# Guest Editorial Special Issue on Secure Data Analytics for Emerging Internet of Things

THE RAPID developments in hardware, software, and communication technologies have facilitated the spread of interconnected sensors, actuators, and heterogeneous devices such as single board computers, which collect and exchange a large amount of data to offer a new class of advanced services characterized by being available anywhere, at any time, and for anyone. This ecosystem is widely referred to as the Internet of Things (IoT). In the past years, the number of deployments both for sensor networks and the IoT grew significantly. This continuous and exponential growth is facilitated by investments and research activities originating from industry, academia, and governments while the penetration of these technologies is also driven by the high technology acceptance rates of both consumers and technologists across disciplines. Such networks collect, store, and exchange a large volume of heterogeneous data. Nevertheless, their rapid and widespread deployment, along with their participation in the provisioning of potentially critical services (e.g., safety applications, healthcare, and manufacturing) raise numerous issues related to the security, data analysis, and energy awareness of the performed operations and provided services.

Accordingly, research on the data analysis and security of IoT is attracting increasing attention from both industry and academia. In line with these efforts, the central theme of this special issue (SI) is to report novel methodologies, theories, technologies, techniques, and solutions for security and data analytics techniques and energy-aware solutions for IoT.

This journal's SI focuses on the recent advancements and different research areas in security and data analysis under the IoT framework. Further, it focuses on addressing these topics across multiple abstraction levels, ranging from architectural models, the provisioning of services, protocols, and interfaces to specific implementation approaches. Furthermore, it extends over the areas related to the role of data mining and machine learning in modeling and deploying secure and trustworthy sensor networks in IoT. This SI brings together the latest industrial and academic progress, research, and development efforts within the rapidly maturing IoT ecosystem.

The response to our Calls for Papers on this SI was highly satisfactory, with 140 submissions from around the globe. Each paper was assigned to and reviewed by at least three experts in the relevant areas, with a rigorous two to three rounds of review during the review process. We were able to accept 25 high-quality articles as discussed below.

In [A1], Zhao *et al.* proposed a blockchain-based auditable privacy-preserving data classification (PPDC) scheme for IoT to prevent the malicious data center/data processor while guaranteeing the utility and privacy of data. Specifically, the authors presented a new controllably linkable group signature (CL-GS) to balance the utility and privacy of data and take advantage of blockchain to audit the correctness of PPDC against malicious data processor/data center.

In [A2], Alasmary *et al.* constructed a neural-network-based model, called ShellCore, to detect malicious shell commands. They used conventional machine and deep-learning-based approaches trained with term- and character-level features to show that the accuracy of ShellCore is above 99% in detecting malicious shell commands and files.

In [A3], Ghosh *et al.* presented the concept of context-aware attribute learning with cipher-policy-attribute-based encryption (CP-ABE) to preserve the privacy of users' information in IoT-enabled 5.0. Specifically, the authors proposed a scheme, namely, CASE, which autonomously learns users' contextual information exploiting edge intelligence, generates attributes, and reduces the post-encryption data size using the learned attributes.

In [A4], Sharma *et al.* proposed a probabilistic framework that facilitates data routing between the nodes and local cloud in an IoT network coupled with a multitier trust and encryption scheme for secure data delivery in the cloud-based IoT network. They also evaluated their proposed scheme and compared with the standard protocols to show the efficiency of their proposed scheme.

In [A5], Bao *et al.* proposed a lightweight-attribute-based searchable encryption (LABSE) scheme. The scheme realizes fine-grained access control and keyword search while reducing the computational overhead for the resource-constrained devices. The authors also constructed a concrete deployment model for LABSE under the healthcare system.

In [A6], Hosen *et al.* developed an algorithm that first derives two objective functions, user and service provider satisfaction, from data concerning service provisioning, user preferences, and resources utilization. The proposed algorithm then combines these functions into a mutual objective function that maximizes the satisfaction of both individuals.

In [A7], Goswami *et al.* proposed a method for optimizing resource allocation using a convolutional neural network (CNN)

Digital Object Identifier 10.1109/JIOT.2021.3126438

to extract the optimal channel state for different applications, which ease the computations along with efficiency. Specifically, the authors provided the solution to the loss of network resources and the vulnerability of data that may arise due to multiobjective network and interference in the path.

