Guest Editorial Special Issue on Trust-Oriented Designs of Internet of Things for Smart Cities

THE Internet of Things (IoT) offers new opportunities for cities to make citizens live and work in more sustainable, healthy, and safe places. Since IoT applications in smart cities are characterized by different devices, networking standards, and data management strategies, trust becomes a fundamental issue in the IoT ecosystem. The explosion of IoT devices, along with their decentralized deployment, constraint resources, limited computational and cryptographic capabilities, brings challenges to trust management in IoT. The coexistence of multiple IoT domains also raises challenges, for example, how to evaluate and maintain trust across domain boundaries. This special issue aims at bringing the researchers from both academia and industry together to disseminate their recent advances related to the challenges and solutions in building trustful IoT for smart cities.

The response to our above theme was overwhelming, with 68 articles submitted in the open Calls for Papers around the world. During the review process, each article was assigned to and reviewed by multiple experts in the relevant areas, with a rigorous two-round review process. Thanks to the great support of the Editor-in-Chief of this journal, we were able to accept 21 excellent articles covering various aspects of trust-oriented designs of IoT for smart cities. In the following, let us introduce these articles and highlight their main contributions.

The article titled "Vcash: A novel reputation framework for identifying denial of traffic service in Internet of Connected Vehicles" proposed Vcash, a reputation framework for identifying the denial of traffic service, to resolve the trustworthiness problem in the application level of the Internet of Connected Vehicles.

The article titled "A decentralized and trusted edge computing platform for Internet of Things" proposed a new edge computing platform, decentralized and trusted platform for edge computing (DeTEC), which provides a unified interface to the users, resolves the user's requests to the most appropriate edge server through DNS, and returns the computational results to the IoT user.

The article titled "Stochastic cost minimization mechanism based on identifier network for IoT security" presented an optimization framework of defense cost for the IoT security and formulate it as a stochastic cost optimization problem by considering the impacts of network address shuffling control, network autoimmunity control, and defense cost.

In the article "LiPSG: Lightweight privacy-preserving Q-learning-based energy management for the IoT-enabled smart grid," the authors proposed a lightweight privacy-preserving Q-learning framework (LiPSG) for the energy management strategy making of the smart grid.

The article titled "Energy-efficient and privacy-preserving data aggregation algorithm for wireless sensor networks" proposed an energy-efficient and privacy-preserving data aggregation algorithm (EPDA). They organized a sensor network into a tree and connect the leaf nodes of the tree to form many chains.

In the article "STIR: A smart and trustworthy IoT system interconnecting legacy IR devices," the authors presented a trustworthy and cost-effective smart IR system that is able to change an IR controllable device into a smart IoT device and interconnect them for smart city/home applications.

The article titled "Reliable fog-based crowdsourcing: A temporal–spatial task allocation approach" proposed the reliable fog-based temporal–spatial crowdsourcing for serving the above tasks. The authors presented a temporal–spatial task allocation scheme (TS-TA) in the fog layer, aiming to make task results more reliable.

In "Lightweight tag-based PHY-layer authentication for IoT devices in smart cities," the authors provided a general and lightweight PHY-layer authentication framework for the IoT devices in smart cities, based on tag embedding and tag verification.

The article titled "An IoT honeynet based on multiport honeypots for capturing IoT attacks" implemented three kinds of honeypots to capture malicious behaviors. On the basis of the CVE-2017-17215 vulnerability, the authors implemented a medium–high interaction honeypot that can simulate a specific series of router UPnP services.

In "Blockchain-enabled decentralized trust management and secure usage control of IoT big data," the authors proposed a permissioned-blockchain-based decentralized trust management and secure usage control scheme of the IoT big data (called BlockBDM), upon which all the data operations and management, such as data gathering, invoking, transfer, storage, and usage are processed over the blockchain smart contract.

In the article "LVPDA: A lightweight and verifiable privacy-preserving data aggregation scheme for edge-enabled IoT," the authors proposed a lightweight and verifiable privacy-preserving data aggregation scheme for the edge-computing-enabled IoT system, where the Paillier

Digital Object Identifier 10.1109/JIOT.2020.2982522

homomorphic encryption method and an online/offline signature technique are combined to ensure the privacy preserving and integrity verification during the data aggregation process.

The article titled "TCEMD: A trust cascading-based emergency message dissemination model in VANETs" presented a novel trust cascading-based emergency message dissemination (TCEMD) model which incorporates the entity-oriented trust values into data-oriented trust evaluation in an efficient manner.

