Computing (2021) 103:357–360
https://doi.org/10.1007/s00607-020-00892-9

EDITORIAL

Special issue on intelligent Edge, Fog, Cloud and Internet of Things (IoT)-based services

Leonard Barolli[1] · Farookh Hussain[2] · Makoto Takizawa[3]

Published online: 6 January 2021

Networks of today are going through a rapid evolution. Different kinds of networks with different characteristics are emerging and they are integrating in heterogeneous networks. For these reasons, there are many interconnection problems which may occur at different levels in the hardware and software design of communicating entities and communication networks. These kinds of networks need to manage an increasing usage demand, provide support for a significant number of services, guarantee their QoS, and optimize the utilization of network resources. Therefore, architectures and algorithms in these networks become very complex and it seems imperative to focus on new models and methods as well as mechanisms, which can enable the network to perform adaptive behaviors.

Now, the information services are constructed by new technologies like intelligent Edge, Fog, Cloud and Internet of Things (IoT)-based computing and networking. The intersection of these research areas with artificial intelligence (AI) is very important topic. The emergence of Edge Computing, Fog Computing, Cloud Computing and IoT Networks bring new research problems and issues. To address these problems, this Special Issue (SI) is focused on the interplay among the above computational platforms, networking, security, and intelligent computing methods. For this SI, we received 27 papers and accepted 8 papers.

✉ Leonard Barolli
barolli@fit.ac.jp

Farookh Hussain
Farookh.Hussain@uts.edu.au

Makoto Takizawa
makoto.takizawa@computer.org

[1] Department of Information and Communication Engineering, Fukuoka Institute of Technology (FIT), 3-30-1 Wajiro-Higashi, Higashi-Ku, Fukuoka 811-0295, Japan

[2] School of Computer Science, University of Technology Sydney, 15 Broadway, Ultimo, NSW, Australia

[3] Department of Advanced Sciences, Faculty of Science and Engineering, Hosei University, 3-7-2 Kajino-Cho, Koganei-Shi, Tokyo 184-8584, Japan

In the first paper by Almansor et al., the authors developed a supervised ensemble automated approach that measures Chatbot Quality of Service (CQoS) based on dialogue breakdown. The proposed approach is able to label the datasets based on sentiment considering the context of the conversion to predict the breakdown. The authors present a supervised ensemble model to measure the CQoS based on breakdown. Then, they handle this problem by using a hand-over mechanism that transfers the user to a live agent. The authors carry out several experiments considering some datasets and state-of-the-art models. They found that using sentiment as a trigger for breakdown outperforms human annotation. The authors conclude that the knowledge acquired from the supervised ensemble model can help to measure CQoS based on detecting the breakdown in conversation.

In the second paper by Durresi et al., the authors investigate the potential privacy risk of mobile Internet users, including the Internet of Things. They proposed a scalable system built on top of public cloud services that can hide a mobile user's network location and traffic from communication peers. The proposed system creates a dynamic distributed proxy network for each mobile user to minimize performance overhead and operation costs.

In the third paper by Seunghyun Park and Hyunhee Park, in order to improve the performance of the oversampling and undersampling approaches, the authors propose an oversampling ensemble method based on the slow-start algorithm (COUSS). The proposed method is based on the congestion control algorithm of the transmission control protocol. Therefore, an imbalanced dataset oversamples until overfitting occurs, based on a minimally applied undersampling dataset. The simulation results obtained using the KDD99 dataset show that the proposed COUSS method improves the F1 score by 8.639%, 6.858%, 5.003%, and 4.074% compared to synthetic minority oversampling technique (SMOTE), borderline-SMOTE, adaptive synthetic sampling, and generative adversarial network oversampling algorithms, respectively. Therefore, the COUSS method can be used as a practical solution in data analysis applications.

In the fourth paper by Yakubu et al., the authors propose a Secure Multi-Resource Trading (SMRT) model that is based on public Ethereum blockchain. The SMRT allows participant of a SMP to trade multiple resources and initiate parallel transactions. The detailed security analysis and adversary model are presented to test the effectiveness and to assess the resilience of the proposed model against the double-spending attack. The adversary model is based on partial progress towards block production which is influenced by time advantage and average computing power. The simulation analysis and comparison of SMRT is also presented in terms of security, performance, cost and latency of transactions. It is observed that SMRT not only provides protection against the double spending attack, but it also reduces the computational overhead of the proposed model up to 50% compared to existing trading models.

