Guest Editorial Special Issue on Trust, Security, and Privacy in Crowdsourcing

THE RECENT proliferation of mobile devices such as smartphones and wearable devices has given rise to crowdsourcing Internet of Things (IoT) applications, such as urban mobility monitoring, virtual/augmented reality, smart city management, and indoor floor plan reconstruction and mapping. Various data collected by mobile devices with small or big volumes can be further processed, analyzed, and mined in order to support multifarious promising services with intelligence.

As we become increasingly reliant on intelligent, interconnected devices in every aspect of our lives, critical trust, security, and privacy concerns are raised as well. First, the sensing data provided by individual participants is not always reliable. It may be noisy or even faked due to various reasons, such as poor sensor quality, lack of sensor calibration, background noise, context impact, mobility, incomplete view of observations, or malicious attacks. The crowdsourcing applications should be able to evaluate the trustworthiness of collected data in order to filter out the noisy and fake data that may disturb or intrude a crowdsourcing system. Second, providing data (e.g., photographs taken with personal mobile devices) or using IoT applications may compromise data providers' personal data privacy (e.g., location, trajectory, and activity privacy) and identity privacy. Therefore, it becomes essential to assess the trust of the data while preserving the data providers' privacy. Third, data analytics and mining in crowdsourcing may disclose the privacy of data providers or related entities to unauthorized parities, which lowers the willingness of participants to contribute to the crowdsourcing system, impacts system acceptance, and greatly impedes its further development. Fourth, the identities of data providers could be forged by malicious attackers to intrude the whole crowdsourcing system. In this context, trust, security, and privacy start to attract a special attention in order to achieve high quality of service in each step of crowdsourcing with regard to data collection, transmission, selection, processing, analysis and mining, as well as utilization.

Trust, security, and privacy in crowdsourcing receives increasing attention. Many methods have been proposed to protect privacy in the process of data collection and processing. For example, data perturbation can be adopted to hide the real data values during data collection. When preprocessing the collected data, data anonymization (e.g., k-anonymization) and fusion can be applied to break the links between the data and their sources/providers. In application layer, anonymity is used to mask the real identities of data sources/providers. To enable privacy-preserving data mining, secure multiparty computation (SMC) and homomorphic encryption provide options for protecting raw data when multiple parties jointly run a data mining algorithm. Through cryptographic techniques, no party knows anything else than its own input and expected results. For data truth discovery, applicable solutions include correlation-based data quality analysis and trust evaluation of data sources.

But current solutions are still imperfect, incomprehensive, and inefficient. Data perturbation could lower the accuracy of data mining. Anonymity or anonymization makes it hard to detect malicious data sources, especially when anonymous identifiers change frequently. This technique could negatively influence the quality of trust evaluation on data sources and data mining. SMC and homomorphic encryption-based solutions suffer from high computational overhead, thus are not suitable for big data processing and are hard to be deployed in practice. In addition, it is very challenging to verify the correctness of data processing and mining results in SMC or when the data are processed in an encrypted form. It is difficult to ensure the trustworthiness of multiparty computation. Another issue is that SMC or homomorphic encryption-based solutions are normally not generic. They are only applicable in certain application scenarios. This fact greatly affects the wide adoption and deployment of this kind of schemes. In addition, privacy preservation conflicts with trust management, which brings additional challenges to trust management in crowdsourcing, especially in detecting distrusted data sources and untrustworthy data. Emerging technologies boost novel solutions for trust, security, and privacy in crowdsourcing. But at the same time, many challenges are yet to be overcome.

This Special Issue aims to bring together researchers and practitioners to discuss various aspects of trust, security, and privacy in crowdsourcing, explore key theories, investigate technology enablers, and innovate solutions for overcoming major challenges in this research field. We selected 11 research papers from more than 30 submissions after rigorous peer-reviews. Next, we categorize these 11 accepted papers into three categories and briefly introduce each paper and highlight its main contributions.

Crowdsourcing Trust: With the popularity of sensor-rich mobile devices, mobile crowdsourcing (MCS) has emerged as an effective method for data collection and processing.

Digital Object Identifier 10.1109/JIOT.2018.2860302

MCS holds many advantages, such as mobility, scalability, cost-efficiency, and collective intelligence. However, MCS still faces many challenges with regard to security, privacy, and trust. The paper entitled "A Survey on Security, Privacy, and Trust in Mobile Crowdsourcing" provides a thorough survey on the current advances of the research in MCS trust, security, and privacy. The authors of this paper analyzed the characteristics of MCS, identified its security threats, and proposed essential requirements of a secure, privacy-preserving, and trustworthy MCS system. They reviewed and commented existing solutions based on these requirements and compared their pros and cons. Open issues were also pointed out with a number of future research directions proposed.