In "Secure and trust-oriented edge storage for Internet of Things," the authors proposed a secure and trust-oriented edge storage model, which would efficiently tackle the aforementioned two challenging issues in the IoT environment.

In "An index-based provenance compression scheme for identifying malicious nodes in multihop IoT network," the authors proposed an index-based provenance compression algorithm, which adopts the idea of common substring matching, combined with a path identifier and a path index to represent the path information in the data provenance, thereby achieving the purpose of reducing the size of data provenance.

The article titled "A highly parallelized PIM-based accelerator for transaction-based blockchain in IOT environment" presented Re-Tangle, a highly parallelized PIM-based accelerator for the transaction-based blockchain. Re-Tangle is composed of a random walking module, a transaction validation module, and a PoW module, to improve the Tangle system performance.

In "Trust-oriented IoT service placement for smart cities in edge computing," the authors proposed a trust-oriented IoT service placement method, abbreviated as TSP, for smart cities in edge computing. Technically, improving the strength Pareto evolutionary algorithm (SPEA2) is leveraged to acquire the balanced placement strategies for the tradeoffs among the execution performance metrics with privacy preservation.

In "Trustful Internet of Surveillance Things based on deeply represented visual co-saliency detection," the authors enabled the co-saliency detection in IoT, which detects the common and salient foreground regions in the group surveillance images.

In the article "A blockchain-based trust management with conditional privacy-preserving announcement scheme for VANETs," a blockchain-based trust management model, combined with conditional privacy-preserving announcement scheme (BTCPS), was proposed for VANETs.

The article titled "DeePGA: A privacy-preserving data aggregation game in crowdsensing via deep reinforcement learning" proposed a payment-privacy protection-level (PPL) game, where each participant submits his sensing data with a specified PPL while the platform chooses a corresponding payment to the participant.

In "Toward incentivizing fog-based privacy-preserving mobile crowdsensing in the Internet of Vehicles," to reduce the risk of privacy leakage in the implementation of incentive mechanisms, the authors proposed a fog computing-based crowdsensing architecture specialized for vehicular crowdsensing and corresponding privacy-preserving solutions for the processes of data reporting, reward issuing, and trust management.

In the article "Blockchain-based dynamic provable data possession for smart cities," the authors described a blockchain-based PDP model to realize the decentralized outsourcing storage framework and then presented a concrete construction of decentralized provable data possession by using multireplica storage tricks.

To conclude, we would like to appreciate all the authors for their support and excellent contributions. We also would like to thank all the reviewers for their efforts in reviewing the articles, and for their valuable comments and constructive suggestions for improving the quality of the articles. Finally, we appreciate Dr. Sherman Shen and Dr. Honggang Wang for their help in the publication process. We hope that this special issue can help both industry and academic research communities to better understand the recent advancements and potential research opportunities on the topic of "Trust-Oriented Designs of IoT for Smart Cities."

MENG SHEN, *Guest Editor*
Department of Computer Science
and Technology
Beijing Institute of Technology
Beijing 100081, China

KE XU, *Guest Editor*
Department of Computer Science
and Technology
Tsinghua University
Beijing 100081, China

XIAOJIANG DU, *Guest Editor*
Department of Computer and
Information Sciences
Temple University
Philadelphia, PA 19122 USA

MARTIN J. REED, *Guest Editor*
School of Computer Science and
Electronic Engineering
University of Essex
Colchester CO4 3SQ, U.K.

MD ZAKIRUL ALAM BHUIYAN, *Guest Editor*
Department of Computer and
Information Sciences
Fordham University
Bronx, NY 10458 USA

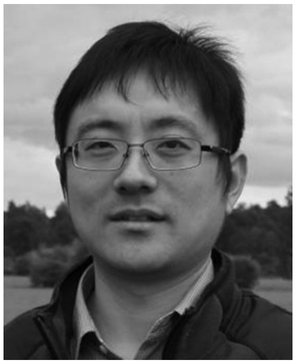
LAN ZHANG, *Guest Editor*
Department of Computer Science
and Technology
University of Science and
Technology of China
Anhui 230026, China

RASHID MIJUMBI, *Guest Editor*
Software and Systems Reliability
Engineering
Nokia Bell Labs
Blanchardstown Dublin 15, Ireland

Meng Shen (Member, IEEE) received the B.S. degree in computer science from Shandong University, Jinan, China, in 2009, and the Ph.D. degree in computer science from Tsinghua University, Beijing, China, in 2014.

