Guest Editorial
Special Issue on Recent Advances of Security, Privacy, and Trust in Mobile Crowdsourcing

WITH the rapid advances in mobile and communication technologies, mobile devices are equipped with powerful processors, various sensors, large memories, and fast wireless communication modules. By taking advantage of powerful mobile devices and human intelligence, mobile crowdsourcing is an emerging paradigm that enables users to outsource tasks (usually difficult to accomplish individually) to a group of people (workers) at an affordable price. Specifically, human mobility offers unprecedented opportunities to sense the surroundings wherever their holders arrive, and human capabilities also offer intelligent human-assisted computation with their devices, e.g., human perception, intelligence, cognition, knowledge, visual recognition, and experiences.

Due to human involvement and crowdsourcing, critical concerns are raised toward security, privacy, and trust in mobile crowdsourcing, e.g., location leakage in sensed data, false data injection by malicious workers. However, it is challenging to protect security and privacy, especially in the IoT era, due to human mobility, device diversity, dynamic topology, and data heterogeneity. To address these challenges, this special issue solicits the latest research outcomes and developments on security, privacy, and trust in mobile crowdsourcing. Topics of interest include, but are not limited to: authentication of mobile crowdsourcing devices, key management in mobile crowdsourcing, access control of task contents and results, trust-aware and privacy-preserving task matching and recommendation, privacy-preserving truth discovery in mobile crowdsensing (MC), privacy-preserving data processing and analytics in the cloud, fog, and IoT, secure and privacy-preserving federated learning and machine learning, trust management of crowdsourcing workers, trust-aware incentive mechanisms, blockchain-assisted crowdsourcing, security and privacy in fog/edge-assisted mobile crowdsourcing, and secure and privacy-preserving mobile crowdsourcing in smart city applications.

The response to our above theme was overwhelming, with 76 papers submitted in the open Calls for Papers around the world. During the review process, each paper was assigned to and reviewed by multiple experts in the relevant areas, with a rigorous two-round review process. Thanks to the courtesy of the Editor-in-Chief of this journal, Dr. Nei Kato, we were able to accept 16 excellent papers covering various aspects of "Recent Advances of Security, Privacy, and Trust in Mobile Crowdsourcing." In the following, let us introduce these papers and highlight their main contributions.

Chen et al. [A1] introduce a privacy-preserving decentralized mobile crowdsourcing federated learning (FL-MCS) scheme based on blockchain. They employ ID-based aggregated decryptable broadcast encryption (ADIBBE) for secure communication, enabling senders to decrypt their ciphertexts individually while allowing aggregated ciphertexts to be decrypted collectively by all receivers within the group. Additionally, they devise a dropout-tolerated aggregation algorithm based on AD-IBBE.

Edirimannage et al. [A2] introduce a method for robust model aggregation in federated learning. It selects high-quality local models and incorporates a quality-aware incentive mechanism to detect and address free-rider attacks, where workers exploit contributions without participating meaningfully.

Fan et al. [A3] introduce the federated learning similar gradients (FLSGs) scheme to protect privacy in vertical federated learning. FLSG generates random gradients similar to the originals from a Gaussian distribution and replaces the originals with these perturbed gradients if they are close enough, safeguarding against inference attacks.

Wang et al. [A4] study cooperative item selection to maximize a submodular function among clients while ensuring strong privacy for their sensitive data. They propose an efficient approximation algorithm that incorporates client-level differential privacy mechanisms, decomposed function evaluations, and two heuristics to reduce privacy costs, computational overhead, and communication.

Wang et al. [A5] introduce a collaborative learning scheme that adapts to varying privacy requirements. They achieve this by adding customized Gaussian noise to local models and perturbing the aggregated model based on clients' privacy needs.

Min et al. [A6] introduce a novel learning-based geo-perturbation mechanism using 3-D geo-indistinguishability (3D-GI) to enhance location privacy protection in 3-D mobile crowdsourcing. They achieve this by defining an optimization objective that balances location privacy and MCS server profit and using the asynchronous advantage actor–critic (A3C) algorithm for reinforcement learning, enabling the derivation of an optimal perturbation policy without prior knowledge of system and attack models.

Lian et al. [A7] tackle the problem of scheduling security critical tasks in a multiserver mobile-edge computing (MEC) environment. They use convergent grey wolf optimizer

Digital Object Identifier 10.1109/JIOT.2023.3339395

(CGWO) metaheuristic algorithms to find optimal scheduling solutions. CGWO employs task permutations and a probability-based mapping scheme within the grey wolf optimizer (GWO). They introduce a novel position update strategy to ensure convergence to the global best solution and performed an analysis to determine appropriate parameter values to avoid local optima.

