J Supercomput (2016) 72:1–4
DOI 10.1007/s11227-015-1595-5

EDITORIAL

Editorial: A special section on "Emerging Platform Technologies"

Changhoon Lee[1] · **Kyusuk Han**[2] · **Juan Li**[3]

Published online: 18 January 2016

1 Introduction

During the last decade, many countries have adopted in recent years roadmap for developing the future infrastructure in emerging platform technology areas such as automobile, big data processing technology, biotechnology, nanotechnology, grid computing and ICT (Information and Communication Technology).

Platform technologies consist of tools, techniques and instruments that enable entirely novel approaches for scientific investigation across a broad range of disciplines, which have captured a significant fraction of all science interests during the last decade. It leads to emerging needs to seek and identify exceptional ideas for revolutionary new platform technologies (from across the full breadth of science, technology, engineering, and math) that could lead to breakthrough advances in the broadly defined life sciences.

The aim of this issue is to promote interdisciplinary research in platform technologies and other applied fields in mathematics, engineering and sciences to investigate specific methodologies and develop technologies that will contribute to the development of the future infrastructure.

✉ Changhoon Lee
changhoonlee08@gmail.com

1 Department of Computer Science and Engineering, Seoul National University of Science and Technology, Seoul, Korea

2 University of Michigan, Detroit, MI, USA

3 Department of Computer Science, North Dakota State University (NDSU), Fargo, ND, USA

2 The papers in part I of this special section

We finally selected 16 manuscripts for part I of this Special Issue. Each manuscript selected was blindly reviewed by at least three reviewers consisting of guest editors and external reviewers.

The first paper in this special issue "Optimal Filter Based on Scale-Invariance Generation of Natural Images", by Feng Jiang et al. proposes a novel scale-invariance nature image prior model by estimating and obtaining the optimal filter whose response distributions have the least KL divergence throughout the scales, and reflects the unique scale invariance character of the current image. This adaptive filter and its responses characterize the scale invariance property more accurately and effectively and are further utilized to model the statistics scale invariance prior.

The second paper entitled "A Novel Secure Architecture of the Virtualized Server System" by Sang Kon Kim et al. proposes a security layer for the secure architecture of a virtualized server system. The authors also constructed a table which summarizes the relationship between the security issues and security elements. According to the results, an appropriate combination of these security elements can effectively prevent the common security issues surrounding virtualized servers. This research is helpful for the design or testing of security layers in virtualized servers.

The third paper is "Smart Knowledge Sharing System for Cyberinfrastructure", by Jin Kim et al. based on the concept of smart knowledge sharing system. This paper introduced a sharing system between smart device and particular cyberinfrastructure (CI) named CyberLab, and also presented a new perspective for management by redefining the CI. In future, through the test by CyberLab user, smart knowledge sharing system is expected to be improved in terms of functionality, easy-access and so on.

The fourth paper in this issue is "A New Approach to Deploying Private Mobile Network Exploits", by Eunyoung Kim and Jongsub Moon. This paper established an experimental environment for private Mobile Communication Systems (MCS) using an open project. The authors show the feasibility of attacks resulting in the leakage of private information, attacks on OpenBSC control, and DNS spoofing at the network level, all of which are possible in commercial MCSs and without subscriber knowledge. A reliable technical solution is also considered to reduce the information collection and utilization of private mobile network threats.

The fifth paper in this issue entitled "Trust Model at Service Layer of Cloud Computing for Educational Institutes" by Sohail Jabbar et al. proposes a model which helps the cloud service users in finding out the efficient and trustworthy cloud service provider (CSP) according to the requirements of user (EI). The proposed model evaluates CSP in terms of services they are offering and quality of service as well. The most differentiable feature of this model is its customized and flexible approach.

The sixth paper "Adaptive Internet of things and Web of things convergence platform for Internet of reality services" by Jaehak Yu et al. proposes an adaptive Internet of things (IoT) and Web of Thing (WoT) convergence platform that can perform mashup of various things and efficient operation in IoT and WoT environments. The proposed platform provides global inter-compatibility to help users to easily communicate with each other by connecting through the webs. In addition, this proposal can guarantee

an efficient IoT or WoT platform management, adaptive synchronization between the things, a stable platform environment, and creating new services.

The seventh paper in this special issue "Security Experts' Capability Design for Future IoT Platform" by Minkyung Kang et al. defines security personnel and various security occupation-specific competencies. In this paper, various occupations were evaluated in regard to their suitability to be labeled security jobs, and core competencies were described for each occupation. How the required core competencies vary according to the occupational cluster is also described. This study can be used as a standard of competencies for given security occupations.