He is an Associate Professor with the Beijing Institute of Technology, Beijing. His research interests include data security and privacy protection, blockchain applications, and encrypted traffic analysis. He has authored more than 60 journal and conference papers in the above areas.

Dr. Shen received the Best Paper Runner-Up Award at IEEE IPCCC 2014.



Ke Xu (Senior Member, IEEE) received the Ph.D. degree from the Department of Computer Science and Technology, Tsinghua University, Beijing, China.

He serves as a Full Professor with Tsinghua University. He has published more than 200 technical papers and holds 11 U.S. patents in the research areas of next-generation Internet, blockchain systems, Internet of Things, and network security. He has guest edited several special issues in IEEE and Springer journals.

Prof. Xu is an Editor of the IEEE INTERNET OF THINGS JOURNAL. He is the Steering Committee Chair of IEEE/ACM IWQoS. He is a member of ACM.

Xiaojiang Du (Fellow, IEEE) received the B.S. and M.S. degrees in electrical engineering from Tsinghua University, Beijing, China, in 1996 and 1998, respectively, and the M.S. and Ph.D. degrees in electrical engineering from the University of Maryland at College Park, College Park, MD, USA, in 2002 and 2003, respectively.

He is a Tenured Professor with the Department of Computer and Information Sciences, Temple University, Philadelphia, PA, USA. He has been awarded more than $5 million research grants from the U.S. National Science Foundation, Army Research Office, Air Force, NASA, the State of Pennsylvania, and Amazon. His research interests are wireless communications, wireless networks, security, and systems. He has authored over 400 journal and conference papers in these areas, as well as a book published by Springer.

Dr. Du won the Best Paper Award at IEEE GLOBECOM 2014 and the Best Poster Runner-Up Award at ACM MobiHoc 2014. He serves on the editorial boards of three international journals. He is a Life Member of ACM.

Martin J. Reed (Member, IEEE) received the Ph.D. degree from the University of Essex, Colchester, U.K., in 1998.

He is currently a Senior Lecturer with the University of Essex. His research interests include network control planes, information centric networking, network security, and multimedia networking. He has been involved in a number of EPSRC, EU, and industrial projects in these areas and has held a Research Fellowship at BT.

Md Zakirul Alam Bhuiyan received the B.Sc. degree in computer science and technology from International Islamic University Chittagong, Chittagong, Bangladesh, in 2005, and the M.Eng. and Ph.D. degrees in computer science and technology from Central South University, Changsha, China, in 2009 and 2013, respectively.

He is currently an Assistant Professor with the Department of Computer and Information Sciences, Fordham University, New York, NY, USA, where he is the Founding Director of the Fordham Dependable and Secure System Lab. He was an Assistant Professor with Temple University, Philadelphia, PA, USA. His work (including more than 40 JCR Q1 papers) has been published in top-tier venues. His several research papers have received recognition of ESI highly cited papers. His research interests include dependability, cybersecurity, big data, and Internet-of-Things/cyber–physical system applications.

Lan Zhang received the bachelor's degree from the School of Software, Tsinghua University, Beijing, China, in 2007, and the Ph.D. degree from the Department of Computer Science and Technology, Tsinghua University in 2014.

She is currently a Research Professor with the School of Computer Science and Technology, University of Science and Technology of China, Hefei, China. She has published more than 50 conference and journal papers. She has applied for three U.S. patents and 28 Chinese patents, and 14 of them have been granted. Her research interests span mobile computing, privacy protection, and data sharing and trading.

Dr. Zhang received the 2015 ACM China Doctoral Dissertation Award (1/2 nationally) and the CCF Outstanding Doctoral Dissertation Award (1/10 nationally). She was honored as the Alibaba DAMO Academy Young Fellow in 2018. She will be or has been a TPC Member of IEEE INFCOM 2020 & 2019 & 2018 IWQOS 2020, IEEE MASS 2018, IEEE ICC 2018, and IEEE SECON 2018.

Rashid Mijumbi received the B.Sc. degree in electrical engineering from Makerere University, Kampala, Uganda, in 2009, and the Ph.D. degree in telecommunications engineering from the Universitat Politècnica de Catalunya (UPC), Barcelona, Spain.

He was a Postdoctoral Researcher with UPC and the Telecommunications Software and Systems Group, Waterford, Ireland, where he participated in several Spanish national, European, and Irish national research projects. His current research focus is on all aspects involving future Internet, 5G, NFV, and SDN.

Dr. Mijumbi was a recipient of the 2016 IEEE Transactions Outstanding Reviewer Award recognizing outstanding contributions to the IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT.