World Wide Web (2020) 23:1089–1100
https://doi.org/10.1007/s11280-019-00773-y

Smart computing and cyber technology for cyberization

Xiaokang Zhou [1,2] · Flavia C. Delicato [3] · Kevin I-Kai Wang [4] · Runhe Huang [5]

Published online: 3 January 2020

1 Introduction

Following the well-known concepts of computerization and informatization, an emerging era of cyberization, which is considered as a reformation of the present physical, social and mental worlds, has become a hotly discussed trend in the new cyber world. Cyberization refers to using communication and computer technologies to interconnect computers and various electronic terminal devices distributed in different locations. It allows users to share software, hardware and data resources according to certain network protocols. Cyberization has greatly improved the practical utility of computers and has been widely applied in transportation, finance, business management, education, telecommunications, commerce, and so on in our daily life [1].

During the cyberization process, a large number of real things will conjugatively map to various kinds and levels of cyber existence in cyber world. It is said that cyberization has already taken place in a variety of fields along with the development of several emerging computing paradigms and information communication technologies, such as ubiquitous/pervasive computing, social computing and networking, and wearable technologies, etc. Specifically, with the rapid growth of Internet of Things and cognitive cyber-physical systems, more and more digital things or cyber entities, are engaged or generated in the integrated cyber world. Emerging technologies in smart environments, such as smart computing and smart objects, become very significant, promising, and enabling issues in cyberization, to enhance

This article belongs to the Topical Collection: *Special Issue on Smart Computing and Cyber Technology for Cyberization*
Guest Editors: Xiaokang Zhou, Flavia C. Delicato, Kevin I-Kai Wang, and Runhe Huang

✉ Xiaokang Zhou
zhou@biwako.shiga-u.ac.jp

[1] Faculty of Data Science, Shiga University, Shiga, Japan

[2] RIKEN Center for Advanced Intelligence Project, RIKEN, Tokyo, Japan

[3] Department of Computer Science, Fluminense Federal University, Niteroi, Brazil

[4] Department of Electrical, Computer, and Software Engineering, The University of Auckland, Auckland, New Zealand

[5] Faculty of Computer and Information Sciences, Hosei University, Tokyo, Japan

the efficiency of sensing, processing, and communication in the conjugations of physical, social and mental worlds. Accordingly, the cyber technology is playing an important role in developing effective methods of resource management, data acquisition, and pattern recognition across cyber-related systems and applications. All these provide us opportunities to explore smart computing methodologies and computational intelligence algorithms, in order to facilitate the cyberization process in cyber world.

This special issue aims to report high-quality research on recent progress in the various areas related to Smart Computing and Cyber Technology for Cyberization. Our goal is to shed light in the multiple aspects involved in the cyberization, encompassing algorithms, techniques, applications, enabling technologies and platforms, besides security issues. A total of 36 papers were submitted from all over the world. After a careful review process performed by reviewers selected by the Guest Editors, 18 papers were accepted addressing subjects that were classified in the following categories: (i) infrastructure and platforms for inteligent systems, (ii) smart sensors and ad-hoc wireless networks, (iii) behavior and influence analytics in social computing, (iv) machine learning and intelligent applications, and (v) privacy and security in smart computing. The detailed contributions of each paper are summarized in the next section.

2 Summary of this issue

2.1 Infrastructure and platforms for intelligent systems

An important component in the cyberization process is the computational intelligence techniques and methods that are at the core of cyber world enabling processes. Recently there has been a tremendous advance in the fields of machine learning (ML) and artificial intelligence (AI). However, much of this advance has focused on algorithms and their applications. Much less emphasis has been given to the underlying infrastructure of these intelligent systems. Currently, the mainstream in ML/AI consists in work being done individually by experts in the field, following ad-hoc processes that make collaboration difficult, and with little support from abstractions and tooling to facilitate the deployment of intelligent systems at scale. Ultimately, this is mainly due to a delay in infrastructure evolution, which has so far been far outweighed by innovation in machine learning techniques. One can say that the systems and tools that helped usher in the present era of hands-on machine learning are not suitable to feed future generations of the intelligent applications they have generated. Therefore, it is important to advance not only the algorithms, but also the infrastructure and computing platforms that allow the effective and efficient execution of such algorithms.

In the context of ubiquitous/pervasive intelligent systems, as well as in the cyber-physical systems (CPSs), cloud computing has been the most prevailing model and platform for data processing and storage. Because of the richness of resources typical of cloud platforms, cloud-based CPSs and cloud-assisted IoT extend and augment the computing capacity of CPSs to conduct resource-hungry applications. The Cloud computing model is keen to use centralized shared resources and addresses the raising popularity of smart apps by integrating exclusive resources and the data obtained from them [2].