The eighth paper in this issue "Data Concealments with High Privacy in New Technology File System" by Shiuh Jeng Wang et al. proposes a novel scheme called file concealer (FC) to conceal files by only modifying NTFS data. The proposed scheme is one of solutions to conceal privacy information into storage systems to avoid detection such that a rootkit can conceal any type of information including the files, processes, drivers, and network connections on a computer. Experimental results show that antivirus software and data recovery software cannot detect and recover files concealed by FC, and the performance overhead of FC is low.

The ninth paper entitled "Cybercrime Investigation Countermeasure Using Created-Accessed-Modified Model in Cloud Computing Environments", by Dayu Kao, proposes a novel cybercrime investigation countermeasure using a novel CAM model for the control and continuous improvement of digital evidence processes in a cloud environment. The proposed countermeasure is an important contribution to the field of cloud storage forensics, helping in the discovery of further knowledge or information and thereby improving the accuracy of date-time stamps in a cloud storage device.

The tenth paper entitled "Neighbor stability-based VANET clustering for urban vehicular environments" by Jung-Hyok Kwon et al. proposes a neighbor stability-based VANET clustering (NSVC) that can efficiently deliver data in urban vehicular environments. The proposed NSVC supports fast cluster formation, minimizes the number of cluster head elections, and moreover guarantees the reliable delivery of data for emergency messages. The results of the simulation indicate that NSVC achieves better network performance when compared with existing approaches.

The eleventh paper in this special issue "Mutual Authentication Scheme between Bio Sensor Device and Data Manager in Healthcare Environment" by Soon Seok Kim proposes a new authentication scheme of exchanging safely information between Personal Health Device (PHD) to measure the bioinformation of a chronic disease patient at home and Data Manager (DM) to collect the bioinformation from the device. This suggested a new security method which can be applied to Healthcare environment aimed at those geographically living away from hospitals, including the elderly living alone, the handicapped, people living in islands and highlands, and chronic disease patients. In addition, the proposed scheme is very useful in the point that it added the mutual authentication function to Personal Health Device and Data Manager to implement safer and more efficient e-Health environment.

The twelfth paper "Coloring-Based Scheduling for Interactive Game Application with Wireless Body Area Networks" by Sanghyun Seo et al. proposes a new coloring-based scheduling method to avoid the interference by allocating different time-slots to adjacent WBANs and to increase the total throughput by allocating more time-slots

to traffic-intensive WBANs. From the results, in the interactive game application with WBANs which have a short communication range, the game environment can be set to be optimal in terms of a place area (i.e., a game room area) and the number of vertexes (i.e., the number of game players).

The thirteenth paper in this special issue "Real-time Motion Control on Android Platform" by Hyeongseok Kang et al. proposes an application-centric approach to achieve good real-time performance on the Android platform, which is based on multi-core partitioning and partition-aware application design. The proposed application is designed in combination of a real-time Android service daemon and a non-real-time Android UI application with a shared memory area as the communication buffer between the two.

The fourteenth paper in this special issue "A Novel Security Architecture of Electronic Vehicle System for Smart Grid Communication" by Kyu-min Cho et al. proposes a novel security architecture for Smart Grid Communication. The proposed architecture is designed based on a logical architecture considering the case of electric vehicle telecommunication, the security techniques, and algorithms applicable to the Smart Grid environment, and applying them to address its security requirements and threats. The Smart Grid security architecture from the telecommunication perspective proposed is expected to be used as baseline data for the application of security to the field of Smart Grid in the future.

The fifteenth paper in this special issue "Anti-Debugging Scheme for Protecting Mobile Apps on Android Platform" by Haehyun Cho et al. proposes an anti-debugging technique for native code debugging and managed code debugging of android apps. Through experiments, the feasibility of the proposed scheme is also verified. By having the proposed method to prevent against the JDWP debugger hook the function pointer to cause the application program to be terminated if debugging occurs, the validity of the method is ensured.

The last paper in this special issue entitled "Privacy Enhanced Middleware for Location based Sub-Community Discovery in Implicit Social Groups" by Ahmed M. Elmisery et al. proposes an enhanced middleware for collaborative privacy (EMCP) which is equipped with cryptography protocols to facilitate private discovery of sub-communities from the sanitized version of participants' profiles in a university scenario. In addition, a new secure distance detection (SDD) protocol that is utilized to calculate the distance between participants and different representatives without revealing their accurate locations is outlined. The authors also developed a formal model for the tradeoff between privacy level and accuracy of referrals. The experimental results show that achieving privacy in discovering sub-communities is feasible under our proposed middleware without hampering the accuracy of the referrals.

Acknowledgments We would like to thank all authors for their contributions to this special issue. Our special thanks also go to Editor-in-Chief Professor Hamid R. Arabnia and all editorial staffs for their valuable supports throughout the preparation and publication of this special section. Moreover, we extend our thanks to all external reviewers for their excellent help in reviewing the manuscripts.