Guest Editorial
Security, Reliability, Privacy, and Quality in Industrial Automation and Control

INDUSTRIAL Internet of Things (IoT) has enabled many new applications such as remote asset monitoring, predictive maintenance in factory, wearable and implanted biomedical sensors-based health and well-being monitoring, smart agriculture and viticulture monitoring, infrastructure monitoring, power system monitoring, energy system security, power grid quality, machine control, and many others. The IoT devices may be embedded, implanted, submerged, or monitor the activity remotely, and feed data to a control system using wired or a variety of wireless networks. A comprehensive infrastructure consisting of densely deployed sensors, actuators, data aggregators, and sophisticated decision and control systems can truly realize the concept of a *smart world*.

The industrial automation systems may operate by making the use of feedback control loop, cascade, feed-forward, and advanced process control. These systems operate in an open environment. Thus, exhibit a large surface area for cyber-attacks. The cyber infrastructure, in these industrial environments, is a network of IoT and information and communication technology devices, and attacks could be in the form of configuration changes, data corruption, manipulating state estimation matrices, SCADA system malfunctioning, and others. The attacks could be launched by organised criminals, hacktivists, or state nations. During the course of attack research, criminals compromise the privacy and steal information. Stolen information about the architecture of the industrial critical industrial automation and control systems plays important role in designing the attack strategy. Extensive investigation can result in identifying the vulnerabilities in the systems, then malware can be written to exploit these vulnerabilities to cause harm to physical systems.

This Special Issue (SI) was organized to provide a multi-aspect up-to-date reference for solutions that leverage techniques and insights from the domains of artificial intelligence, Internet of Things, edge computing, and big data, to address security, reliability, privacy, and quality challenges in industrial applications. We received a total of sixty-five original submissions from various institutions all over the world. After a rigorous review process, nineteen papers were accepted and are presented for inclusion in this SI of the IEEE Transactions on Industry Applications. Each paper is multidisciplinary and addresses differing challenges in industrial automation and control systems. The papers have been organized in the following categories to facilitate their reading.

- Security, privacy, and trust aspects of industrial automation and control systems including threat intelligence, collaborative trust, authentication, key agreement protocols, state estimation, and false data injection attacks (9 papers);
- Reliability issues in power control and management in cyber-physical systems and their communication networks (6 papers); and
- Power quality in power systems and electrical machines (4 papers).

ACKNOWLEDGMENT

As guest editors, we would like to convey our heartiest gratitude to all the authors who have submitted their knowledgeable contributions and to the highly qualified anonymous reviewers. We would also like to thank Dr. Thomas A. Nondahl, the Editor-in-Chief (EiC) of the IEEE Transactions on Industry Applications and Professor Massimo Mitolo, the Deputy EiC of the IEEE Transactions on Industry Applications, for giving us the opportunity to organize this SI and for all the encouragement, help, and support given throughout the process. Finally, a special thank you goes to the IEEE Industry Applications Society Publications Editorial Office, particularly, Dr. Peter Wung for sharing their experience and knowledge of the review process and for continuous suggestions and technical support. We also sincerely appreciate the effective and dedicated work of the associate editors, who made the management of the reviews possible: (i) Prof. Akshay Kumar Rathore, Concordia University, Canada; (ii) Prof. Sukumar Kamalasadan, University of North Carolina at Charlotte, USA; (iii) Prof. Kashem Muttaqi, University of Wollongong, Australia; and (iv) Prof. Anurag Srivastava, Washington State University, USA.

MUHAMMAD USMAN, *Guest Editor*
Faculty of Computing, Engineering and Science
University of South Wales
Cardiff, Newport CF37 1DL, UK

ALIREZA JOLFAEI, *Guest Editor*
Department of Computing
Macquarie University
Sydney, NSW 2109, Australia

IQBAL GONDAL, *Guest Editor*
School of Science, Engineering and Information Technology
Federation University Australia
Mt. Helen, 3355 VIC, Australia