In order to provision the physical resources dynamically, virtualized technology is extensively used for resource management in the cloud platforms, which provides an effective way to improve the resource efficiency of the cloud-based CPSs. Running applications on the virtual machines (VMs) makes it possible for high resource utilization and low energy consumption [3]. Although virtualization techniques have been extensively studied in the cloud computing field, there are still several open issues involved in the allocation and migration of VMs to meet the quality of service (QoS) demands of cloud-based CPSs. A key challenge involves considering the benefits of migrating VMs to provide better QoS to the user while taking into account migration costs, for example in terms of transmission delays. In addition, energy consumption in cloud-based systems is also an increasingly relevant challenge to consider. To meet the growing demand for new scenarios such as CPSs and IoT, capabilities of cloud data centers have grown steadily. Such growth results in the increasing power consumption of these data centers. In times of energy crisis and with the growing demand for greener and more sustainable technology solutions, reducing energy consumption in data centers has become a key goal. The authors in the paper "*A QoS-Aware Virtual Machine Scheduling Method for Energy Conservation in Cloud-based Cyber-Physical Systems*" [3] aim to tackle the aforementioned challenges. Their goal is to find an optimal VM scheduling strategy in cloud-based CPSs with QoS enhancement. For such, they propose a QoS-aware VM scheduling method for energy conservation, named QVMS. By offloading several applications to other physical machines (PMs), the workloads on some under-load physical servers are migrated out, and these servers could be set to idle mode for energy saving. In the paper, they first define some basic concepts and present the system model. Then, they formalize the objective function and present the constraints assumed to model the solution. Non-dominated Sorting Genetic Algorithm (NSGA-III) is adopted to find the optimal VM scheduling strategies and achieve the goal of QoS enhancement including energy consumption, downtime and resource utilization. Besides, SAW (Simple Additive Weighting) and MCDM (Multiple Criteria Decision Making) are adopted to select the most optimal scheduling strategy. They performed extensive experimental evaluations to verify the effectiveness of their proposed VM scheduling method.

However, despite the popularity of cloud computing as a backend of intelligent ubiquitous systems and CPSs, newly emerging applications and information technologies are very demanding when it comes to the latency and bandwidth. Their requirements for the optimized transport network and processing of data performed as close to the end devices as possible is also rapidly increasing [4]. Some of the drawbacks of cloud platforms such as latency and jitter effects, distance to the server, data security and privacy, and support of mobility cannot be solved by adoption of the hyper-scale cloud computing technology. To overcome some of such limitations, the Edge Computing paradigm has recently emerged as a solution for delivering data and real-time data processing closer to the data source [5]. The combination of Edge Computing with ML/AI gave rise to a new paradigm known as Edge intelligence (EI). EI comprises edge computing that is supported with machine learning algorithms and advanced networking abilities. The implication is that a number of information technology and operational technology industries are gravitating to the edge of the network. The result is that issues such as cybersecurity, self-learning, real-time networks and tailored connectivity can all be adequately dealt with [2]. In their previous work [6], the authors of the paper "*A Lightweight and Cost Effective Edge Intelligence Architecture based on Containerization Technology*" [2] proposed the idea to build and integrate Docker containers within the edge and pinpoint the Edge Intelligence's potential in the vertical-specific scenarios of use. Their current study, included in this Special Issue, extends this idea further and focuses on the utilization of Docker technology into the recognition of human activity. They expect their presented architecture to provide significantly shorter delays in communication and decision-making as well as decrease the costs related to these processes thanks to adoption of lightweight and economical platform.

Since the proposed architecture is using ML algorithms and eliminating any unnecessary communication with cloud, it is able to provide more effective and quick decision-making. Unwanted delays are decreased thanks to avoiding of unreasonable roundtrips. As another contribution of their proposal, decreased use of public wide area networks along with the adoption of local algorithms and caching result in less costly communication. They also promote a good balance of application's, network's and user's requests among the edge and core infrastructure. Finally, the proposed computing model can utilize decisions related to the pre-processed data and adopt alarms traded between several edge devices.

Also leveraging the computational resources at the edge of the network, the paper "*LW-CoEdge: A lightweight virtualization model and collaboration process for Edge Computing*" [7] proposes a novel distributed and lightweight virtualization model targeting the edge tier. Besides a novel virtualization model tailored to the edge tier and meeting the specific requirements of IoT applications, their proposal encompasses a set of heuristic algorithms along with a P2P collaboration process to operate upon the virtualization model. The algorithms perform (i) a distributed resource management process, and (ii) data sharing among neighboring virtual nodes (VNs, deployed at edge nodes). The distributed resource management process provides each edge node with decision-making capability, engaging neighboring edge nodes to allocate or provision on-demand VNs. Thus, the distributed resource management improves system performance, serving more requests and handling edge node geographical distribution. Meanwhile, data sharing reduces the data transmissions between end devices and edge nodes, saving energy and reducing data traffic for IoT-edge infrastructures.