In the fifth paper by Kwon et al., the authors analyze the countermeasures and verification methods of eavesdropping vulnerabilities within IoT devices that use the current 5G Non-Standalone (NSA) network system. The network hierarchical structure of 5G-based IoT was evaluated for vulnerability analysis, performed separately for 5G Access Stratum (AS), Non-Access Stratum (NAS) and Internet Protocol (IP)

Multimedia Subsystem (IMS). The AS keystream reuse, NAS null-ciphering and Multimedia Subscriber (IMS) IP security (IPsec) off vulnerabilities were tested on mobile carrier networks to validate it on the 5G NSA network as well. A countermeasure against each vulnerability was presented and the authors show that the proposed Intrusion Detection System (IDS) based on these countermeasures successfully detected the presented controlled attacks.

In the sixth paper by Xie et al., the authors propose a novel differential privacy optimization algorithm based on quantum particle swarm theory which is suitable for both convex optimization and non-convex optimization. The authors apply adaptive contraction–expansion and chaotic search to overcome the premature problem and provide theoretical analysis in terms of convergence and privacy protection. They verify through experiments that the performance of the algorithm is consistent with the theoretical analysis.

In the seventh paper by Christian Salim and Nathalie Mitton, the authors propose a data reduction technique based on a data correlation technique by applying the Pearson correlation coefficient functions and equations in Wireless Sensor Networks (WSNs) implemented for agriculture to detect any abnormal situation in the meteorological data. This data reduction technique relies on the observation of the variation of every monitored parameter as well as the degree of correlation between different parameters. This approach is validated by MATLAB simulations using real meteorological datasets from Weather-Underground sensor network. The results show the validity of the proposed approach which reduces the amount of data by a percentage up to 88% while maintaining the accuracy of the information having a standard deviation of 2 degrees for the temperature and 7% for the humidity.

In the eighth paper by Xhafa et al., the authors propose some clustering techniques for creating virtual computing nodes from Fog/Edge nodes by combining semantic description of resources with semantic clustering techniques. Then, the authors use such clusters for optimal allocation (via heuristics and Liner Programming) of applications to virtual computing nodes. The simulation results are reported to support the feasibility of the model and efficacy of the proposed approach. The First Fit Heuristic Algorithm (FFHA) outperformed ILP method for medium and large size instances. Likewise, FFHA performed more consistently than ILP on various experimental setting. The simulation results showed that the proposed clustering techniques deliver relatively fast response times, while enabling the service of a larger number of applications, with more demanding requirements.

As we conclude this overview, we would like to thank all the authors for submitting their papers and the reviewers for their good work to make it possible to publish this SI.

In particular, we would like to express our special thanks to Editors-in-Chief of Computing Journal Prof. Schahram Dustdar for his strong encouragement and support.

1 List of accepted papers

1. Ebtesam Hussain Almansor, Farookh Khadeer Hussain, Omar Khadeer Hussain, Supervised Ensemble Sentiment-Based Framework to Measure Chatbot Quality of Services.

2. Arjan Durresi, Ping Zhang, Mimoza Durresi, Internet Network Location Privacy Protection with Multi-access Edge Computing.
3. Seunghyun Park and Hyunhee Park, Combined Oversampling and Undersampling Method Based on Slow-Start Algorithm for Imbalanced Network Traffic.
4. Bello Musa Yakubu, Majid Iqbal Khan, Nadeem Javaid, Abid Khan, Blockchain-based Secure Multi-Resource Trading Model for Smart Marketplace.
5. Sungmoon Kwon, Seongmin Park, HyungJin Cho, Youngkwon Park, Dowon Kim, Kangbin Yim, Towards 5G-based IoT Security Analysis against Vo5G Eavesdropping.
6. Yun Xie, Peng Li, Jindan Zhang, Marek R. Ogiela, Differential Privacy Distributed Learning Under Chaotic Quantum Particle Swarm Optimization.
7. Christian Salim and Nathalie Mitton, K-Predictions Based Data Reduction Approach in WSN for Smart Agriculture.
8. Fatos Xhafa, Alhassan Aly, Angel A Juan, Allocation of Applications to Fog Resources via Semantic Clustering Techniques With Scenarios from Intelligent Transportation Systems.