Guest Editorial: Special Issue on Computational Intelligence for Cloud Computing

CLOUD computing has emerged as an exciting new computing environment where computing infrastructure, platforms, and software application services are offered at low cost from remote very-large-scale data centers accessed over the Internet. Since it offers huge savings in business costs, cloud computing has recently received large amounts of attention and continued to be of high priority for researchers and developers in both academia and industry. The emergence of cloud computing environments poses a number of difficulties, complex issues in optimization and learning as well as other aspects. They call for new paradigms because the arising problems have become intractable when dealt with the use of traditional methods. Computational Intelligence (CI) research could provide important technical innovations to develop intelligent solutions for the new computing environments and their real world applications. The development of new CI theories and techniques for cloud computing has attracted significant amount of attention recently from academia, industry, and government as well.

The goal of this special issue is to present the state-of-the-art research on utilizing novel CI techniques for cloud computing environments, and to provide a forum for experts to disseminate their recent advances and views on future perspectives in the field. In particular, we invited papers that present new CI theories, methods and techniques applied to cloud computing. We particularly encouraged papers demonstrating novel CI strategies to new types of cloud computing domains such as mobile cloud computing, social cloud computing, etc. Applications were drawn based on the usage of CI for all aspects of the cloud computing system, including the architecture analysis, system design, prototype implementation, performance optimization, operation maintenance, and security management.

This Special Issue contains four papers. In "A Three-Layer Privacy Preserving Cloud Storage Scheme based on Computational Intelligence in Fog Computing", Wang *et al.* propose a Three-Layer Storage (TLS) framework based on fog computing to effectively resist attack on the user data from the inside of cloud server. The TLS framework makes full use of fog server's storage whilst protecting the data privacy. Based on computational intelligence, Hash-Solomon code algorithm is designed to divide data and compute the distribution proportion stored in cloud, fog and local machine, separately. Theoretical analysis and experimental evaluation demonstrate that the scheme is a powerful supplement to existing cloud storage schemes.

In "Entropy4Cloud: Using Entropy-based Complexity to Optimize Cloud Service Resource Management", Chen *et al.* identify the origin of complexity in cloud service resource management system through the study of Local Activity Principle. Then they propose an Entropy-based methodology which covers identifying, measuring, analyzing and controlling of complexity. The idea is also implemented in a popular cloud engine, Apache Spark, for running Analysis as a Service (AaaS). Comparisons are given to the Fair Scheduler in Apache Spark. Results show that the proposed Entropy Scheduler has significantly outperformed it.

In "Scheduling for Time-constrained Big-file Transfer over Multiple Paths in Cloud Computing", Lin *et al.* consider two types of scheduling problems for big-file transfer in cloud computing, ie, single-file transfer scheduling (SFTS) and multi-file transfer scheduling (MFTS). Both problems aim to maximize the bandwidth utilization under delay constraint. For SFTS, a heuristic algorithm is developed by adopting maximum flow over time. For MFTS, a heuristic is developed with an intelligent scheme to maximize the throughput and schedule the multi-file flow dynamically.

In "A Deep Learning Approach to Network Intrusion Detection", Shone *et al.* present a novel deep learning technique for intrusion detection, which addresses the concerns regarding the feasibility and sustainability of current Network Intrusion Detection Systems (NIDSs) approaches. They first propose a non-symmetric deep auto-encoder (NDAE) for unsupervised feature learning and then propose a novel deep learning classification model constructed using stacked NDAEs. The new technique has been implemented in GPU-enabled TensorFlow and evaluated using some popular benchmark datasets. Results demonstrate significant improvements over existing approaches and the strong potential to be applied in modern NIDSs.

Overall, the Special Issue was attractive since it received a total of **xx** submissions. The above 4 papers were selected following a very rigorous peer review. The guest editors would like to thank all the authors for their contributions and all the reviewers for their hard work in completing the reviewing timely. Last but not least, we thank Editor-In-Chief, Prof Yew-Soon Ong, for the constant support and assistance offered during the editing process of this Special Issue.

We hope that you will enjoy reading these novel contributions!

H. Cheng, *Guest Editor*
Liverpool John Moores University
Liverpool L3 3AF, UK
H.Cheng@ljmu.ac.uk

X. Yao, *Guest Editor*
Southern University of Science and Technology
Shenzhen 518055, China
xiny@sustc.edu.cn

S. Yang, *Guest Editor*
De Montfort University
Leicester LE1 9BH, UK
syang@dmu.ac.uk.

M. ZHANG, ***Guest Editor***
Victoria University of Wellington
Wellington 6012, New Zealand
mengjie.zhang@ecs.vuw.ac.nz