Among the existing CPSs, manufacturing and enterprise applications are one of the major drivers of advanced and intelligent networked systems following the trend of Industry 4.0. Massive data are generated in a distributed fashion and cross-domain data need to be shared and analyzed in an efficient manner to realize an effective supply chain management. Therefore, master data management (MDM) that manages how data are stored in a distributed system plays a critical role for enterprise data warehousing and analyses. The paper "*Master Data Management for Manufacturing Big Data: A Method of Evaluation for Data Network*" [8] proposes a multi-layer master data management architecture and investigates the use of Set Pair Analysis (SAP) to model the distributed data network. The proposed methodology is validated using an aviation enterprise data and has demonstrated the ability to support timely update, response, distribution of data at each stage of the supply chain.

2.2 Smart sensors and ad-hoc wireless networks

CPSs rely on a strong synergy between computational and physical components. A CPS is the integration of abstract computations and physical processes [9] where sensors, actuators, and embedded devices are networked to sense, monitor, and control the physical world. Therefore, smart sensors and wireless sensor networks are major components of CPSs. Wireless sensor networks (WSNs) are composed of tiny devices equipped with sensing, processing, storage, and wireless communication capabilities. Each node of the network can typically have several sensing units, able to perform measurements of physical variables, such as temperature, luminosity, humidity, and vibration, thus being the main components to create a perception of the physical world. WSN nodes operate collaboratively, extracting environmental data, performing same (often) simple processing, and then transmitting them to external systems, via sink nodes, to be analyzed and further processed.

Sensor nodes are severely constrained regarding memory, energy, and processing capabilities. Therefore, several approaches have been proposed to reduce the energy consumption of these nodes in order to extend the overall lifetime of the system. Since radio communication is the dominant factor of energy consumption in most WSN (except for the hungry devices of multimedia sensor networks), an effective approach is the reduction of data transmission between the sink and the sensing nodes. One of the most commonly used technique to reduce radio communication is the dual prediction mechanism and several proposals are reported in the literature [10–12]. However, while all existing approaches have been proven to be very effective in reducing the amount of data reported to the sink, their efficiency is countered by an increase in complexity. Moreover, they are very sensitive to data loss which renders the dual prediction mechanism obsolete [13]. In the paper "*Fault Tolerant Data Transmission Reduction Technique in Wireless Sensor Networks*" [13], the authors present an alternative technique that has as a major benefit to be simple yet robust, and more effective in terms of prediction accuracy and data reduction. Their approach exploits the fact that sensor data changes smoothly over time, therefore they leverage the prediction model proposed in [14] to forecast future readings. They coupled this technique with a data reconstruction algorithm [15] that exploits both temporal smoothness and spatial correlation among different sensed features in order to estimate missing values.

Vehicular ad hoc networks (VANETs) are a subclass of mobile ad hoc networks (MANETs), and a promising approach for future intelligent transportation systems (ITS). A VANET typically supports two communication models, namely Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I). Currently, most VANET applications rely on V2V communications since they do not require costly infrastructure. However, as VANET is a very dynamic network, information must be exchanged between mobile vehicles in an efficient way by avoiding as far as possible the broadcast storm problem, that occur whenever a huge number of vehicles broadcast messages at the same time thus leading to a network saturation, packet delay and collision issues. In this context, data aggregation is an appealing approach allowing to integrate several data about similar events to generate a summary (aka aggregate) and as a consequence potentially reducing the network traffic. There are several proposals for data aggregation in VANETs already reported in the literature. However, the highly complex urban and highway networks produce an overwhelming traffic information data that requires efficient selection criteria and smart filtering before the aggregation process. The design of an efficient data aggregation approach that combines correlated traffic information or Floating Car Data (FCD) is still a challenging issue. The authors of the paper "*Towards a Smarter Directional Data Aggregation in VANETs*" [16] introduce a new data aggregation protocol, called Smart Directional Data Aggregation (SDDA), with the goal of selecting the most appropriate FCD messages that have to be aggregated.

