Special Issue on Intelligent Edge Computing for Cyber Physical and Cloud Systems

Cyber Physical Systems (CPS) and Cloud Computing have received tremendous research interest and efforts from both academia and industry. Cloud computing extends the computing and storage ability of CPS and leads to a new paradigm—Cyber Physical and Cloud Systems (CPCS), which is a product of combining CPS and Cloud Computing together. It enables a new breed of applications and services, such as industrial process control, video surveillance, structural health monitoring, and intelligent agriculture, and can fundamentally change the way that people interact with the physical world. However, CPCS face many important challenges. First, the Cloud can neither manage CPS devices directly nor satisfy requirements of real-time. Second, communication bottleneck exists between CPS and the Cloud. Third, new security challenges need to be overcome to accelerate the development of these integrated applications. In particular, edge computing, acting as a new computing scheme, is a promising technology to address these challenges. It extends the Cloud Computing paradigm to the edge of the network. For example, edge computing devices, which are capable of intelligent computing, can reduce the network latency by enabling computation and storage capacity at the edge network. These so-called edge devices can bridge the gap between CPS and Cloud. The intelligent computing and storage on edge devices offer the potential to solve the communication problem, real-time problem, and security problem.

The accepted papers represent the urgent needs to be considered in developing an intelligent computing for edge devices and to fill the gap between CPS and Cloud. Moreover, the outcome of this special section exhibits the latest research achievements and state-of-art research results to solve intelligent computing issues for CPCS.

INTELLIGENT COMPUTING FOR EDGE DEVICES IN CYBER PHYSICAL AND CLOUD SYSTEMS

Through a peer-review process, we have accepted 10 submissions, and each selected article has received at least two rounds of rigorous reviews. The accepted articles represent activities in areas around the world and propose various theoretical research results and applications on applying Intelligent Edge Computing for Cyber Physical and Cloud Systems in industrial informatics. A brief introduction is provided to each of the articles as follows:

The first three articles introduce intelligent computing for edge devices in Cyber Physical and Cloud Systems. In "Deep Reinforcement Learning for Vehicular Edge Computing: An Intelligent Offloading System," Zhaolong Ning et al. construct an intelligent offloading system for vehicular edge computing in the development of smart vehicles, bringing a comfortable and safe environment to drivers and passengers. In this research, the author has investigated two-sided matching scheme and a deep reinforcement learning to solve sub-optimization problems. Numerical results demonstrate that the matching algorithm in the first module can reach 95% of the exhaustive algorithm in different network scenarios and decrease the execution time by more than 90%. For the

2157-6904/2019/12-ART60e
https://doi.org/10.1145/3372277

second module, Double DQN (DDQN)-based algorithm performs 10%–15% better than that of the traditional Deep Q-Network (DQN) method.

The article entitled "A Trust Computing–based Security Routing (TDSR) Scheme for Cyber Physical Systems," by Yuxin Liu et al., proposed the TDSR scheme to establish security routes from source nodes to the sink for environmentally powered wireless sensor network (EPWSN) under malicious environment to ensure network security. Performance evaluation through simulation is carried out for success routing ratio, compromised node detection ratio, and detection routing overhead. The experiment results show that the performance can be improved in the TDSR scheme compared to previous schemes.

The article titled "Crowdsourcing Mechanism for Trust Evaluation in CPCS Based on Intelligent Mobile Edge Computing," by Tian Wang et al., proposed a novel trust evaluation mechanism using crowdsourcing and Intelligent Mobile Edge Computing. In this article, two incentive mechanisms, i.e., Trustworthy Incentive and Quality-aware Trustworthy Incentive Mechanisms, are proposed for motivating mobile edge users to conduct trust evaluation. The first one aims to motivate edge users to upload their real information about their capability and costs. The purpose of the second one is to motivate edge users to make trustworthy effort to conduct tasks and report results. Detailed theoretical analysis demonstrates the validity of Quality-aware Trustworthy Incentive Mechanism from data trustfulness, effort trustfulness, and quality trustfulness, respectively.

INFLUENCE MEASURES AND MODEL IN CYBER PHYSICAL AND CLOUD SYSTEMS

The next four articles present the influence measures for modelling of cyber physical and cloud systems under edge computing environment. In "Edge-enabled Disaster Rescue: A Case Study of Searching for Missing People," Fang Liu et al. design a highly efficient disaster rescue framework based on edge computing that uses a computer vision detector to understand the contents of crowdsourced photos, uploads only relevant images that meet the requirements to the cloud, and utilizes the uploaded images to assist with rescue efforts. In this article, authors have proposed an adaptive detection mechanism to improve the efficiency under unstable network bandwidth conditions. The experimental results of this study have used a prototype implementation case study analysis such as running on four Android mobile phones, an x86-based edge server, and a Face++ cloud server.

