luci Pirmez, Wei Wei, Houbing Song, Albert Zomaya, Samee Khan, System modelling and performance evaluation of a three-tier cloud of things, Future Gener. Comput. Syst. 70 (2017) 104–125.

[4] Kirill Belyaev, Indrakshi Ray, Component-oriented access control—Application servers meet tuple spaces for the masses, Future Gener. Comput. Syst. 86 (2018) 726–739.

[5] Bogdan-Cosmin Chifor, Ion Bica, Victor-Valeriu Patriciu, Florin Pop, A security authorization scheme for smart home Internet of Things devices, Future Gener. Comput. Syst. 86 (2018) 740–749.

[6] Chahrazed Labba, Narjès Bellamine Ben Saoud, Julie Dugdale, A predictive approach for the efficient distribution of agent-based systems on a hybrid-cloud, Future Gener. Comput. Syst. 86 (2018) 750–764.
[7] Mahmoud Al-Ayyoub, Muneera Al-Quraan, Yaser Jararweh, Elhadj Benkhelifa, Salim Hariri, Resilient service provisioning in cloud based data centers, Future Gener. Comput. Syst. 86 (2018) 765–774.
[8] Bo Yuan, Lu Liu, Nick Antonopoulos, Efficient service discovery in decentralized online social networks, Future Gener. Comput. Syst. 86 (2018) 775–791.
[9] Mário Antunes, Diogo Gomes, Rui L. Aguiar, Towards IoT data classification through semantic features, Future Gener. Comput. Syst. 86 (2018) 792–798.
[10] Khawar Hasham, Kamran Munir, Richard McClatchey, Cloud infrastructure provenance collection and management to reproduce scientific workflows execution, Future Gener. Comput. Syst. 86 (2018) 799–820.
[11] Ragib Hasan, Mahmud Hossain, Rasib Khan, Aura: an incentive-driven ad-hoc iot cloud framework for proximal mobile computation offloading, Future Gener. Comput. Syst. 86 (2018) 821–835.
[12] Zhou Zhou, Jemal Abawajy, Morshed Chowdhury, Zhigang Hu, Fangmin Li, Hongbing Cheng, Abdulhameed A. Alelaiwi, Fangmin Li, Minimizing SLA violation and power consumption in cloud data centers using adaptive energy-aware algorithms, Future Gener. Comput. Syst. 86 (2018) 836–850.