Based on the aforementioned research works, it is clear that the future CPSs and intelligent applications heavily rely on the presence and widespread of physical sensors and WSNs. To ensure the functionality of an application, such as intruder detection, it is of critical importance to guarantee the coverage and availability of wireless sensors during deployment. As such, barrier coverage is a critical issue for wireless sensor deployment for many industrial and military applications, where each wireless sensor can sense within its range and a collection of wireless sensors can be deployed to cover the entire range of a barrier. Over the last decade, different barrier coverage algorithms had been established for different types of sensors such as seismic [17] and acoustic [18] sensors, while in recent years, more research efforts are dedicated to radar sensor systems [19, 20]. In *"Optimal Placement of Barrier Coverage in*

Heterogeneous Bistatic Radar Sensor Networks" [21], authors investigate the barrier coverage problem for bistatic radar sensor systems. Different to the traditional passive sensing model, the Cassini oval sensing model is investigated and an optimal placement strategy for heterogeneous transmitters and receivers has been proposed to achieve maximum barrier length coverage. The proposed algorithm has been validated through theoretical simulations to demonstrate the optimal coverage.

Cyber-social networks have significantly improved social relationships among mobile users across device-to-device communications. In the paper *"A Detailed Review of D2D Cache in Helper Selection*" [22], the authors present a survey work which focuses on D2D helper selection techniques according to three basic categories, including the network frame, computing method, and social-aware attribute. Differing from other surveys which mainly consider the energy consumption and latency minimization in D2D networks, they discuss the selection of D2D helper based on different network architectures, such as content distribution networks, peer-to-peer networks, named data networks, cellular networks, and vehicular ad-hoc networks. In particular, a variety of computing paradigms are taken into account to classify D2D helper selection techniques, such as mobile cloud computing, fog computing, and mobile edge computing.

2.3 Behavior and influence analytics in social computing

In recent years, the recommendation system has been well developed and is playing an important role across social media. In the paper *"ICFR: An Effective Incremental Collaborative Filtering based Recommendation Architecture for Personalized Websites"* [23], the user-based collaborative filtering algorithm is applied in an incremental recommendation implementation method, in which three important elements: user, item, and rating, are redefined, and relationships between user preferences and recommended content are utilized to improve the user-based collaborative filtering algorithm. Moreover, users' browsing behaviors are extracted based on the analysis of Web logs from personalized websites, which can facilitate the update of users' historical preference in the design of an incremental algorithm. Experiments demonstrate the high performance of the proposed method comparing with traditional updating methods.

Following the rapid development of mobile social networks, the paper *"From Crowdsourcing to Crowdmining: Using Implicit Human Intelligence for Better Understanding of Crowdsourced Data"* [24] discusses the concept of crowdmining and presents a generic model for the development of crowdmining systems. The basic idea is to discover and better utilize the implicit human intelligence hidden in individual behavior patterns and crowd-object interaction patterns under a certain community context. The authors introduce a basic framework to understand the crowdsourced data with a formal description and discuss its usage in several general tasks in terms of data mining including classification, filtering and grouping. Based on these, they describe two case studies, namely the crowdevent and crowdtrip, which utilize the power of implicit human intelligence to facilitate the event sharing and trip planning respectively. Detailed scenario applications are presented, and the experiment evaluation demonstrate the effectiveness of the proposed method in event localization and detection, and travel route generation using online/offline crowdsourced data.

Behavioral analysis has drawn more and more attentions for mobile computing application in big data environments. In the paper *"TBI2Flow: Travel Behavioral Inertia Based Long-Term Taxi Passenger Flow Prediction"* [25], the authors focus on the analysis of travel patterns of taxis in cities using GPS data. Specifically, the travel behavioral inertia, which mainly includes two basic components: driver inertia and passenger inertia, is newly defined and introduced as a new metric for the long-term taxi passenger flow prediction. A traffic flow prediction framework, called TBI2Flow, is designed to forecast the distribution of taxi passengers in each small region of a district over different time intervals. The multi-layered neural network is utilized to extract and represent the new features from the taxi trajectory data based on the travel behavior analysis. The results of simulation-based experiments demonstrate the significance and efficiency of the proposed model for traffic management in the design of a smart city.

To deal with the special problem of influence maximization in social networks, the paper *"Three-hop Velocity Attenuation Propagation Model for Influence Maximization in Social Networks"* [26] proposes a three-hop speed attenuation propagation model, based on which the authors design an algorithm for the maximum of influence considering the greedy algorithm with heuristic algorithm. In the constructed network model, the sum of modified degrees of the active nodes is employed to measure the impact of a node. In such a way, the influence of a single node can be effectively modeled and represented, and the lack of subtle influence caused by the three-hop simulation can be further made up. Two different datasets collected from DBLP and Facebook are used to conduct the propagation simulations, and the experiment results demonstrate the high efficiency of the proposed method comparing the traditional greedy algorithms.