In [A8], Mothukuri *et al.* proposed a federated learning (FL)-based anomaly detection approach to proactively recognize intrusion in IoT networks using decentralized on-device data. The proposed approach uses federated training rounds on gated recurrent units (GRUs) models and keeps the data intact on local IoT devices by sharing only the learned weights with the central server of the FL. Further, the ensembler part of the approach aggregates the updates from multiple sources to optimize the accuracy of the global ML model.

In [A9], Yuan *et al.* attempted first to explore the record-level privacy leakage against natural language processing (NLP) tasks in FL. The authors proposed a framework to investigate the exposure of the records of interest in federated aggregations by leveraging the perplexity of language modeling. Specifically, they presented two correlation attacks to identify the corresponding clients when extracting the specific records.

In [A10], Anajemba *et al.* presented a study for focusing to establish a secured connection in a multiple-antenna transmission when the channel state information (CSI) of eavesdropper (Eve) is unknown to the network users. Further, the authors proposed a model that comprises a secure wireless communication standard where Eve performs either optimal matched filtering (OMF) or a basic matched filtering (BMF) while the transmitting IoT node employs a smart jamming strategy in order to compromise the activities of Eve.

In [A11], Tanveer *et al.* presented a lightweight user authenticated key exchange (AKE) scheme for 6LoWPAN-based smart home networks (LAKE-6SH) to achieve authenticity of remote users and establish private session keys between the users and network entities by employing the SHA-256 hash function, exclusive-OR operation, and a simple authenticated encryption primitive. The authors also validated formally through the random oracle model and illustrated that LAKE-6SH is protected against different pernicious security attacks.

In [A12], Otoum *et al.* proposed an adaptive framework that integrates both FL and blockchain to achieve both network trustworthiness and security. The proposed solution is capable of dealing with individuals' trust as a probability and estimates the end-devices' trust values belonging to different networks subject to achieving security criteria.

In [A13], Sigh *et al.* developed a white-box adversarial attack mechanism to generate adversarial examples for data obtained from smart meters installed in residential houses. The authors presented an analysis to demonstrate that the statistical properties of adversarial datapoints are indistinguishable from those of the true datapoints. Further, they evaluated the effectiveness of defense mechanisms for white-box adversarial attacks on the proposed attack mechanism and showed that while they can reduce the potency of the attack, the original models still remain significantly affected by the adversarial attack.

In [A14], Chakraborty *et al.* analyzed the feasibility of implementing a honeyword-based defense strategy to prevent the latest developed server-side threat on the IoT domain's password. The authors also proposed a generic attack model, namely, a matching attack utilizing the compromised password-file to perform the security check of any legacy-UI approach for meeting the all essential flatness security criterion.

In [A15], Karim and Rawat presented a privacy risk reduction model for electronic toll transponder data. The authors proposed a fully homomorphic encryption protocol, named TollsOnly, that preserves the post-quantum privacy and enables users to share specific data with smart cities via blockchain technology.

In [A16], Tang *et al.* proposed a new systematic framework named software-defined edge-cloud computing (SD-ECC), which applies a standard software to control the hardware infrastructure regardless of vendor variations. Further, the authors presented the study on an optimal slicing-based resource orchestration problem by considering slice-initiated attacks as possible adversaries, which includes both interslice and intraslice resource orchestrations.

In [A17], Masud *et al.* presented a lightweight and anonymity-preserving user authentication protocol to counter threats, such as a denial-of-service attack, man-in-the-middle attack, and modification attack in IoT networks. The proposed scheme provides a secure session for the legitimate user and prohibits unauthorized users from gaining access to the IoT sensor nodes.

In [A18], Peng *et al.* designed a Chinese remainder theorem conversion method with the counter to encode multidimensional data into large integers, which can be operated by linear homomorphic encryption schemes. The authors introduced a multifunctional data analysis method supporting diversified aggregation functions, including linear, polynomial, and continuous functions. Further, they demonstrated that their proposed scheme can achieve confidentiality, integrity, authentication, and resistance against false data injection attacks.

