Holistic Technologies for Managing Internet of Things Services

Ranjan, Rajiv; Hsu, Ching-Hsien; Chen, Lydia Y.; Georgakopoulos, Dimitrios

DOI
10.1109/TSC.2020.3000844

Publication date
2020

Document Version
Final published version

Published in
IEEE Transactions on Services Computing

Citation (APA)
Ranjan, R., Hsu, C.-H., Chen, L. Y., & Georgakopoulos, D. (2020). Holistic Technologies for Managing Internet of Things Services. *IEEE Transactions on Services Computing*, *13*(4), 597-601. Article 9159958. https://doi.org/10.1109/TSC.2020.3000844

Holistic Technologies for Managing Internet of Things Services

Rajiv Ranjan, *Senior Member, IEEE*, Ching-Hsien Hsu, *Senior Member, IEEE*, Lydia Y. Chen, *Senior Member, IEEE*, and Dimitrios Georgakopoulos

Abstract—The Internet of Things (IoT) is the latest Internet evolution that incorporates billions of sensors, actuators, and related software services that collectively distill high value information, perform actions that affect the physical world, and support a variety of applications controlled by different organizations and individuals. IoT's ability to observe and affect the physical world presents a unprecedented opportunity for creating IoT-based smart services and products that address grant challenges in emerging opportunities in areas such as climate change, precision agriculture, smart health, advanced manufacturing, and smart cities. This special issue identifies and addresses some of the key issues that hinder the development of IoT-based solutions. It includes articles that present the latest innovations in IoT security and privacy, IoT data quality and analysis, IoT resources and task management, as well as examples of IoT-based application services and domains.

Index Terms—Internet of Things, IoT security and privacy, IoT data processing

1 Background

The Internet of Things (IoT) is the latest Internet evolution that incorporates billions of sensors and other machines (we refer to these as IoT devices or Things) that support the development of novel IoT-based services and related smart products [1], [2]. IoT devices (e.g., wearables, smart-phones, sensors, industrial machines, radio-frequency identification smart vehicles, etc.) sense the physical world and send observation data (we refer to as IoT data) to IoT-based software services that run in the cloud, edge computers, and/or the IoT devices themselves. These computing resources are interconnected via a variety of networks ranging from broadband to low-power narrowband and low power wide-area networks. The unprecedented ability of IoT ecosystem to observe the physical world and provide valuable information allows IoT-based services to address a magnitude of grand challenges in our society that were unsolvable before due to lack of critical information from the physical world.

Nevertheless, the full potential of IoT ecosystem is still far from being realized because of the lack of comprehensive solutions that ensure the security and quality of IoT data, guarantee the privacy of those being observed by the IoT devices and the users of IoT-based services, and provide for efficient resource management and task scheduling techniques that are appropriate for IoT data analysis providing for information classification, optimization, and personalization.

This special issue consists of thirteen high quality research papers in these critical areas that will enable devising applications that are secure and trustworthy, scalable and provide the high quality and high value information that is needed to address major challenges in our society. More specifically, in Section 2, we provide an overview of the articles that are included in this special issue. In Section 3, we discuss further research challenges, while Section 4 present a conclusion.

2 Articles in This Special Issue

This special issue is dedicated to reporting novel techniques and/or models for IoT security and privacy, IoT data quality and analysis, as well as IoT computing resource and task management. For this special issue, we received 71 submissions and 14 of these were accepted for publication (i.e., ~19.7% acceptance rate). Each article went through a rigorous peer review process, in addition to multiple follow-up rounds with the authors. We summarize the articles below, before identifying further, less understood research challenges. We categorize accepted papers in this special issue into four broad categories that are discussed in two the following sections.