2.4 Machine learning and intelligent applications

Sensors and WSNs play an important role in the CPSs and intelligent applications by offering fundamental infrastructure and data sources. However, how to process data to support decision making and provide "intelligence" in systems and applications remains a big challenge. In recent years, ML has demonstrated great potential to many applications in consumer electronics, industrial, and security and surveillance applications. In this special issue, several unique research works are presented on various novel ML techniques and intelligent applications.

As networked systems are becoming more and more complex, automated operations and maintenance are becoming highly important to ensure efficient and reliable system operations. The paper *"Intelligent Maintenance Frameworks of Large-scale Grid using Genetic Algorithm and K-Mediods Clustering Methods"* [27] investigates the automation and scheduling problem of maintenance of a large-scale smart grid system, where a smart grid management system (GMS) is proposed with genetic algorithm and K-mediods clustering. This research identifies and addresses different severity levels according to the faulty devices. The two proposed algorithms are validated with five real-world datasets collected in five different cities in China.

As the technologies evolved, the focus of advanced technologies also shifted to offer more intelligent and more "personalized" services to end users. This trend can be observed from consumer electronics to even manufacturing enterprises to have customized products and services. Therefore, advanced technologies for identifying the user are becoming a very important topic to ensure the delivery of safe and secure personal services. While there are various unimodal personal identification techniques such as password, facial, voice, and fingerprint, each modality exists its own weaknesses which may make the overall system vulnerable. In the paper *"An Accurate Multi-Modal Biometric Identification System for Person Identification via Fusion of Face and Finger Print"* [28], a multi-modal person identification approach is proposed by fusing facial and fingerprint information. The proposed method has been verified with four different datasets and has achieved a promising recognition accuracy of 99.59%.

Different to traditional artificial intelligence (or machine intelligence), research efforts are also dedicated to mimicking unique human traits, behaviors, and personalities. In addition to offer intelligence, researchers are seeking ways to capture and represent the uniqueness of human beings in achieving human-like (or even individual-like) artifacts such as digital avatars and humanoid robots. However, there is yet a comprehensive model to systematically describe human traits and personalities. The paper *"From Affect, Behavior, and Cognition to Personality: An Integrated Personal Character Model for Individual-like Intelligent Artifacts"* [29] offers a broad overview on the existing Personal Character Models (PCMs) from different research arenas and perspectives such as psychology and computational intelligence. A novel PCM is proposed to capture comprehensively personal affects, behaviors, cognition, and the intra- and inter-relationships between these personal characteristics. The feasibility of the proposed PCM model has been demonstrated by extracting representative personal characteristics through various personal data such as wearable devices and cognitive tests.

2.5 Privacy and security in smart computing

One of the biggest concerns in the cyber world is security. By delegating control of physical processes to virtual entities, often accessed via wireless networks, a number of vulnerabilities arise. Without solving security issues, it is not possible to leverage the paradigms linked to the cyber physical systems. As cyber-attacks become more frequent, the research community has presented several approaches (e.g. heuristic methods) to detect and analyze malicious programs (also referred to as malware). However, designing effective and efficient malware detection approaches poses several challenges and still has open issues [30], for example due to counter-malware detection efforts by malware authors and cyber criminals. There are three major approaches for analyzing malware: static, dynamic and hybrid [31, 32], each of them with their own pros and cons. Trying to mitigate some of the drawbacks of current static, dynamic and hybrid malware detection approaches, multi-view learning is a promising solution. Multi-view data are very common in real world applications, where data are often collected from different sources, using different measuring methods. Different data sources form different feature sets, and each set is referred to as a view. Any particular single-view data cannot comprehensively describe the phenomenon under observation. Motivated by this, multi-view learning is an emerging direction in machine learning which considers learning with multiple views to improve the generalization performance [33]. To adapt multi-view learning for malware threat hunting, the authors of the paper "*A Multiview Learning Method for Malware Threat Hunting: Windows, IoT and Android as Case Studies*" [34] leverage the potential of using executable files for either malware or goodware (i.e. non-malware) as the source for multi-view data extraction. The challenge they tackle in this context is to determine what algorithm can be used to effectively extract features from executable files. Existing approaches generally use single view information for malware detection or a combination of some views in the form of a single view [35, 36, 39]. In their paper, the authors propose an efficient ensemble multi-view learning method, which automatically assigns optimized weights to different views. The proposed method is a large margin classifier that improves generalization using a global optimum hypothesis. To demonstrate adaptability of the proposed approach in detecting malware on different platforms, they evaluate their system with datasets comprising Internet of Things (IoT), Windows and Android malware.