In [A19], Ullah *et al.* presented a critical data reclamation (CDR) protocol that provides secure data transmission for isolated clusters. Specifically, the authors proposed the data transfer, data aggregation algorithms for sensing nodes, and data receiving and extraction at CH and sink.

In [A20], Tsemogne *et al.* proposed a zero-sum one-sided partially observable stochastic game (OS-POSG) model, in which a defender strategically places honeypots in the IoT network in order to deceive attacker's actions and mitigate the botnet propagation. Specifically, the authors focused on finding an optimal deception strategy for the defender that better limits from above the proportion of infected IoT devices.

In [A21], Ullah *et al.* presented a multimessage and multireceiver signcryption scheme for the multicast channel in a certificateless setting to solve the key escrow problem. The authors also eliminated the need of a secure channel in their proposed scheme.

In [A22], Yu *et al.* presented a secure Artificial Intelligence of Things (AIoT) for implicit group recommendations (SAIoT-GR). Specifically, the authors developed a secure IoT structure as the bottom support platform for the hardware module whereas they introduced a collaborative Bayesian network model and noncooperative game as algorithms for the software module.

In [A23], Bera *et al.* proposed a new access control protocol, called ACPBS-IoT, for battlefield surveillance in a drone-assisted IoT environment. The authors also demonstrated that the proposed ACPBS-IoT can resist several potential attacks needed in battlefield surveillance.

In [A24], He *et al*. introduced an efficient ciphertext-policy attribute-based encryption framework to implement an efficient collaborative decryption. The authors also implemented the functions of their framework and built a private chain to verify the feasibility of data transfer between users.

In [A25], Sun *et al*. presented an efficient and practical identity-based public key encryption (IBE) scheme having a revocation functionality to preserve data privacy in IoT applications. Based on the security of SM9 encryption and the bilinear DiffieŰHellman assumption, the proposed scheme can be proved secure against chosen ciphertext attacks.

We are thankful to the authors for their excellent contributions to this SI. We would like to deliver our appreciation to all the reviewers for dedicating their efforts in reviewing these articles, and for their valuable comments and suggestions that significantly improve the quality of the articles. Also, we would like to express our sincere gratitude to the Editor-in-Chief, Prof. H. Wang, for providing this opportunity and his important guidance throughout the process. We hope that this SI will serve as a good reference for the researchers and scientists from academia and industry in the field of secure data analytics for emerging IoT.

## APPENDIX: RELATED ARTICLES

[A1] Y. Zhao, X. Yang, Y. Yu, B. Qin, X. Du, and M. Guizani, "Blockchain-based auditable privacy-preserving data classification for Internet-of-Things," *IEEE Internet Things J.*, vol. 9, no. 4, pp. 2468–2484, Feb. 15, 2022, doi: 10.1109/JIOT.2021.3097890.

[A2] H. Alasmary *et al.*, "SHELLCORE: Automating malicious IoT software detection using shell commands representation," *IEEE Internet Things J.*, vol. 9, no. 4, pp. 2485–2496, Feb. 15, 2022, doi: 10.1109/JIOT.2021.3086398.

[A3] T. Ghosh, A. Roy, S. Misra, and N. S. Raghuwanshi, "CASE: Context-aware security scheme for preserving data privacy in IoT-enabled society 5.0," *IEEE Internet Things J.*, vol. 9, no. 4, pp. 2497–2504, Feb. 15, 2022, doi: 10.1109/JIOT.2021.3101115.

[A4] D. K. Sharma, K. K. Bhardwaj, S. Banyal, R. Gupta, N. Gupta, and L. Nkenyereye, "An opportunistic approach for cloud service based IoT routing framework administering data, transaction, and identity security," *IEEE Internet Things J.*, vol. 9, no. 4, pp. 2505–2512, Feb. 15, 2022, doi: 10.1109/JIOT.2021.3078810.

[A5] Y. Bao, W. Qiu, and X. Cheng, "Secure and lightweight fine-grained searchable data sharing for IoT-oriented and cloud-assisted smart healthcare system," *IEEE Internet Things J.*, vol. 9, no. 4, pp. 2513–2526, Feb. 15, 2022, doi: 10.1109/JIOT.2021.3063846.