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

Muhammad Usman received the M.S. degree in computer science from Pir Mehr Ali Shah Arid Agriculture University, Rawalpindi, Pakistan, with first class, and the Ph.D. degree from the School of Information and Communication Technology, Griffith University, Brisbane, Australia. He was a Postdoctoral Research Fellow in cyber security and machine learning with the University of Surrey, Guildford, U.K. He possesses over 17 years of experience during which he has held several academic and industrial positions in different parts of the globe, including Australia, Asia, and Europe. His current research interests include design and analysis of security, privacy, and trust techniques for complex cyber–physical and IoT-driven systems; security, trust, and privacy of cross-discipline domains; formal and statistical modeling; applied machine learning; and data analytics in several domains. He has authored over 40 research papers in international journals and conferences, including prestigious journals, such as the IEEE TRANSACTIONS ON CONSUMER ELECTRONICS, the IEEE TRANSACTIONS ON INDUSTRY APPLICATIONS, the IEEE TRANSACTIONS ON EMERGING TOPICS IN COMPUTATIONAL INTELLIGENCE, and a book. He has successfully supervised over 25 postgraduate research and undergraduate project students and supervising Ph.D. students. Dr. Usman has been a recipient of several research and travel grants. He has led and acted as a Guest Editor for special issues in several IEEE transactions. He has served in different leading capacities, such as a focal person, publication Chair, organizing committee member, and/or TCP member of several international IEEE conferences. He is a member of COVID 19 Outbreak Expert Database of UK Parliament. He is also a member of Computer Science Teachers Association, endorsed by Association for Computing Machinery, USA. He is a Juniper certified networking and security specialist. His research paper received a Best Paper Award in IEEE ComTech 2017.

Alireza Jolfaei received the Ph.D. degree in Applied Cryptography from Griffith University, Gold Coast, Australia. He is the Program Leader of Cyber Security at Macquarie University, Sydney, Australia. Before this appointment, he worked as an Assistant Professor at Federation University Australia and Temple University in Philadelphia, USA. His current research areas include Cyber and Cyber Physical Systems Security. He received the prestigious IEEE Australian council award for his research paper published in the IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY. He received a recognition diploma with a cash award from the IEEE Industrial Electronics Society for his publication at the 2019 IEEE IES International Conference on Industrial Technology. He is a founding chair of the Federation University IEEE Student Branch. He served as the Chairman of the Computational Intelligence Society in the IEEE Victoria Section and also as the Chairman of Professional and Career Activities for the IEEE Queensland Section. He has served as the guest associate editor of IEEE journals and transactions, including the IEEE SENSORS JOURNAL, IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, IEEE TRANSACTIONS ON INDUSTRY APPLICATIONS, IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, and IEEE TRANSACTIONS ON EMERGING TOPICS IN COMPUTATIONAL INTELLIGENCE. He has served over 10 conferences in leadership capacities including program co-Chair, track Chair, session Chair, and Technical Program Committee member, including IEEE TRUSTCOM and IEEE INFOCOM. He is a Distinguished Speaker of the ACM on the topic of Cyber Security and a Senior Member of the IEEE.

Iqbal Gondal is the Director of Internet Commerce Security Lab (ICSL), Federation University. ICSL conducts research in the application of advance analytics techniques for cybersecurity and provides innovative Cybersecurity solutions to the industry. He is also working as member of the University Governing Council & a member of the engineering advisory committee for Federation University, Non Exec Director of Oceania Cyber Security Centre and University engagement for Defence Science Institute. He has been responsible for establishing collaborative partnerships between Federation University and Australian Cyber Security Centre (ACSC) & Australian Federal Police (AFP). In the past, he was Director of ICT strategy for the faculty of IT in Monash. He has served in the capacity of Director of Postgraduate studies for six years, member of faculty board and member of Monash academic board. He has received commendation from Vice-Chancellor and Pro Vice-Chancellor (Learning and Teaching) for his excellent teaching in Monash. He has received significant industry funding to support research in ICSL in the area of Intelligent Malware analysis, threat intelligence, fraud detection, cyber-attack triage, malware webinject detection, phishing attack identification and mitigation and blockchain. He has published over 164-refereed conference and journal papers. To date he has successfully supervised 19 PhD students. He is Fellow of Institute of Engineers Australia and a Graduate member of Australian Institute of Company Directors. He is a member of the advisory board for International Journal for Distributed Sensors networks, Editor of Journal of Information Processing in Agriculture, China. His research interests are Cyber security, Remote condition monitoring, Wireless and sensor networks information processing.

Krishna Kant is currently a professor in the Computer and Information Science Department at Temple University in Philadelphia, PA where he directs the IUCRC center on Intelligent Storage. Earlier he was a research professor in the Center for Secure Information Systems at George Mason University. From 2008-2013 he served as a program director at NSF where he managed the computer systems research program and was instrumental in the development and running of NSF-wide sustainability initiative named science, engineering and education for sustainability (SEES). Prior to NSF, he served in industry for 18 years (at Intel, Bellcore, and Bell Labs) and 10 years in academia (at Penn State and Northwestern Univ.). He carries a combined 40 years of experience in academia, industry, and government. He received his Ph.D. degree in Mathematical Sciences from the University of Texas at Dallas in 1981. He has published in a wide variety of areas in computer science, authored a graduate textbook on performance modeling of computer systems. His research interests span a wide range including energy efficiency, robustness, and security in cyber and cyber-physical systems. He is a Fellow of the IEEE.