2.1 IoT Security and Privacy

IoT security and privacy includes unique challenges due to the limited computing power of IoT devices, and the diversity of IoT devices and their related providers. Existing research in lightweight security for IoT (e.g., in [5], [6], [7])

- *R. Ranjan is with the School of Computing at Newcastle University, NE17RU Newcastle upon Tyne, United Kingdom. E-mail: rranjans@gmail.com.*
- *C.-H. Hsu is with the College of Information and Electrical Engineering, Asia University, Taichung 41354, Taiwan; and also with the Department of Computer Science and Information Engineering, National Chung Cheng University, Chiayi County 41354, Taiwan. E-mail: robertchh@gmail.com.*
- *L. Y. Chen is with the Department of Computer Science at the Delft University of Technology, 2628 CD, Delft, The Netherlands. E-mail: y.chen-10@tudelft.nl.*
- *D. Georgakopoulos is with the Computer Science in Swinburne University of Technology, Hawthorn 3122, VIC, Australia. E-mail: dgeorgakopoulos@swin.edu.au.*

(Corresponding author: Rajiv Ranjan.)

Digital Object Identifier no. 10.1109/TSC.2020.3000844

have provided some solutions for these challenges. This special issue includes complementary innovations in hardware security, blockchain-based security, and privacy preserving service composition.

Hardware security: In the article entitled "ThinORAM: Towards Practical Oblivious Data Access in Fog Computing Environment", Huang *et al.* propose a ThinORAM for providing oblivious IoT data access in a fog computing environment with a minimum client cost. This novel hardware solution combines a secure application of expensive Oblivious RAM with a novel thin client that removes complicated computations in the client side. This combination requires only O(1) communication cost and provides a reasonable response time.

Blockchain-based IoT security: In the article entitled "GUARDIAN: Blockchain-Based Secure Demand Response Management in Smart Grid System", Jindal *et al.* propose a blockchain-based secure demand response management scheme for supporting energy trading decisions and securely managing the overall load of residential, commercial, and industrial sectors. This scheme is lightweight in terms of communication and computation costs.

Blockchain-based Software-defined Networking (SDN)-IoT Security: In this article entitled "An Energy-efficient SDN Controller Architecture for IoT Networks with Blockchain-based Security", Yazdinejad *et al*. proposed a blockchain architecture for secure and energy-efficient management of SDN controllers for cluster structure-based IoT networks. To make blockchain suitable for IoT, a peer-to-peer mechanism along with authentication based on distributed trust has been employed in the proposed architecture.

IoT privacy: In the article entitled "Privacy in Data Service Composition, Barhamgi *et al.* propose a flexible privacy-preserving data integration solution for answering data integration queries that do not require a trusted mediator in situations where information about a specific individual is collected and managed by autonomous data collection services that may have different privacy policies. The paper proposes a novel untrusted mediator that links subjects across the different services.

Cyber-Physical System Security: In this article entitled "Buoy Sensor Cyberattack Detection in Offshore Petroleum Cyber-Physical Systems", Mu *et al*. deployed a stochastic processd known as Partially observable Markov decision process to design a Buoy Sensor Cyberattack detection (PBSC) technique. This technique evaluates the probability of the occurrence of the cyber attacks on the buoy sensors. The experimental results depict a 50% improvement in detection accuracy along with x6 faster running speed.

2.2 IoT Data Quality and Analysis

Recent advances in machine learning have fueled innovations that improve the quality and analysis of IoT data (e.g., in [9], [8]). This special issue includes further research outcomes in the following aspects of data quality and analysis:

Gap recovery in incomplete IoT datasets: In the article entitled "ARDIAN: Blockchain-Based Secure Demand Response Management in Smart Grid System", Lujic *et al*. propose a framework featuring a generic mechanism for recovery of multiple gaps in incomplete datasets, using both single-technique recovery (STR) and multiple-technique recovery (MTR) involving projection recovery maps (PRMs). Experimental evaluations using time series from smart buildings show that the proposed framework reduces errors due to data quality issues by up to 65.48% and the data storage needed by an average of 39.9%, while keeping accuracy to 98.8%.

Personalization, recommendation, and optimization in IoT: In the article entitled "MMDP: A Mobile-IoT Based Multimodal Reinforcement Learning Service Framework", Wang *et al.* propose a multi-modal reinforcement learning service framework that provides personalized services in Mobile IoT applications. Novel contributions include an Action-aware High-order Transition Tensor (AHTT) to fuse the heterogeneous data from Mobile IoT in a unified form, a Multi-modal Markov Decision Process (MMDP) to model the multi-modal reinforcement learning as a mobile IoT service framework, and a Tensor Policy Iteration algorithm (TPIA) to solve the optimal tensor policy problem. Experiment results from taxi driver dataset shows that a taxi driver who uses the proposed model earns more revenue.

In another article entitled "Personalized Recommendation System based on Collaborative Filtering for IoT Scenarios", Cui *et al.* introduce a novel recommendation model called Time Correlation Coefficient (TCC) and CSK-means that is based on a combination of a time correlation coefficient with an improved K-means with cuckoo search (CSK-means). The paper also proposes a personalized recommendation model that improves TCCF further by analysing specific user behaviours. Experimental evaluation conducted using the MovieLens and Douban datasets show that the proposed personalised recommendation provides a 5.2% improvement when compared with other existing models.

This special issue also includes an article titled "Improving Brain E-Health Services via High-Performance EEG Classification With Grouping Bayesian Optimization", where Ke *et al.* present an automatic machine learning method that includes a dual CNN (convolutional neural network) for classification of brain health conditions. Unlike other existing models that largely remain static, the proposed CNN-based model can continuously optimize its hyperparameters. Experimental results in the evaluation of depression using real EEG datasets indicate that the proposed dual CNN model performs 3.5 times faster compared other existing models, and it is more accurate, than conventional techniques, in identifying Major Depression Disorder.

2.3 IoT Task and Resources Management

Existing research related to cloud and edge computing has extensively covered the problems of resource and task management (e.g., [10]). However, resource and task management in IoT is far more challenging due to the volatility of IoT devices, the potential use of the limited computing resources that IoT devices provide, and changing volume and velocity of "live" IoT data streams. This special issue provides novel research contributions in the following topics:

Resource monitoring for IoT-based services: In the article entitled "An Efficient Resource Monitoring Service for Fog Computing Environments", Battula *et al.* propose a technique for optimizing the resource usage in monitoring cloud computing resources in IoT applications. The performance of this novel technique was evaluated by using an IoT emulator that generated synthetic real-time traffic data. In this experiment, the proposed technique achieve a 19% reduction in use of computing resources, with aid of online monitoring, when it was compared to other existing techniques that lack real-time monitoring capability.

Resource allocation for IoT-based services: In the article entitled "A Cyclic Game for Service-Oriented Resource Allocation in Edge Computing", Ma *et al.* tackle the edge computing problem where service resource and edge nodes providers autonomously adjust the resource allocations they provide. This paper propose a three-sided cyclic game involving users, edge nodes, and service providers who make their individual decisions by choosing respectively high-quality services, high-value users, and cost-effective edge nodes for service deployment. The authors prove the existence and approximation ratio of pure-strategy Nash equilibriums (NEs). Experimental results validate the effectiveness and convergence of the proposed game.

Virtual Machine migration for IoT-based services: In the article entitled "Towards Service Composition Aware Virtual Machine Migration Approach in the Cloud", Zhou *et al.* propose a novel service composition-aware virtual machine migration approach that reduces the data center network resource consumption. Experimental evaluation results in a large-scale cloud data center demonstrate that this solution significantly reduces the network resource consumption compared to other existing approaches.

Scheduling of IoT task processing/analysis tasks: In this special issue article with the title "Security-Critical Energy-Aware Task Scheduling for Heterogeneous Real-Time MPSoCs in IoT", Zhou *et al.* tackle the problem of scheduling IoT data processing tasks with precedence dependences in a heterogeneous multiprocessor systems on a chip (MPSoC). This article proposes a mixed-integer linear programming (MILP)-based solution for allocating and scheduling tasks and introduced a two-stage technique for determining the allocation, processing frequency and security of the task at hand. Simulation is used to demonstrate that the proposed two-stage technique outperforms existing approaches in saving energy and improving security.