[A6] A. S. M. S. Hosen, P. K. Sharma, and G. H. Cho, "MSRM-IoT: A reliable resource management for cloud, fog and mist assisted IoT networks," *IEEE Internet Things J.*, vol. 9, no. 4, pp. 2527–2537, Feb. 15, 2022, doi: 10.1109/JIOT.2021.3090779.

[A7] P. Goswami, A. Mukherjee, M. Maiti, S. K. S. Tyagi, and L. Yang, "A neural network based optimal resource allocation method for secure IIoT network," *IEEE Internet Things J.*, vol. 9, no. 4, pp. 2538–2544, Feb. 15, 2022, doi: 10.1109/JIOT.2021.3084636.

[A8] V. Mothukuri, P. Khare, R. M. Parizi, S. Pouriyeh, A. Dehghantanha, and G. Srivastava, "Federated learning-based anomaly detection for IoT security attacks," *IEEE Internet Things J.*, vol. 9, no. 4, pp. 2545–2554, Feb. 15, 2022, doi: 10.1109/JIOT.2021.3077803.

[A9] X. Yuan, X. Ma, L. Zhang, Y. Fang, and D. Wu, "Beyond class-level privacy leakage: Breaking record-level privacy in federated learning," *IEEE Internet Things J.*, vol. 9, no. 4, pp. 2555–2565, Feb. 15, 2022, doi: 10.1109/JIOT.2021.3089713.

[A10] J. H. Anajemba, T. Yue, C. Iwendi, P. Chatterjee, D. Ngabo, and W. S. Alnumay, "A secure multi-user privacy technique for wireless IoT networks using stochastic privacy optimization," *IEEE Internet Things J.*, vol. 9, no. 4, pp. 2566–2577, Feb. 15, 2022, doi: 10.1109/JIOT.2021.3050755.

[A11] M. Tanveer, G. Abbas, Z. H. Abbas, M. Bilal, A. Mukherjee, and K. S. Kwak, "LAKE-6SH: Lightweight user authenticated key exchange for 6LoWPAN-based smart homes," *IEEE Internet Things J.*, vol. 9, no. 4, pp. 2578–2591, Feb. 15, 2022, doi: 10.1109/JIOT.2021.3085595.

[A12] S. Otoum, I. A. Ridhawi, and H. Mouftah, "Securing critical IoT infrastructures with blockchain-supported federated learning," *IEEE Internet Things J.*, vol. 9, no. 4, pp. 2592–2601, Feb. 15, 2022, doi: 10.1109/JIOT.2021.3088056.

[A13] Sigh *et al.*, "Adversarial attack and defence strategies for deep learning based IoT device classification techniques," *IEEE Internet Things J.*, vol. 9, no. 4, pp. 2602–2613, Feb. 15, 2022, doi: 10.1109/JIOT.2021.3138541.

[A14] N. Chakraborty, M. Mukherjee, J. Li, M. Shojafar, and Y. Pan, "Cryptanalysis of a honeyword system in the IoT platform," *IEEE Internet Things J.*, vol. 9, no. 4, pp. 2614–2626, Feb. 15, 2022, doi: 10.1109/JIOT.2021.3080676.

[A15] H. Karim and D. B. Rawat, "TollsOnly please—Homomorphic encryption for toll transponder privacy in Internet of Vehicles," *IEEE Internet Things J.*, vol. 9, no. 4, pp. 2627–2636, Feb. 15, 2022, doi: 10.1109/JIOT.2021.3056240.

[A16] J. Tang, J. Nie, Z. Xiong, J. Zhao, Y. Zhang, and D. Niyato, "Slicing-based reliable resource orchestration for secure software defined edge-cloud computing systems," *IEEE Internet Things J.*, vol. 9, no. 4, pp. 2637–2648, Feb. 15, 2022, doi: 10.1109/JIOT.2021.3107490.