In addition to the challenges of dealing with cyber-attacks, which occur in a variety of scenarios and application domains, cyberization poses several security and privacy challenges in the specific scenario of IoT systems. Given its highly dynamic and heterogeneous scenario, besides the opportunistic and ad-hoc nature of interactions, in an IoT system it is difficult to perform identity management, guarantee the trustworthiness of data, detect abnormal behaviors and control the access to various data. Data provenance has the potential to solve some of the aforementioned issues in IoT by recording information about data origins, data operations and processing history from its source to current state. Thus, it becomes possible to track the sources or origins of several types of issues related to abnormal behavior, trustworthiness and data access in IoT. Although long adopted in archives systems and data mining techniques, for the purpose of identifying the owner of an object/data or its origin, creator and how the data was communicated or processed, investigations of data provenance in the context of IoT have only recently begun [37]. The authors in [37] designed a conceptual model as a common architecture of data provenance in IoT. Since this first work, more and more researchers started to pay attention to data provenance in IoT and some provenance management schemes were proposed and applied in various intelligent IoT services. However, the literature still lacked a comprehensive survey on data provenance in IoT. In order to fulfil this gap, the paper "*A Survey on Data Provenance in IoT*" [1] reports the findings of a comprehensive survey on existing works related to this field. As main contributions, the authors (i) propose uniform criteria on data provenance in IoT by analyzing IoT distributed architecture and reviewing data provenance techniques and applications, (ii) review existing works on data provenance in IoT and analyze their pros and cons according to our proposed criteria and security requirements, and (iii) point out a number of open issues based on the thorough survey and attempt to provide guidance for future research in the field of data provenance in IoT by evaluating its recent advance.

The paper *"Secure Limitation Analysis of Public-key Cryptography for Smart Card Settings"* [38] focuses on a special case of smart card used in intelligent application systems with high security requirements. The authors first summarize the features of three main types of attacks in smart card security, including invasive attacks, semi-invasive attacks, and non-invasive attacks, and review the public key cryptography algorithms regarding security issues. Based on these, they convert secure problems of public-key cryptography into the capacity of attack channels of adversaries. The insecure limitation is then defined and introduced based on a communication framework with Shannon information theory. Several metrics are given to analyze security restrictions according to the average mutual and conditional mutual information. The authors discuss a series of attack models with the security limitation of encryption, such as ciphertext-only attack channel model, chosen plaintext attack channel Model, chosen ciphertext attack channel Model, adaptive chosen ciphertext attack channel Model, direct forgery attack channel Model, and tampering attack channel model.

3 Final remarks

This special issue aims to promote the development of cyber-related information and communication technologies in smart computing. In Particular, a variety of important topics are addressed in this special issue, including: Knowledge Modeling and Management for

Cyberization, Information Sharing and Dissemination in Smart Computing, Smart Control and Monitoring for Cyberization, Cognitive Physical-Social Networks, Content Analysis and Mining in Cyber-Social Networks, Behavioral Analytics across Smart Networks, Deep Learning in Cyberization, Resource Management in heterogeneous Networks, Intelligent Transportation Systems Using Smart Networks, Smart Internet of Things, Cyber-Physical-Social Data Processing and Intelligence Mining, Smart Data Streaming and Real-Time Processing, Smart Sensors and Ad-Hoc Wireless Networks, Data Storage and Integration in Cyberspace, Semantic Web Mining in Smart Computing, Infrastructure and Platform for Intelligent Network Systems, Wearable Technologies in Smart Environments, Mobile Computing with Smart Sensors, Smart Energy Management and Sustainability, Privacy and Security in Smart Computing, and etc.

The accepted papers have attracted researchers (corresponding authors) across transdisciplinary research fields from 11 different countries, including Australia, Brazil, China, Finland, France, Japan, Saudi Arabia, Singapore, UK, US, and Tunisia. Consequently, this special issue may have a great significance and impact on: i) studying cyber and cyber-conjugated things for the cyber-enabled new worlds; ii) organizing the body of knowledge in cyber-related researches and applications with comprehensive frameworks in inter-, trans- and multi-discipline fields; iii) enhancing cyber technologies not only in fundamental research works, but also in application system development.

Acknowledgments The guest editors would like to thank all the authors and the reviewers for their hard work and for making possible this Special Issue. They would also like to express their heartfelt gratitude to the Editors-in-Chief, for giving us this opportunity, and the members of the Editorial Staff for their support during the process.