2.4 Application-Specific IoT-Based Services

This special issue also includes an article that describes an IoT-based service that has been designed for a specific industrial application. More specifically, in the paper entitled "IoT-enabled service for crude-oil production systems against unpredictable disturbance", Duan *et al.* propose an IoT-enabled disruption management service for crude-oil refineries. This service provides refinery monitoring and alarm generation, as well as makes changes in the refinery configuration to deal with unforeseen disruptions. Experimental evaluation results show that this solution achieves better efficiency and stability compared to other existing solutions.

3 Further Research Challenges

This special issue includes significant research contributions to several well-understood IoT challenges that range from IoT security and privacy, to IoT data quality and analysis, and resource and task management for processing IoT data. Further critical but currently less-understood IoT research challenges stem from the need to:

- improve the efficiency of existing IoT device (re)use,
- provide better support for time sensitive IoT applications, and
- expand the core machine-centric scope of IoT to better support critical industrial applications and the industry 4.0 vision.

For example, demand-based discovery and integration of existing IoT devices from any provider can reduce both the time needed to create IoT applications and their operating cost (via a pay-as-you-go model) of IoT devices. Dynamic resource and task management and scheduling (not only in the cloud and edge but also in the IoT devices themselves) can help to better meet the application-specific time bounds of time-sensitive IoT applications. Extending the scope of IoT to include complex machines (e.g., industrial machines, vehicles, etc.) instead of only dealing with simple sensors that produce data we can understand directly. Extending the scope will help solve many difficult problems in our industry and society. These currently less well understood research challenges are discussed further in the following paragraphs.

Dynamic IoT device discovery and integration: The full potential of IoT is still far from being realized because sharing and reusing existing IoT devices is currently severely hindered by lack of a comprehensive solution that permits the discovery and integration of existing IoT devices. Due to the lack of any comprehensive solution for sharing and (re)using existing IoT devices, the IoT device deployment and maintenance cost/effort is often too high compared to the benefits such IoT devices provide to their owners [2]. Therefore, to achieve a reasonable benefit/cost ratio there is a need for an IoT service that facilitates effective sharing and (re)use of existing IoT devices that are owned by different providers. Such an IoT device discovery and integration service [2] must be: (1) scalable to serve a vast number of IoT devices, (2) global, i.e., capable of dealing with any variety of IoT devices and heterogeneity of IoT data, (3) autonomous IoT devices, i.e., not owned by specific individuals (following the principles of the internet), and (4) revenue generating for IoT device providers to provide for cost sharing and promote the deployment of more IoT devices.

Dynamic resource and task management and scheduling for time-sensitive IoT applications: Many IoT data applications have time-bound requirements, i.e., require their IoT data analysis to be completed within a specific time. If the time-bound requirements are not met, the information produced by the application will no longer be useful. For example, a vehicle accident prediction IoT application must analyze IoT data collected from traffic cameras, onboard cameras in the car and sensors, to predict possible accidents and prevent the accidents by informing the corresponding driver in near real-time (e.g., within a fixed time frame, say 30 ms). The ability to meet the time-bound requirements of a Time-Sensitive IoT (TS-IoT) application is largely determined by end-to-end response time of the application executed in the IoT environment. End-to-end response time for a TS-IoT application is measured as the sum of total execution time and total IoT data communication delay of the application. Total execution time is influenced by the selection of IoT resource nodes where the IoT data analysis is performed while total data communication delay is influenced by the relevant network delays involved in transferring the IoT data to corresponding IoT resource nodes. Therefore, meeting time-bound requirements of TS-IoT applications heavily depends on the selection of appropriate IoT resource nodes from the perspective of communication delays and needed computing resources. However, meeting the time-bound requirements of TS-IoT applications is not a trivial task, especially due to the volatility and mobility of IoT. As a result of this, it has become a major research challenge to devise techniques (i.e., techniques that are used to manage resource selection, distribution, scheduling of TS-IoT applications in IoT environment etc.) and approaches (i.e., application modelling, simulation and system implementations for TS-IoT applications) that can be used to address the challenges of meeting time-bound requirements of such TS-IoT applications.