In the paper entitled "Dynamic Trust Relationships Aware Data Privacy Protection in Mobile Crowd-Sensing," Wu *et al.* proposed a dynamic trust relationships aware data privacy protection mechanism for mobile crowd-sensing. It combines key distribution with trust management. The trust value of a public key is evaluated according to the number of supporters and the trust degree of the public key, as well as the accuracy of the public key provided by the encountering nodes. The authors also applied trust to decide the path of data relay in crowd-sensing.

Crowdsourcing Security: Remote user authentication is highly essential for a hazard-free use of crowdsourcing IoT services. In the paper entitled "Chaotic Map-Based Anonymous User Authentication Scheme With User Biometrics and Fuzzy Extractor for Crowdsourcing Internet of Things," Roy *et al.* proposed a secure remote user authentication protocol based on extended chaotic maps in order to avoid computationally expensive elliptic curve point multiplication or modular exponentiation operation. The protocol adopts three factors for authentication: 1) smart card; 2) password; and 3) personal biometrics. Formal security analysis based on ProVerif 1.93, real-or-random model and Burrows–Abadi–Needham logic shows its security.

For identifying missing key tags in anonymous RFID systems, Chen *et al.* proposed a vector-based missing key tag identification protocol (VEKI) and an improved protocol called iVEKI in the paper entitled "Efficiently and Completely Identifying Missing Key Tags for Anonymous RFID Systems." iVEKI consists of two phases: 1) ordinary tag deactivation and 2) missing key tag identification. The parameters of the proposed VEKI and iVEKI protocols were theoretically optimized to maximize time efficiency.

In order to improve the quality of existing protocols in terms of vulnerability and computation complexity, in the paper entitled "Dynamic Authentication Protocol Using Self-Powered Timers for Passive Internet of Things," Afifi *et al.* presented variants of a novel authentication protocol that can overcome the security flaws of previous protocols while being well suited to the computational capability of the tags. They applied self-powered timing devices for robust time-keeping and synchronization without the need for any external powering.

Crowdsourcing Privacy: In the paper entitled "Analyzing and Evaluating Efficient Privacy-Preserving Localization for Pervasive Computing," Wang *et al.* proposed an adjacent subtraction-based localization (ASL) model to achieve privacy-preserving localization in crowdsourcing in order to overcome high computational and communication overheads in the solutions based on homomorphic encryption techniques. They developed an efficient privacy-preserving localization (EPPL) algorithm under ASL without using any homomorphic encryption technique. Through analysis, proof, and simulations, the performance of EPPL regarding the correctness, privacy, and efficiency was evaluated.

In order to enable mobile users to issue search queries and achieve fine-grained access control over ciphertexts in a privacy-preserving manner in cloud-based MCS, Miao *et al.* studied multikeyword search in the context of MCS in the paper entitled "Practical Attribute-Based Multi-Keyword Search Scheme in Mobile Crowdsourcing." They devised a practical cryptographic primitive called attribute-based multikeyword search scheme to support comparable attributes by utilizing 0-encoding and 1-encoding. This scheme is selectively secure against chosen-keyword attack in generic bilinear group model with improved computational and storage costs.

Signcryption is the significant cryptographic primitive that meets the requirements of authenticity and confidentiality of crowdsourced data among users/industries. In the paper entitled "Provably Secure Identity-Based Signcryption Scheme for Crowdsourced Industrial Internet of Things Environments," Karati *et al.* presented a new identity-based signcryption (IBSC) scheme using bilinear pairing for Industrial IoT deployment. They studied two hard problems: 1) modified bilinear Diffie–Hellman inversion assumption and 2) modified bilinear strong Diffie–Hellman assumption. Rigorous security analysis and performance comparison demonstrate that the IBSC scheme is appropriate for industrial IoT crowdsourcing environments and is applicable for low-bandwidth communications.

In the paper entitled "Privacy-Preserving Double-Projection Deep Computation Model With Crowdsourcing on Cloud for Big Data Feature Learning," Zhang *et al.* proposed a double-projection deep computation model (DPDCM) for big data feature learning. It can project raw input data into two separate subspaces in hidden layers to learn interacted features of big data by replacing the hidden layers of the conventional deep computation model with double-projection layers. A learning algorithm was also devised to train the DPDCM. To protect data privacy, a privacy-preserving DPDCM (PPDPDCM) was further proposed based on the BGV encryption scheme with expected efficiency.