[A17] M. Masud, G. S. Gaba, K. Choudhary, M. S. Hossain, M. F. Alhamid, and G. Muhammad, "Lightweight and anonymity-preserving user authentication scheme for IoT-based healthcare," *IEEE Internet Things J.*, vol. 9, no. 4, pp. 2649–2656, Feb. 15, 2022, doi: 10.1109/JIOT.2021.3080461.

[A18] C. Peng, M. Luo, P. Vijayakumar, D. He, O. Said, and A. Tolba, "Multi-functional and multi-dimensional secure data aggregation schemes in WSNs," *IEEE Internet Things J.*, vol. 9, no. 4, pp. 2657–2668, Feb. 15, 2022, doi: 10.1109/JIOT.2021.3077866.

[A19] A. Ullah, M. Azeem, H. Ashraf, N. Z. Jhanjhi, L. Nkenyereye, and M. Humayun, "Secure critical data reclamation scheme for isolated clusters in IoT enabled WSN," *IEEE Internet Things J.*, vol. 9, no. 4, pp. 2669–2677, Feb. 15, 2022, doi: 10.1109/JIOT.2021.3098635.

[A20] O. Tsemogne, Y. Hayel, C. Kamhoua, and G. Deugoué, "Game theoretic modeling of cyber deception against epidemic botnets in Internet of Things," *IEEE Internet Things J.*, vol. 9, no. 4, pp. 2678–2687, Feb. 15, 2022, doi: 10.1109/JIOT.2021.3081751.

[A21] I. Ullah *et al.*, "An efficient and secure multi-message and multi-receiver signcryption scheme for edge enabled Internet of Vehicles," *IEEE Internet Things J.*, vol. 9, no. 4, pp. 2688–2697, Feb. 15, 2022, doi: 10.1109/JIOT.2021.3093068.

[A22] K. Yu, Z. Guo, Y. Shen, W. Wang, J. C.-W. Lin, and T. Sato, "Secure artificial intelligence of things for implicit group recommendations," *IEEE Internet Things J.*, vol. 9, no. 4, pp. 2698–2707, Feb. 15, 2022, doi: 10.1109/JIOT.2021.3079574.

[A23] B. Bera, A. K. Das, S. Garg, M. J. Piran, and M. S. Hossain, "Access control protocol for battlefield surveillance in drone-assisted IoT environment," *IEEE Internet Things J.*, vol. 9, no. 4, pp. 2708–2721, Feb. 15, 2022, doi: 10.1109/JIOT.2020.3049003.

[A24] He *et al.*, "An efficient ciphertext-policy attribute-based encryption scheme supporting collaborative decryption with blockchain," *IEEE Internet Things J.*, vol. 9, no. 4, pp. 2722–2733, Feb. 15, 2022, doi: 10.1109/JIOT.2021.3099171.

[A25] Sun *et al.*, "Efficient identity-based encryption with revocation for data privacy in Internet of Things," *IEEE Internet Things J.*, vol. 9, no. 4, pp. 2734–2743, Feb. 15, 2022, doi: 10.1109/JIOT.2021.3109655.

SACHIN S. SHETTY, *Guest Editor*
Old Dominion University
Norfolk, VA 23529 USA
(e-mail: sshetty@odu.edu)

JHING-FA WANG, *Guest Editor*
National Cheng Kung University
Tainan 701, Taiwan
(e-mail: jameswangjf@gmail.com)

UTTAM GHOSH, *Guest Editor*
Vanderbilt University
Nashville, TN 37235 USA
(e-mail: ghosh.uttam@ieee.org)

SCHAHRAM DUSTDAR, *Guest Editor*
TU Wien
1040 Vienna, Austria
(e-mail: dustdar@dsg.tuwien.ac.at)

**Sachin S. Shetty** received the Ph.D. degree in modeling and simulation from Old Dominion University, Norfolk, VA, USA, in 2007, under the supervision of Prof. M. Song.

He is a Professor with the Virginia Modeling, Analysis and Simulation Center, Old Dominion University. He holds a joint appointment with the Department of Modeling, Simulation and Visualization Engineering and the Center for Cybersecurity Education and Research. Prior to joining Old Dominion University, he was an Associate Professor with the Electrical and Computer Engineering Department, Tennessee State University, Nashville, TN, USA, where he was also the Associate Director of the Tennessee Interdisciplinary Graduate Engineering Research Institute and directed the Cyber Security Laboratory. He also holds a dual appointment as an Engineer with Naval Surface Warfare Center, Crane, IN, USA. His research interests lie at the intersection of computer networking, network security, and machine learning. His laboratory conducts cloud and mobile security research and has received over U.S. $10 million in funding from National Science Foundation, Air Office of Scientific Research, Air Force Research Lab, Office of Naval Research, Department of Homeland Security, and Boeing. He is the site lead on the DoD Cyber Security Center of Excellence, the Department of Homeland Security National Center of Excellence, the Critical Infrastructure Resilience Institute, and the Department of Energy, Cyber Resilient Energy Delivery Consortium. He has authored and coauthored over 140 research articles in journals and conference proceedings and two books.

Prof. Shetty is the recipient of the DHS Scientific Leadership Award and has been inducted in Tennessee State University's Million-Dollar Club. He has served on the technical program committee for ACM CCS and IEEE INFOCOM.

**Jhing-Fa Wang** received the bachelor's and master's degrees from National Cheng Kung University (NCKU), Tainan, Taiwan, in 1973 and 1979, respectively, and the Ph.D. degree from the Stevens Institute of Technology, Hoboken, NJ, USA, in 1983.

He is currently the Chair and the Distinguished Professor with the Department of Electrical Engineering, NCKU. His research area is mainly on multimedia signal processing, including speech signal processing, image processing, VLSI system design, and AI robots. Concerning about the publication, he has published about 160 journal papers on IEEE, SIAM, IEICE, and IEE and about 300 international conference papers since 1983. He recently has explored the research on Orange Technology. Orange Technology refers to a newly evolved interdisciplinary research area for integration and innovation of health, happiness, and care technologies. The objective of Orange Technology is to bring more health, happiness, and warming care to the society.

Prof. Wang received the Outstanding Research Awards and Outstanding Researcher Award from National Science Council in 1990, 1995, 1997, and 2006, respectively. He also received the Outstanding Industrial Awards from ACER and Institute of Information Industry and the Outstanding Professor Award from the Chinese Engineer Association, Taiwan, in 1991 and 1996, respectively. He also received the Culture Service Award from the Ministry of Education, Taiwan, in 2008, the Distinguished Scholar Award of KT Li from NCKU in 2009, the IEEE Tainan Section Best Service Award in 2011, the Innovation Education Award in 2013, and the Seoul International Invention Fair and Special Award from 2017 Kuwait International Invention Fair. He was also invited to give the Keynote Speeches in PACLIC 12 in Singapore, 1998, UWN 2005 in Taipei, WirlessCom 2005 in Hawaii, IIH-MSP 2006 in Pasadena, USA, ISM 2007 in Taichung, PCM 2008 in Tainan, 2011 ICAST in Dalian, China, 2011 ICSPCC in Xi'an, China, Keer 2012 in Penghu, Taiwan, HIS 2017 in Moscow Region, Russia, and ICOT 2015, ICOT 2016, and ICOT 2017 in Hong Kong, Australia, and Singapore, respectively. He also served as an Associate Editor for IEEE TRANSACTIONS ON NEURAL NETWORKS and IEEE TRANSACTIONS ON VERY LARGE SCALE INTEGRATION (VLSI) SYSTEMS and the Editor-in-Chief for *International Journal of Chinese Engineering* from 1995 to 2000. He was the President of Tajen University from 2012 to 2020, the formal chair of IEEE Tainan Section from 2005 to 2009, the Coordinator of Section/Chapter, IEEE Region 10 from 2011 to 2012, and the Industry Liaison-Coordinator of IEEE Region 10 from 2009 to 2011. He was elected as an IEEE Fellow in 1999 for his contribution on "Hardware and Software Co-design on Speech Signal Processing." He was also the General Chair of ISCAS 2009.

**Uttam Ghosh** (Senior Member, IEEE) received the Ph.D. degree in electronics and electrical engineering from the Indian Institute of Technology Kharagpur, Kharagpur, India, in 2013.