Ma et al. [A8] propose a scheme for privacy-preserving aggregation in industrial IoT crowdsourcing. They address the balance between privacy and data benefits by introducing protocols for dynamic virtual area construction, a low-cost aggregation algorithm, and a supervised mechanism for energy-aware aggregation. The scheme ensures data privacy and integrity using polynomial functions and binary data characteristics, validated by an iterative game model.

Lu et al. [A9] introduce a fast double-perturbation scheme for a cloud–fog–edge data-sharing platform. They design a swift spherical G-lattice sampling algorithm using G-perturbation and G-lattice samplers. Additionally, they optimize computational task assignment in PGS-LT by considering entity capabilities in the cloud–fog–edge platform.

Fu et al. [A10] introduce a unified encrypted-tensor model to represent heterogeneous data, including unstructured, semi-structured, and structured data from various sources and formats. To handle this data heterogeneity, they develop an encrypted query index and implemented a query scheme that transforms the diverse data into a unified graph structure.

Tang et al. [A11] introduce the BTV-CMAB scheme, which addresses worker quality and trust in mobile crowdsourcing. They use a truth quality discovery approach and a bidirectional trust verification (BTV) mechanism to assess requesters' trust and workers' reputations. Top-performing workers are selected using an upper confidence bound (UCB) index, ensuring truthfulness and individual rationality.

Huang et al. [A12] introduce a secure blockchain-assisted socially aware MC framework using Ethereum's smart contract technology. They apply a two-stage Stackelberg game model to help the requester set task prices, allowing mobile users to choose tasks and participation levels. They analyze game equilibrium using an extended Hessian matrix method for multiuser–multitask settings.

Chen et al. [A13] propose a scheme called SecTangle, aimed at reducing IOTA's vulnerability to double-spending attacks. The key idea is to adjust critical factors of the security threshold to identify fake tangle branches efficiently, enhancing tangle robustness. Additionally, they develop a transaction recovery algorithm to restore time-sensitive legitimate transaction branches.

Li et al. [A14] introduce a blockchain-based streaming media platform with smart contracts. They design a pay-as-you-go billing model and an incentive mechanism using probabilistic payments. To improve fairness, they introduce a refund protocol for consecutive payments. The framework is resistant to censorship and transparent. They implement two schemes: Scheme I relies on smart contracts for high security but higher costs, while Scheme II uses off-chain channels for faster execution with lower costs.

Wang et al. [A15] introduce an efficient framework for managing large-scale mixed traffic. This framework combines privacy-preserving crowdsourcing and dynamic vehicle routing and comprises three key modules: 1) a privacy-protecting crowdsensing method; 2) a traffic forecasting approach based on graph propagation; and 3) a privacy-preserving route selection mechanism.

Chang et al. [A16] propose 3PFT, a privacy-preserving scheme for smart grids. It ensures user privacy on smart meters with minimal resource use, offers fault tolerance, supports complex data analysis, and safeguards against key leakage attacks. They incorporate secret sharing, a flexible data aggregation protocol, and a negotiation-based key update method to achieve these objectives.

In conclusion, we extend our heartfelt appreciation to all the authors for their outstanding contributions and unwavering support. We also express our gratitude to the diligent reviewers for their dedicated efforts in reviewing the papers, offering valuable comments, and providing constructive suggestions that have significantly enhanced the quality of the papers. Finally, we would like to acknowledge and thank the Editor-in-Chief of this journal, Dr. Nei Kato, for his invaluable guidance and support throughout the entire publication process.

APPENDIX: RELATED ARTICLES

[A1] T. Chen, X. Wang, H.-N. Dai, and H. Yang, "A dropout-tolerated privacy-preserving method for decentralized crowdsourced federated learning," *IEEE Internet Things J.*, vol. 11, no. 2, pp. 1788–1799, Jan. 15, 2024.

[A2] S. Edirimannage, C. Elvitigala, I. Khalil, P. Wijesekera, and X. Yi, "QARMA-FL: Quality-aware robust model aggregation for mobile crowdsourcing," *IEEE Internet Things J.*, vol. 11, no. 2, pp. 1800–1815, Jan. 15, 2024.

[A3] K. Fan, J. Hong, W. Li, X. Zhao, H. Li, and Y. Yang, "FLSG: A novel defense strategy against inference attacks in vertical federated learning," *IEEE Internet Things J.*, vol. 11, no. 2, pp. 1816–1826, Jan. 15, 2024.

[A4] Y. Wang, T. Zhou, C. Chen, and Y. Wang, "Federated submodular maximization with differential privacy," *IEEE Internet Things J.*, vol. 11, no. 2, pp. 1827–1839, Jan. 15, 2024.