In the paper entitled "Efficient and Privacy-Preserving Proximity Detection Scheme for Social Applications," Zhu *et al.* proposed two efficient and privacy-preserving proximity detection schemes, named AGRQ-P and AGRQ-C, for location-based social applications, including crowdsourcing. The proposed schemes can preserve user location query information and accurate location information since users' query and location information is blurred into chipertext, thus no one but the user knows her/his own sensitive information.

In the paper entitled "A Privacy-Aware Architecture at the Edge for Autonomous Real-Time Identity Reidentification in Crowds," Miraftabzadeh *et al.* proposed an embedding

algorithm pipeline to extract and administrate the crowdsourced facial image. The proposed facial embedding is a privacy-aware parameterized function, which maps facial images to high-dimensional vectors in order to facilitate the identification and tracking of individuals.

Editing this Special Issue has been an invaluable experience for us. We would like to express our appreciation to all authors for their contributions and the reviewers for their valuable review comments. We also sincerely thank the Editor-in-Chief and the Editorial Board of this JOURNAL for approving this Special Issue and their continuous support on its final publication. We hope this Special Issue will provide a useful reference to its readers and contribute to advances in crowdsourcing trust, security, and privacy, as well as stimulate additional innovation in this promising field.

ACKNOWLEDGMENT

This work was supported in part by the NSFC under Grant 61672410 and Grant U1536202, in part by the National Key Research and Development Program of China under Grant 2016YFB0800704, in part by the Project Supported by the Natural Science Basic Research Plan in Shaanxi Province of China under Grant 2016ZDJC-06, in part by 111 Project under Grant B16037 and Grant B08038, and in part by the Academy of Finland under Grant 308087. The work of T. Hou was supported by the U.S. National Science Foundation under Grant CNS-1443889, Grant CNS-1446478, and Grant CNS-1405747.

ZHENG YAN, *Guest Editor*
School of Cyber Engineering
Xidian University
Xi'an 710071, China
and
Department of Communications and Networking
Aalto University
02150 Espoo, Finland

KAI ZENG, *Guest Editor*
Department of Electrical and Computer Engineering
George Mason University
Fairfax, VA 22030 USA

YU XIAO, *Guest Editor*
Department of Communications and Networking
Aalto University
02150 Espoo, Finland

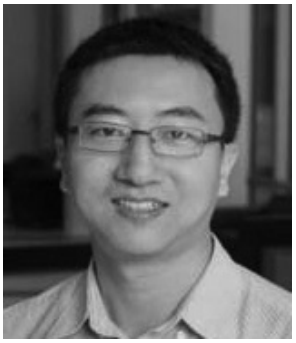
THOMAS HOU, *Guest Editor*
Bradley Department of Electrical and Computer Engineering
Virginia Polytechnic Institute and State University
Blacksburg, VA 24061 USA

PIERANGELA SAMARATI, *Guest Editor*
Department of Computer Science
Università degli Studi di Milano
26013 Crema, Italy

Zheng Yan (M'06–SM'14) received the Doctor of Science degree in technology from the Helsinki University of Technology, Espoo, Finland.

She is currently a Professor with Xidian University, Xi'an, China, and a Visiting Professor and a Finnish Academy Research Fellow with Aalto University, Espoo. She has authored or co-authored about 200 peer-reviewed papers, 8 conference proceedings, and solely authored 2 books about trust management. She holds over 60 granted patents and PCT patents, all of them adopted by industry. Some of her granted patents are applied in international standards. Her current research interests include trust, security, and privacy, blockchain, data mining, mobile applications and services, social networking, and cloud computing.

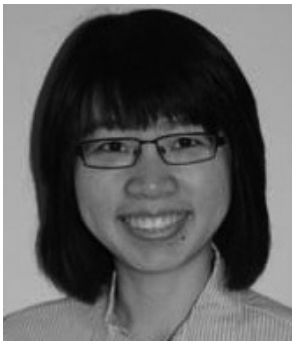
Prof. Yan was a recipient of number of Outstanding Leadership Awards of IEEE conference organization, the 2017 IEEE ComSoc TCBD Best Journal Paper Award, the Outstanding Associate Editor of 2017 for IEEE ACCESS, the Best Individual of Shaanxi Province from Abroad in 2014, "100 Expert Plan" Winner of Shaanxi Province, China, in 2011, and the Sisu Award of Nokia Research Center in 2010. She serves as an Organizational and Technical Committee member for over 80 international conferences and workshops. She is an Associate Editor of the IEEE INTERNET OF THINGS JOURNAL, *Information Fusion*, *Information Sciences*, IEEE ACCESS, the *Journal of Network and Computer Applications*, *Soft Computing*, *IEEE Blockchain Newsletter*, and *Security and Communication Networks* and as a special issue leading Guest Editor of the *ACM Transactions on Multimedia Computing, Communications, and Applications*, IEEE SYSTEMS JOURNAL, *Future Generation Computer Systems*, *Computers & Security*, the *International Journal of Computer Systems*, and *Mobile Networks and Applications*. She is a Founder Steering Committee Co-Chair of the IEEE Blockchain Conference. She is organizing/has organized over 10 conferences, such as IEEE Blockchain 2018, NSS/ICA3PP/IEEE CIT2017, IEEE TrustCom/BigDataSE/ISPA-2015, and IEEE CIT2014. She has given 20 keynotes and invited talks at international conferences and universities.



