



Introducing the Special Topic on “Mitigating Cyber Threats and Defense in Data Intensive Smart Cities”

Kim-Kwang Raymond Choo¹ · Deepak Puthal² · Charles Zhechao Liu¹ · Chonggang Wang³

Published online: 10 November 2022

© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2022

Technologies are increasingly pervasive in our data intensive smart cities, as evidenced by the broad range of Internet-connected devices (also referred to as ‘Internet of Things’ (IoT)) and systems, ranging from smart grids to intelligent systems and technology to critical information infrastructure. There is also increasing recognition for the need to have rigorous foundations in cyber security; thus, the emphasis on developing innovative managerial, technological and strategic integrative solutions. For example, according to National Institute of Standards and Technology’s International Technical Working Group on IoT-Enabled Smart City Framework¹:

Two barriers currently exist to effective and powerful smart city solutions. First, many current smart city ICT deployments are based on custom systems that are not interoperable, portable across cities, extensible, or cost-effective. Second, a number of architectural design efforts are currently underway (e.g. ISO/IEC JTC1, IEC, IEEE, ITU and consortia) but have not yet converged, creating uncertainty among stakeholders. To reduce these barriers, NIST and its partners are convening an international public working group to compare and distill from these architectural efforts and city stakeholders a consensus framework of common architectural features to enable smart city solutions that meet the needs of modern communities.

In this special topic, a total of nine (9) manuscripts were received and after several rounds of reviews by subject matter experts, only two (2) manuscripts were accepted for publication and inclusion in this special topic.

¹ <https://pages.nist.gov/smartcitiesarchitecture/> (last accessed September 20, 2022)

✉ Kim-Kwang Raymond Choo
raymond.choo@fulbrightmail.org

Deepak Puthal
deepak.puthal@ieee.org

Charles Zhechao Liu
charles.liu@utsa.edu

Chonggang Wang
cgwang@ieee.org

As the title of the first article “An Examination of Gain- and Loss-Framed Messaging on Smart Home Security Training Programs” suggests, the authors (Miloslava Plachkinova and Philip Menard) used the lens of the gain- and loss-framed principles to design a security education training and awareness program, with the objective of identifying related cybersecurity and privacy needs for smart home users (e.g., those involving IoT devices and systems).

The second article entitled “Assessing Privacy and Security of Information Systems from Audit Data” authored by J. Christopher Westland examined internal control security breaches ‘in corporate information systems to determine whether U.S. Securities and Exchange Commission (SEC) data are information bearing with respect to breaches of security and privacy’. The findings revealed several auditing-related factors that can facilitate security breach prediction.

This special topic would not have been possible without the support of the authors who trusted us with their high quality submissions, the subject matter experts who selflessly devoted their time to review the submissions (e.g., Emmanuel Wusuhon Yanibo Ayaburi, Francis Kofih Andoh-Baidoo, Nicole Beebe, Benjamin Dowling, Paul Jen-Hwa Hu, Sang-Yong Tom Lee, Xiong Li, Juan Mao, Stefano Mariani, Philip Menard, Weizhi Meng, Rajhans Mishra, Daniel Edmund O’Leary, Federico Pigni, Morteza Safaei Safaei Pour, Bhupendra Singh, Vijayan Sugumaran, Jongtae Yu, Xiaolu Zhang), and the Editor-in-Chief (H.R. Rao) and the journal staff for their guidance and patience throughout the process.

Publisher’s Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

¹ University of Texas at San Antonio, San Antonio, TX, USA

² Khalifa University, Abu Dhabi, United Arab Emirates

³ Future Wireless North America, InterDigital, Inc., Conshohocken, PA, USA

Kim-Kwang Raymond Choo received the Ph.D. in Information Security in 2006 from Queensland University of Technology, Australia. He currently holds the Cloud Technology Endowed Professorship at The University of Texas at San Antonio. He is the founding co-Editor-in-Chief of ACM Distributed Ledger Technologies: Research & Practice, the founding Chair of IEEE Technology and Engineering Management Society's Technical Committee on Blockchain and Distributed Ledger Technologies, and is the recipient of the IEEE Systems, Man, and Cybernetics Technical Committee on Homeland Security Research and Innovation Award in 2022, and the 2019 IEEE Technical Committee on Scalable Computing Award for Excellence in Scalable Computing (Middle Career Researcher).

Deepak Puthal focuses on cybersecurity, Blockchain, and the Internet of Things research, and has won several competitive international awards in recognition of original research and innovations that led to advancements in the research specialization. He is currently an Assistant Professor at Khalifa University; and before this he was an Assistant Professor at Newcastle University, UK. He received his Ph.D. from the Faculty of Engineering and IT, University of Technology Sydney (UTS), Australia, and is currently an honorary fellow at UTS. He has been serving as a member of IEEE Computer Society STC ExCom, Chair of IEEE Bio-inspired Computing STC, and on the editorial board of IEEE Transactions on Big Data, IEEE Transactions on Computational Social Systems, IEEE Consumer Electronics Magazine, International Journal of Communication Systems, and Springer Nature Computer Science Journal.

Charles Zhechao Liu is a Professor of Information Systems at The University of Texas at San Antonio. He received his Ph.D. in Management Information Systems from the Katz Graduate School of Business, University of Pittsburgh. His research interests include the

economics of information systems, social media analytics, mobile apps, and electronic markets. Dr. Liu is an ICIS Doctoral Consortium Fellow (2006) and a recipient of the Net Institute Research Grant (2007), UTSA College of Business Dean's Distinguished Research Award, and the E. Lou Curry Teaching Excellence Award for Tenured Faculty. His research has been presented at ICIS, HICSS, AMCIS, WISE, and INFORMS conferences and published in leading information systems journals such as MIS Quarterly, Information Systems Research (ISR), Journal of Management Information Systems (JMIS), IEEE Internet of Things Journal, Communications of the AIS, and Communications of the ACM, among others.

Chonggang Wang received the Ph.D. degree from Beijing University of Posts and Telecommunications, Beijing, China, in 2002. He is a Principal Engineer with InterDigital, Inc., Wilmington, DE, USA. He has over 20 years of experience in the field of communications, networking, and computing, including research, development, and standardization of Wireless Systems, Internet of Things, Quantum Internet, and Internet protocols. He participates industry standardization activities with NextG Alliance, ETSI, IETF, 3GPP, oneM2M, and IEEE. He holds more than 100 granted U.S. patents. His current research interests include blockchain technologies and applications, 5G/6G systems, distributed and edge intelligence, and quantum Internet. Dr. Wang is the Founding Editor-in-Chief of the IEEE Internet of Things Journal. He is currently the Editor-in-Chief of IEEE Network, The Magazine of Global Internetworking. He is a Fellow of the IEEE for his contributions to IoT-enabling technologies.