Industrial IoT and Digital Twins: Most existing IoT research assume that IoT devices are simple sensors and produce data that IoT applications and users can directly understand. The reality is totally different. In the real world, even IoT data produced by simple IoT sensors usually need to be translated to information that are useful in the context of an IoT application. For example, using solar radiation sensors to determine if a crop needs to be irrigated, requires building and using a machine learning model that translates solar radiation observation data to plant irrigation needs, and to do this for the various environmental conditions during the lifetime of each plant variety, crop, soil, and geographical area being observed. Furthermore, many IoT machines (e.g., industrial machines, vehicles, etc.) are far more complex than simple sensors as they incorporate many sensors, and actuators, and have control loop). An IoT application that utilizing such complex machines must understand/translate their data, interact with the machines to cause the actions it needs to be performed by each machine, and do these within the constraints of the control loop of each machine. New paradigms such as digital twins for complex machines need to be developed and used in building such applications. Solutions to this and above challenges will give rise to the so called Industrial IoT (IIoT) and a more capable and useful IoT.

4 Concluding Remarks

In this special issue, we outlined novel holistic technologies for managing Internet of Things services for security and privacy, data quality and analysis, as well as resource and task management. We also outlined further research challenges for creating more powerful IoT applications that provide better services to our society. The combination of these services provide more useful tools and a path forward to a more powerful IoT.

Acknowledgments

This article was supported by Sustainable Urban Power Supply through intelligent control and enhanced restoration of AC/DC networks, EPSRC-NSFC Call in Sustainable Power Suppl, 2019-2022. (EP/T021985/1), Smotic MindSphere: Multi-Resolution Air Quality Modelling across Cloud and Edge, Pitch-In: Connecting capabilities for the Internet of Things, Research England, 2019-2021. (P35792/BH192113), and Privacy-Aware Cloud Ecosystems, Engineering and Physical Sciences Research Council, 2018-2021. (EP/R033293/1).

References

[1] D. Georgakopoulos and P. P. Jayaraman, "Internet of Things: From internet scale sensing to smart services," *Computing*, vol. 98, no. 10, pp. 1041–1058, 2016.

[2] A. Dawod, D. Georgakopoulos, P. P. Jayaraman, and A. Nirmalathas, "Advancements towards global IoT device discovery and integration," in *Proc. IEEE Int. Congr. Internet Things*, 2019, pp. 147–155.

[3] M. Compton *et al.*, "The SSN ontology of the W3C semantic sensor network incubator group," *Web Semantics: Sci. Serv. Agents World Wide Web*, vol. 17, pp. 25–32, 2012.

[4] A. Haller *et al.*, "The modular SSN ontology: A joint W3C and OGC standard specifying the semantics of sensors, observations, sampling, and actuation," *Semantic Web*, vol. 10, pp. 1–24, 2019.

[5] P. P. Jayaraman, X. Yang, A. Yavari, D. Georgakopoulos, and X. Yi, "Privacy preserving Internet of Things: From privacy techniques to a blueprint architecture and efficient implementation," *Future Gener. Comput. Syst.*, vol. 76, pp. 540–549, Nov. 2017. doi: 10.1016/j.future.2017.03.001.

[6] A. S. Panah, A. Yavari, R. Y. Schyndel, D. Georgakopoulos, and X. Yi, "Context-driven granular disclosure control for Internet of Things applications," *IEEE Trans. Big Data*, vol. 5, no. 3, pp. 12–26, Sep. 2019.

[7] A. Yavari, A. S. Panah, D. Georgakopoulos, P. P. Jayaraman, and R. Y. Schyndel, "Scalable role-based data disclosure control for the Internet of Things," in *Proc. IEEE 37th Int. Conf. Distrib. Comput. Syst.*, 2017, pp. 2226–2233.