[A5] X. Wang, H. Zhang, M. Yang, X. Wu, and P. Cheng, "Privacy-preserving collaborative learning: A scheme providing heterogeneous protection," *IEEE Internet Things J.*, vol. 11, no. 2, pp. 1840–1853, Jan. 15, 2024.

[A6] M. Min et al., "Geo-perturbation for task allocation in 3D mobile crowdsourcing: An A3C-based approach," *IEEE Internet Things J.*, vol. 11, no. 2, pp. 1854–1865, Jan. 15, 2024.

[A7] Z. Lian, J. Shu, Y. Zhang, and J. Sun, "Convergent grey wolf optimizer metaheuristics for scheduling crowdsourcing applications in mobile edge computing," *IEEE Internet Things J.*, vol. 11, no. 2, pp. 1866–1879, Jan. 15, 2024.

[A8] R. Ma, T. Feng, J. Xiong, Q. Li, and Y. Tian, "DScPA: A dynamic sub-cluster privacy-preserving aggregation scheme for mobile crowdsourcing in Industrial IoT," *IEEE Internet Things J.*, vol. 11, no. 2, pp. 1880–1892, Jan. 15, 2024.

[A9] H. Lu, Y. Zhu, C. E. Chen, R. Feng, L. Zhang, and D. Ma, "Efficient key generation on lattice cryptography for privacy protection in mobile IoT crowdsourcing," *IEEE Internet Things J.*, vol. 11, no. 2, pp. 1893–1909, Jan. 15, 2024.

[A10] X. Fu, L. T. Yang, J. Li, X. Yang, and Z. Yang, "A searchable symmetric encryption-based privacy protection scheme for cloud-assisted mobile crowdsourcing," *IEEE Internet Things J.*, vol. 11, no. 2, pp. 1910–1924, Jan. 15, 2024.

[A11] J. Tang et al., "BTV-CMAB: A bi-directional trust verification based combinatorial multi-armed bandit scheme for mobile crowdsourcing," *IEEE Internet Things J.*, vol. 11, no. 2, pp. 1925–1938, Jan. 15, 2024.

[A12] S. Huang et al., "Gather or scatter: Stackelberg game based task decision for blockchain-assisted socially-aware crowdsensing framework," *IEEE Internet Things J.*, vol. 11, no. 2, pp. 1939–1951, Jan. 15, 2024.

[A13] Y. Chen, Y. Guo, M. Wang, E. Xu, H. Xie, and R. Bie, "Securing IOTA blockchain against tangle vulnerability by using large deviation theory," *IEEE Internet Things J.*, vol. 11, no. 2, pp. 1952–1965, Jan. 15, 2024.

[A14] T. Li et al., "Enabling secure and flexible streaming media with blockchain incentive," *IEEE Internet Things J.*, vol. 11, no. 2, pp. 1966–1980, Jan. 15, 2024.

[A15] D. Wang, W. Li, and J. Pan, "Large-scale mixed traffic control using dynamic vehicle routing and privacy-preserving crowdsourcing," *IEEE Internet Things J.*, vol. 11, no. 2, pp. 1981–1989, Jan. 15, 2024.

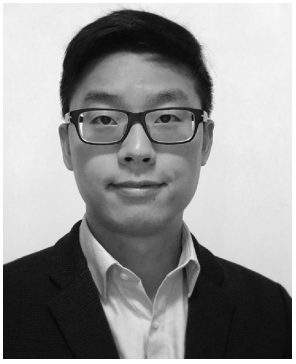
[A16] Y. Chang, J. Li, N. Lu, W. Shi, Z. Su, and W. Meng, "Practical privacy-preserving scheme with fault tolerance for smart grids," *IEEE Internet Things J.*, vol. 11, no. 2, pp. 1990–2005, Jan. 15, 2024.

KAN YANG, *Guest Editor*
Department of Computer Science
The University of Memphis
Memphis, TN 38152 USA
E-mail: kan.yang@memphis.edu

RONGXING LU, *Guest Editor*
Faculty of Computer Science
University of New Brunswick
Fredericton, NB E3B 5A3, Canada
E-mail: RLU1@unb.ca

MOHAMED M. E. A. MAHMOUD, *Guest Editor*
Department of Electrical and Computer Engineering
Tennessee Technological University
Cookeville, TN 38505 USA
E-mail: mmahmoud@tntech.edu

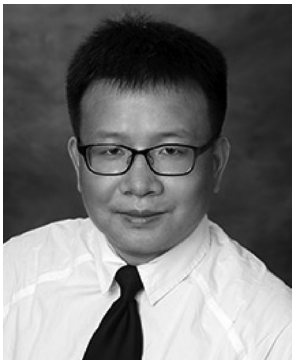
XIAOHUA JIA, *Guest Editor*
Department of Computer Science
City University of Hong Kong
Hong Kong, China
E-mail: csjia@cityu.edu.hk



Kan Yang (Senior Member, IEEE) received the B.Eng. degree in information security from the University of Science and Technology of China, Hefei, China, in 2008, and the Ph.D. degree in computer science from the City University of Hong Kong, Hong Kong, in 2013.

He was a Postdoctoral Fellow with the City University of Hong Kong from 2013 to 2014 and the University of Waterloo, Waterloo, ON, Canada, from 2014 to 2016. He is currently an Assistant Professor with the Department of Computer Science and an Associate Director of the Center for Information Assurance (a CAE-CDE and CAE-R designated center), The University of Memphis, Memphis, TN, USA. His research interests include data security, blockchain, AI security, network security, and applied cryptography.

Dr. Yang is an active reviewer for over 20 journals. He served as the Travel Grant Chair for ICDCS'23. He has also organized several cybersecurity outreach activities, such as cybersecurity summit and cybersecurity summer camp. He has served as a TPC member for many conferences, including Globecom, ICC, MASS, Blockchain, ICNC, ICCCN, and IPCCC.



Rongxing Lu (Fellow, IEEE) received the Ph.D. degree from the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada, in 2012.

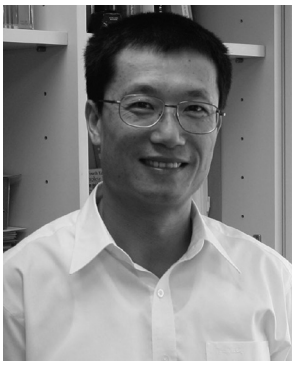
He is a University Research Scholar and a Professor with the Faculty of Computer Science (FCS), University of New Brunswick (UNB), Fredericton, NB, Canada. Before that, he worked as an Assistant Professor with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore, from April 2013 to August 2016. He worked as a Postdoctoral Fellow with the University of Waterloo from May 2012 to April 2013. He has published extensively in his areas of expertise (with H-index 78 from Google Scholar as of October 2021). His research interests include applied cryptography, privacy-enhancing technologies, and IoT-big data security and privacy.

Dr. Lu was awarded the most prestigious "Governor General's Gold Medal" in 2012, and won the 8th IEEE Communications Society (ComSoc) Asia–Pacific Outstanding Young Researcher Award in 2013. He was the recipient of nine best (student) paper awards from some reputable journals and conferences. He is the winner of the 2016–2017 Excellence in Teaching Award, FCS, UNB. He currently serves as the Vice-Chair (Conferences) of IEEE ComSoc Communications and Information Security Technical Committee and the Founding Co-Chair of IEEE TEMS Blockchain and Distributed Ledgers Technologies Technical Committee.

Mohamed M. E. A. Mahmoud received the Ph.D. degree from the University of Waterloo, Waterloo, ON, Canada, in April 2011.

He is currently a Professor with the Department of Electrical and Computer Engineering, Tennessee Tech University, Cookeville, TN, USA. He is the author of more than 100 papers published in IEEE conferences and journals. His research interests include security and privacy preserving schemes for smart grid, e-health, and intelligent transportation systems.

Dr. Mahmoud has received the NSERC-PDF Award. He won the Best Paper Award from IEEE International Conference on Communications 2009, Dresden, Germany. He serves as an Associate Editor for IEEE INTERNET OF THINGS JOURNAL and *Peer-to-Peer Networking and Applications* (Springer). He served as a technical program committee member for several IEEE conferences.



Xiaohua Jia (Fellow, IEEE) received the B.Sc. and M.Eng. degrees from the University of Science and Technology of China, Hefei, China, in 1984 and 1987, respectively, and the D.Sc. degree in information science from the University of Tokyo, Tokyo, Japan, in 1991.

He is currently a Chair Professor with the Department of Computer Science, City University of Hong Kong, Hong Kong. His research interests include cloud computing and distributed systems, data security and privacy, computer networks, and mobile computing.

Prof. Jia is an Editor of IEEE TRANSACTIONS ON COMPUTERS since 2021, IEEE INTERNET OF THINGS JOURNAL from 2013 to 2018, IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS from 2006 to 2009, *Journal of World Wide Web*, and *Journal of Combinatorial Optimization*. He is the General Chair of ACM MobiHoc 2008, the TPC Co-Chair of IEEE GlobeCom 2010—Ad Hoc and Sensor Networking Symposium, the Area Chair of IEEE INFOCOM 2015–2017, the Track Chair of IEEE ICDCS 2019, and the General Chair of ACM ICN 2019. He is a Fellow of IEEE (Computer Society) and a Distinguished Member of ACM.