References

1. Hu, R., Yan, Z., Ding, W., Yang, L.T.: A survey on data provenance in IoT. World Wide Web. 1–23 (2019). https://doi.org/10.1007/s11280-019-00746-1
2. Al-Rakhami, M., Gumaei, A., Alsahli, M., et al.: A lightweight and cost-effective edge intelligence architecture based on containerization technology. World Wide Web. 1–20 (2019). https://doi.org/10.1007/s11280-019-00692-y
3. Qi, L., Chen, Y., Yuan, Y., et al.: A QoS-aware virtual machine scheduling method for energy conservation in cloud-based cyber-physical systems. World Wide Web. (2019). https://doi.org/10.1007/s11280-019-00684-y
4. Derhamy, H., Eliasson, J., Delsing, J.: IoT interoperability—on-demand and low latency transparent multiprotocol translator. IEEE Internet Things J. **4**(5), 1754–1763 (2017)
5. Shi, W., Cao, J., Zhang, Q., Li, Y., Xu, L.: Edge computing: vision and challenges. IEEE Internet Things J. **3**(5), 637–646 (2016)
6. M. Al-Rakhami, M. Alsahli, M. M. Hassan, A. Alamri, A. Guerrieri and G. Fortino, "Cost Efficient Edge Intelligence Framework Using Docker Containers," 2018 IEEE 16th Intl Conf on dependable, autonomic and secure computing, 16th Intl Conf on pervasive intelligence and computing, 4th Intl Conf on big data intelligence and computing and cyber science and technology congress, Athens, 2018, pp. 800–807. doi: https://doi.org/10.1109/DASC/PiCom/DataCom/CyberSciTec.2018.00138
7. Alves, M.P., Delicato, F.C., Santos, I.L., Pires, P.F.: LW-CoEdge: a lightweight virtualization model and collaboration process for edge computing. World Wide Web. 1–49 (2019). https://doi.org/10.1007/s11280-019-00722-9
8. Chun Zhao, Lei Ren, Ziqiao Zhang, and Zihao Meng, “Master Data Management for Manufacturing Big Data: A Method of Evaluation for Data Network,” World Wide Web (2019)