In the article titled "Using Sparse Representation to Detect Anomalies in Complex WSNs," Xiaoming Li et al. propose an algorithm based on dictionary learning to detect faulty sensor anomalies in the entire interdependent network system. In this article, a dictionary learning algorithm based on a non-negative constraint is developed, and a sparse representation anomaly node detection method for sensor networks is proposed based on the dictionary learning. An experiment on a specific thermal power plant in China to verify the robustness of the proposed method in detecting abnormal nodes against four state-of-the-art approaches proved the method is more robust. Furthermore, the experiments are conducted on the obtained abnormal nodes to prove the interdependence of multi-layer sensor networks and reveal the conditions and causes of a system crash.

In the article titled "Energy-efficient Static Task Scheduling on VFI-based NoC-HMPSoCs for Intelligent Edge Devices in Cyber-physical Systems," Umair Ullah Tariq et al. investigate energy-efficient and contention-aware scheduling on intelligent edge devices. This study investigates energy-efficient and contention-aware static scheduling for tasks with precedence and deadline constraints on intelligent edge devices deploying heterogeneous Voltage Frequency Island (VFI)-based NoC-MPSoCs (VFI-NoC-HMPSoC) with DVFS-enabled processors. Unlike the existing population-based optimization algorithms, this article proposes a novel population-based algorithm called ARSH-FATI that can dynamically switch between explorative and exploitative search modes at run-time. The proposed static scheduler ARHS-FATI collectively performs task mapping, scheduling, and voltage scaling. Consequently, its performance is superior to the existing state-of-the-art approach proposed for homogeneous VFI-based NoC-MPSoCs.

In the next article, "Lightweight Convolution Neural Networks for Mobile Edge Computing in Transportation Cyber Physical Systems," Dai, Hong-Ning et al. design and develop a lightweight deep learning model to support mobile edge computing (MEC) applications in transportation cyber-physical systems (T-CPS). Experiments are conducted at a realistic MEC platform. Extensive experimental results show that proposed lightweight CNN-FC can greatly decrease the number of unnecessary parameters, thereby reducing the model size while maintaining the high accuracy in contrast to conventional CNN models. In addition, the authors have evaluated the performance of the proposed model via conducting experiments at a realistic MEC platform. Specifically, experimental results at this MEC platform show that the proposed model can maintain high accuracy while preserving the portable model size.

APPLICATIONS, DETECTION, TRANSMISSION, AND TRACKING FOR CYBER PHYSICAL AND CLOUD SYSTEMS

The last three articles introduce several interesting applications, detection, transmission, and tracking for Cyber Physical and Cloud Systems. In the article "Comparison and Modelling of Country-level Micro-blog User and Activity in Cyber-physical-social Systems using Weibo and Twitter Data," Po Yang et al. design a Country Level Micro-Blog User (CLMB) behaviour and activity model for supporting CPSS applications. They propose a CLMB model for analysis of micro-blogging user behaviour and their activity across different countries in the CPSS applications. They evaluated CLBM model under the collected microblog dataset from 16 countries with the largest number of representative and active users in the world.

The article titled "Efficient and Privacy-preserving Fog-assisted Health Data Sharing Scheme," by Wenjuan Tang et al., proposes an efficient and privacy-preserving fog-assisted health data sharing (PFHDS) scheme for e-healthcare systems. Moreover, this study is to design an enhanced attribute-based encryption method through combination of a personal access policy on patients and a professional access policy on the fog node for effective medical service provision. Performance evaluations demonstrate cost-efficient encryption computation, storage, and energy consumption.

The last article, titled "Secure Deduplication System with Active Key Update and Its Application in IoT," by Jin Li et al., proposes a novel encryption scheme for secure chunk-level deduplication. Based on this scheme, they present two constructions of the secure deduplication system that support an efficient key update protocol. The key update protocol does not involve any edge node in computational tasks, so the deduplication system can adopt an active key update strategy. Moreover, advance construction can provide access to privacy assurances for edge nodes. The security analysis is given in terms of the proposed threat model. The experimental analysis demonstrates that the proposed deduplication system is practical.

Prof. Weijia Jia
University of Macau, Macau
E-mail: weijiaj@gmail.com

Prof. Geyong Min
University of Exeter, UK
E-mail: G.Min@exeter.ac.uk

Prof. Yang Xiang
Swinburne University of Technology, Australia
E-mail: yxiang@swin.edu.au

Dr. Arun Kumar Sangaiah
VIT University, Vellore, India
E-mail: arunkumarsangaiah@gmail.com