He is working as an Associate Professor of Cybersecurity with the Computer Science and Data Science Department, Meharry School of Applied Computational Sciences, Nashville, TN, USA. He worked as an Assistant Professor of the Practice with the Department of Computer Science, Vanderbilt University, Nashville, where he was awarded the 2018–2019 Junior Faculty Teaching Fellow (JFTF). He has a Postdoctoral experience with the University of Illinois at Urbana–Champaign, Urbana, IL, USA, Fordham University, New York, NY, USA, and Tennessee State University, Nashville. He has published over 80 papers at reputed international journals, including IEEE TRANSACTIONS, Elsevier, Springer, IET, Wiley, InderScience, and IETE, and also in top international conferences sponsored by IEEE, ACM, and Springer. He is co-editing ten books on Smart IoT, Security, and Data Analysis with CRC Press and Springer. His main research interests include cybersecurity, wireless 5G networks, SDN, energy delivery systems, and cloud computing.

Dr. Ghosh is serving as an Associate Editor of *Human-Centric Computing and Information Sciences*, *Springer and International Journal of Computers and Applications*, and Taylor & Francis. He is also a reviewer for international journals, including IEEE TRANSACTIONS, Elsevier, Springer, and Wiley. He serves as a guest editor for special issues with IEEE SENSORS, IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, IEEE JOURNAL OF HEALTH INFORMATICS, IEEE TRANSACTION ON NETWORK SCIENCE AND ENGINEERING, *ACM Transactions on Internet Technology*, *Computer Communications* (Elsevier), *Multimedia Tools and Applications* (Springer), *Internet Technology Letters* (Wiley), *Sensors and Future Internet* (MDPI). He has conducted several sessions and workshops related to cyberphysical systems (CPS), SDN, IoT, and smart cities as the co-chair at top international conferences, including IEEE Globecom 2020–2021, IEEE MASS 2020, SECON 2019–2020, CPSCOM 2019, and ICDCS 2017. He has served as a Technical Program Committee Member at renowned international conferences. He is a member of ACM and Sigma-Xi.

**Schahram Dustdar** (Fellow, IEEE) is a Full Professor of Computer Science heading the Research Division of Distributed Systems with TU Wien, Vienna, Austria. He holds several honorary positions with the University of California at Los Angeles, Los Angeles, CA, USA; Monash University, Melbourne, VIC, Australia; Shanghai University, Shanghai, China; Macquarie University, Sydney, NSW, Australia; and the University of Groningen, Groningen, The Netherlands, from 2004 to 2010. From December 2016 to January 2017, he was a Visiting Professor with the University of Sevilla, Seville, Spain, and from January 2017 to June 2017, he was a Visiting Professor with the University of California at Berkeley, Berkeley, CA, USA. From 1999 to 2007, he worked as the Co-Founder and the Chief Scientist of Caramba Labs Software AG, Vienna (acquired by Engineering NetWorld AG), a venture capital co-funded software company focused on software for collaborative processes in teams. Caramba Labs was nominated for several (international and national) awards: World Technology Award in the category of Software in 2001; Top-Startup companies in Austria (Cap Gemini Ernst & Young) in 2002; and MERCUR Innovation Award of the Austrian Chamber of Commerce in 2002.

Prof. Dustdar is the recipient of the ACM Distinguished Scientist Award in 2009 and the IBM Faculty Award in 2012. He is the Founding Co-Editor-in-Chief of the new *ACM Transactions on Internet of Things* as well as the Editor-in-Chief of *Computing* (Springer). He is the Co-Founder of edorer.com and sinoaus.net. He is an Associate Editor of IEEE TRANSACTIONS ON SERVICES COMPUTING, IEEE TRANSACTIONS ON CLOUD COMPUTING, *ACM Transactions on the Web*, and *ACM Transactions on Internet Technology*, as well as on the editorial board of IEEE INTERNET COMPUTING and IEEE COMPUTER. He is an Elected Member of the Academia Europaea: The Academy of Europe, where he is the Chairman of the Informatics Section. He is an AAAI Fellow and the President in 2021.