Kai Zeng received the Ph.D. degree in electrical and computer engineering from the Worcester Polytechnic Institute (WPI), Worcester, MA, USA, in 2008.

He is currently an Associate Professor with the Department of Electrical and Computer Engineering, the Department of Computer Science, and the Center for Secure Information Systems, George Mason University, Fairfax, VA, USA. From 2008 to 2011, he was a Post-Doctoral Scholar with the Department of Computer Science, University of California at Davis (UCD), Davis, CA, USA. From 2011 to 2014, he was an Assistant Professor with the Department of Computer and Information Science, University of Michigan–Dearborn, Dearborn, MI, USA. His current research interests include wireless security, cyber-physical system/IoT security and privacy, and cognitive radio networks.

Dr. Zeng was a recipient of the Sigma Xi Outstanding Ph.D. Dissertation Award from WPI in 2008, the Excellence in Post-Doctoral Research Award from UCD in 2011, and the U.S. National Science Foundation Faculty Early Career Development (CAREER) Award in 2012. He currently serves as an Editor for the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS.



Yu Xiao received the bachelor's and master's degrees from the Beijing University of Posts and Telecommunications, Beijing, China, in 2004 and 2007, respectively, and the doctoral degree (with Distinction) from Aalto University, Espoo, Finland, in 2012.

She is an Assistant Professor with the Department of Communications and Networking, Aalto University. Her current research interests have spanned from energy-efficient mobile computing, to edge computing, to crowdsensing, and to wearable cognitive computing.

Dr. Xiao was a recipient of the Young Researcher Award of the Finnish Foundation for Technology Promotion in 2017.

Thomas Hou received the Ph.D. degree from the New York University Tandon School of Engineering, New York, NY, USA, in 1998.

He is a Bradley Distinguished Professor of Electrical and Computer Engineering with the Virginia Polytechnic Institute and State University, Blacksburg, VA, USA. From 1997 to 2002, he was a Researcher with the Fujitsu Laboratories of America, Sunnyvale, CA, USA. He authored two textbooks entitled *Cognitive Radio Communications and Networks: Principles and Practices* (Academic/Elsevier, 2009) and *Applied Optimization Methods for Wireless Networks* (Cambridge Univ. Press, 2014). The first book has been selected as one of the Best Readings on Cognitive Radio by the IEEE Communications Society. He holds five U.S. patents. His current research interests include develop innovative solutions to complex cross-layer optimization problems in wireless networks. He is particularly interested in exploring new performance limits at the network layer by exploiting advances at the physical layer.

Prof. Hou was a recipient of five Best Paper Awards from the IEEE and two paper awards from the ACM for his research. He is the Steering Committee Chair of IEEE INFOCOM. He is a member of the Board of Governors and a Distinguished Lecturer of the IEEE Communications Society.

Pierangela Samarati (F'12) is a Professor with the Department of Computer Science, Università degli Studi di Milano, Milan, Italy. She has been a Computer Scientist with the Computer Science Laboratory, SRI, Menlo Park, CA, USA. She has been a Visiting Researcher with the Computer Science Department, Stanford University, Stanford, CA, USA, and with the Center for Secure Information Systems, George Mason University, Fairfax, VA, USA. She has authored or co-authored over 260 peer-reviewed papers in international journals, conference proceedings, and book chapters. Her current research interests include data and applications security and privacy, especially in emerging scenarios. She has participated in several projects involving different aspects of information protection.

Ms. Samarati was a recipient of the IEEE Computer Society Technical Achievement Award in 2016, the IFIP TC11 Kristian Beckman Award in 2008, and the IFIP WG 11.3 Outstanding Research Contributions Award in 2012. She is the Chair of the IEEE Systems Council Technical Committee on Security and Privacy in Complex Information Systems, the ERCIM Security and Trust Management Working Group, and the ACM Workshop on Privacy in the Electronic Society. She is a member of several Steering Committees. She was an ACM Distinguished Scientist in 2009. She has served as the General Chair, Program Chair, and Program Committee member for several international conferences and workshops (http://www.di.unimi.it/samarati).