[8] A. R. M. Forkan *et al.*, "An industrial IoT solution for evaluating workers' performance via activity recognition," in *Proc. IEEE 39th Int. Conf. Distrib. Comput. Syst.*, 2019, pp. 1393–1403.

[9] F. Montori, P. P. Jayaraman, A. Yavari, A. Hassani, and D. Georgakopoulos, "The curse of sensing: Survey of techniques and challenges to cope with sparse and dense data in mobile crowd sensing for Internet of Things," *Pervasive Mobile Comput.*, vol. 49, pp. 111–125, Sep. 2018. doi:10.1016/j.pmcj.2018.06.009.

[10] R. K. Naha *et al.*, "Fog computing: Survey of trends, architectures, requirements, and research directions," *IEEE Access*, vol. 6, pp. 47980–48009, Aug. 2018.

[11] R. Ranjan *et al.*, "The next grand challenges: Integrating the Internet of Things and data science," *IEEE Cloud Comput.*, vol. 5, no. 3, pp. 12–26, May/Jun. 2018.

Rajiv Ranjan (Senior Member, IEEE) is currently a chair and professor of computing science and Internet of Things with Newcastle University (from August 2018), United Kingdom. He is an internationally established scientist with more than 300 scientific publications and expertise in cloud computing, big data, and the Internet of Things. He has secured more than $24 Million AUD in the form of competitive research grants from both public and private agencies. He is an innovator with strong and sustained academic and industrial impact and a globally recognized R&D leader with the proven track record. His work has been extensively cited (17K+, Google Scholar; 9K+ Scopus; 6K+ Web of Science). He serves on the editorial boards of top-quality international journals including the *IEEE Transactions on Computers*, *IEEE Transactions on Cloud Computing*, *IEEE Cloud Computing*, and *Future Generation Computer Systems*.

Ching-Hsien Hsu (Senior Member, IEEE) is currently a chair professor and dean of the College of Information and Electrical Engineering, Asia University, Taiwan; and professor with the Department of Computer Science and Information Engineering, National Chung Cheng University. His research includes high performance computing, cloud computing, parallel and distributed systems, big data analytics, ubiquitous/pervasive computing and intelligence. He has published 200 referred papers. He was awarded six times talent awards from Ministry of Science and Technology, Ministry of Education, and nine times Distinguished Award for his excellence in research from Chung Hua University, Taiwan. He is a fellow of the IET (IEE); chair of the IEEE Technical Committee on Cloud Computing (TCCLD).

Lydia Y. Chen received the BA degree from National Taiwan University, and the PhD degree from Pennsylvania State University. She is currently an associate professor with the Department of Computer Science at the Delft University of Technology, The Netherlands. Prior to joining TU Delft, she was a research staff member at the IBM Research Zurich Lab from 2007 to 2018. Her research interests include distributed machine learning, dependability management, resource allocation for large-scale data processing systems and services. More specifically, her work focuses on developing stochastic and machine learning models, and applying these techniques to application domains, such as data centers and AI systems.

Dimitrios Georgakopoulos is currently a professor of computer science with the Swinburne University of Technology, and the inaugural director the IoT Lab with the University's Digital Innovation Capability Platform. He also leads the university's Industry 4.0 program which is a key part of Swinburne's Manufacturing Futures Research Institute. Before that, he served as research director of CSIRO's ICT Centre and a professor at RMIT University. Prior to joining CSIRO, he held research and management positions in several industrial laboratories in the USA, including Telcordia, Microelectronics and Computer Corporation (MCC), GTE Laboratories (currently Verizon), and Bell Communications Research (Bellcore). He is a research leader in IoT and Industry 4.0, where he is devising large-scale, high-performance IoT Systems, semantic data models and machine learning-based analysis techniques for massive data sets produced by sensors and other complex machines, industrial processes, humans, and products. He has received numerous research and related impact awards in Australia, USA and EU; cited 16.5K+ times; and chaired 20+ major conferences. His research has attracted significant research funding ($42M+) from industry and various government research funding agencies in Australia, EU and USA.