9. Lee, E. A. Cyber physical systems: design challenges. Proceedings of the 11th IEEE Symposium on Object/Component/Service-Oriented Real-Time Distributed Computing (ISORC '08)May 20083633692-s2.0–49649119406https://doi.org/10.1109/ISORC.2008.25
10. Raza, U., Camerra, A., Murphy, A.L., Palpanas, T., Picco, G.P.: Practical data prediction for real-world wireless sensor networks. IEEE Transactions on Knowledge and Data Engineering. **27**(8), 2231–2244 (2015)
11. Tan, L., Wu, M.: Data reduction in wireless sensor networks: A hierarchical lms prediction approach. IEEE Sensors Journal. **16**(6), 1708–1715 (2016)
12. Wu, M., Tan, L., Xiong, N.: Data prediction, compression, and recovery in clustered wireless sensor networks for environmental monitoring applications. Information Sciences. **329**(Supplement C), 800–818 (2016)
13. Gaby Bou Tayeh, Abdallah Makhoul, Jacques Demerjian, Christophe Guyeux, Jacques Bahi. Fault Tolerant Data Transmission Reduction Technique in Wireless Sensor Networks. World Wide Web (2019)
14. Tayeh, G.B., Makhoul, A., Demerjian, J., Laiymani, D.: A new autonomous data transmission reduction method for wireless sensors networks. In: 2018 IEEE Middle East and North Africa Communications Conference (MENACOMM), pp. 1{6 (2018)
15. Li, J., McCann, J., Pollard, N., Faloutsos, C.: Dynammo: Mining and summarization of coevolving sequences with missing values. ACM SIGKDD, June/July 2009, pp 527{ 534 (CMU-RI-TR-) (2009)
16. Sabri Allani, Taoufik Yeferny, Richard Chbeir, Sadok Ben Yahia. Towards a Smarter Directional Data Aggregation in VANETs. World Wide Web (2019)
17. Reekie, L., Chow, Y.T., Dakin, J.P.: Optical in-fibre grating high pressure sensor. Electron. Lett. **29**(4), 398–399 (1993)
18. H. T. Nguyen, “State-of-the-art in mac protocols for underwater acoustics sensor networks,” in Emerging Directions in Embedded and Ubiquitous Computing, EUC 2007 Workshops: TRUST, WSOC, NCUS, UUWSN, USN, ESO, and SECUBIQ, Taipei, Taiwan, December 17–20, 2007, Proceedings, 2007, pp. 482–493
19. P. K. Dutta, A. K. Arora, and S. B. Bibyk, “Towards radar-enabled sensor networks,” in International Conference on Information Processing in Sensor Networks, 2006, pp. 467–474
20. X. Gong, J. Zhang, and D. Cochran, “When target motion matters: Doppler coverage in radar sensor networks,” in IEEE INFOCOM, 2013, pp. 1169–1177
21. Xianghua Xu, Chengwei Zhao, Zichen Jiang, Zongmao Cheng, and Jinjun Chen, “Optimal Placement of Barrier Coverage in Heterogeneous Bistatic Radar Sensor Networks,” World Wide Web (2019)
22. Tong Wang, Yunfeng Wang, Xibo Wang, and Yue Cao, “A Detailed Review of D2D Cache in Helper Selection,” World Wide Web (2019)
23. Yayuan Tang, Kehua Guo, Ruifang Zhang, Tao Xu, Jianhua Ma, and Tao Chi, “ICFR: An Effective Incremental Collaborative Filtering based Recommendation Architecture for Personalized Websites,” World Wide Web (2019)
24. Bin Guo, Huihui Chen, Yan Liu, Chao Chen, Qi Han, and Zhiwen Yu, “From Crowdsourcing to Crowdmining: Using Implicit Human Intelligence for Better Understanding of Crowdsourced Data,” World Wide Web (2019)
25. Xiangjie Kong, Feng Xia, Zhenhuan Fu, Xiaoran Yan, Amr Tolba, and Zafer Almakhadmeh, “TBI2Flow: Travel Behavioral Inertia Based Long-Term Taxi Passenger Flow Prediction,” World Wide Web (2019)
26. Weimin Li, Yuting Fan, Jun Mo, Wei Liu, Can, Wang, Minjun Xin, and Qun Jin, “Three-hop Velocity Attenuation Propagation Model for Influence Maximization in Social Networks”
27. Weifeng Wang, Bing Lou, Xiong Li, Xizhong Lou, Ning Jin, and Ke Yan, “Intelligent Maintenance Frameworks of Large-scale Grid using Genetic Algorithm and K-Mediods Clustering Methods,” World Wide Web (2019)
28. Sidra Aleem, Po Yang, Saleha Masood, Ping Li, and Bin Sheng, “An Accurate Multi-Modal Biometric Identification System for Person Identification via Fusion of Face and Finger Print,” World Wide Web (2019)
29. Ao Guo, Jianhua Ma, Shunxiang Tan, and Guanqun Sun, “From Affect, Behavior, and Cognition to Personality: An Integrated Personal Character Model for Individual-like Intelligent Artifacts,” World Wide Web (2019)
30. Nguyen-Vu, L., Ahn, J., Jung, S.: Android fragmentation in malware detection. Computers & Security. **87**, 101573 (2019)
31. Cui, H., Zhou, Y., Wang, C., Li, Q., Ren, K.: Towards privacy-preserving malware detection systems for android. In: 2018 IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS), pp. 545{552. IEEE (2018)
32. Darabian, H., Dehghantanha, A., Hashemi, S., Homayoun, S., Choo, K.K.R.: An opcode-based technique for polymorphic internet of things malware detection. Concurrency and Computation: Practice and Experience p.e5173 (2019)

33. Jing Zhao, Xijiong Xie, Xin Xu, Shiliang Sun, Multi-view learning overview: recent progress and new challenges, Information Fusion, Volume 38, 2017, Pages 43–54, ISSN 1566-2535, https://doi.org/10.1016/j.inffus.2017.02.007
34. Hamid Darabian, Ali Dehghantanha, Sattar Hashemi, Mohammad Taheri, Amin Azmoodeh, Sajad Homayoun, Kim-Kwang Raymond Choo, Reza Parizi, a Multiview Learning Method for Malware Threat Hunting: Windows, IoT and Android as Case Studies. World Wide Web (2019)
35. Prayudi, Y., Riadi, I., et al.: Implementation of malware analysis using static and dynamic analysis method. International Journal of Computer Applications 117(6) (2015)
36. Santos, I., Devesa, J., Brezo, F., Nieves, J., Bringas, P.G.: Opem: A static-dynamic approach for machine-learning- based malware detection. In: International Joint Conference CISIS'12-ICEUTE 12-SOCO 12 Special Sessions, pp. 271{280. Springer (2013)
37. S. Bauer and D. Schreckling, "Data provenance in the internet of things," in Proceedings of 32nd International Conference on Advanced Information Networking and Applications Workshops, 2018, pp.727–731
38. Youliang Tian, Qiuxian Li, Jia Hu, and Hui Lin, "Secure Limitation Analysis of Public-key Cryptography for Smart Card Settings," World Wide Web (2019)
39. Shijo, P., Salim, A.: Integrated static and dynamic analysis for malware detection. Procedia Computer Science. **46**, 804–811 (2015)

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.