Guest Editorial: Computational Intelligence for Human-in-the-Loop Cyber Physical Systems

RECENT advances in computational intelligence, real-time computing and control, have given momentum to Human-in-the-Loop Cyber Physical Systems (HitLCPS) to enable game-changing communication and collaboration paradigms that operate in connection with humans' natural behaviour patterns. Despite the ongoing advancement of computational intelligence techniques for analyzing the interactions between the cognitive and cyber domains, there are growing concerns regarding the security, privacy, and safety of humans when they interact with smart cyber physical environments (IoT ecosystems). The large-scale integration of heterogeneous IoT devices to manage and control a wide variety of sensors and settings will hugely increase the attack surface and the scope for misconfigurations. These could lead to unsafe or conflicting behaviour of various devices and subsystems, which in turn, can place the human in unsafe and hazardous situations, both mentally and physically. It is still unclear how to design optimized collaborative systems between people and machines in a scalable manner, how to design triggers for pro-active engagement and disengagement, and how to handle the consequences of implied actions. For example, when the system misbehaves as a result of erroneous data, it is important to have real-time rules that can guarantee a fail-safe state for the HitLCPS. The verification of operations in a large HitLCPS can be very complex due to the evolving nature of human-in-the-loop networks both in terms of physical aspects and the operational environment. Therefore, understanding the semantics of HitLCPS and the context of control behaviour is critical to detect or entirely avoid incorrect configurations and build a proactive resilience and a reactive defence against evolving threats.

This special section of the IEEE Transactions on Emerging Topics in Computational Intelligence (TETCI) aims to capture the most recent advances of computational intelligence for HitLCPS from both theoretical and empirical perspectives. We received a total of nineteen papers from different research groups and a variety of perspectives for this special section. After a thorough evaluation of the papers by reviewers, the editorial board chose two high-quality research articles which cover a range of topics from the special section theme, as specified in the call. These papers, as will be explained in more detail in the following, are representative solutions that attempt to present novel applications of computational intelligence for HitLCPS and collectively reflect the advances, challenges, and directions for current and future research.

This special section opens with the paper entitled *Human-in-the-Loop-Aided Privacy-Preserving Scheme for Smart Healthcare* by Zhou *et al.*, which addresses the individuals' privacy concerns when medical data is being used for training and testing of predictive data mining models. The proposed method obfuscates the personal medical data by employing a combinatoric block design with special structural properties, so that the perturbed health indicators would be distinct from one another. In addition, the proposed Human-in-the-Loop machine learning model uses a randomized selection of health indicators for making medical diagnosis and this helps in reinforcing personal privacy. The authors compare various prediction models using an Euclidean distance of representative vectors and identify models that provide better privacy by revealing a smaller similarity. The authors also improve the accuracy of the predictions by optimising the data-sets used in smart healthcare. The performance analysis and case studies indicate the effectiveness of the proposed method.

Despite the recent research efforts in the protection of personal data in shared HitLCPS environments, the focus of privacy-preserving methods is mainly to handle single threshold problems for data sanitization. However, using a single threshold to verify the importance of attributes and applying a fixed threshold to different lengths of patterns may not be practical approaches for real applications where longer patterns could be identified in a database with a higher probability. Particularly, if a sensitive itemset has a larger size, it could be identified with a higher probability due to a higher specificity. To this end, a new concept of multiple support thresholds has been proposed by Wu *et al.* in the paper entitled *Security and Privacy in Shared HitLCPS using a GA-based Multiple-Threshold Sanitization Model*. The proposed technique is a modified version of a compact genetic algorithm that assigns a stricter threshold for each itemset. Furthermore, the algorithm design is based on a genetic-algorithm based model which minimizes three side effects, that is, the failure to hide a given sensitive pattern, inserting artificial knowledge into knowledge discovery in databases, and hiding non-sensitive patterns that occur with a high frequency. The experimental results show that the proposed method maintains a higher level of privacy protection compared to the traditional greedy privacy-preserving data mining approaches.

As guest editors, we would like to convey our heartiest gratitude to all the authors who submitted their contributions and to the highly qualified anonymous reviewers for dedicating their efforts in completing timely and constructive reviews. We would also like to thank Prof. Yew-Soon Ong, the Editor-in-Chief (EiC) of the IEEE TETCI, for giving us the opportunity to organize this special section and for all the encouragement, help, and

Digital Object Identifier 10.1109/TETCI.2021.3139998

support given throughout the process. We hope that this SI will serve as good reference for researches, scientists, engineers, and academics in the field of computational intelligence.

ALIREZA JOLFAEI, *Guest Editor*
Department of Computing
Macquarie University
Sydney, NSW 2113, Australia
alireza.jolfaei@mq.edu.au

MUHAMMAD USMAN, *Guest Editor*
Faculty of Computing, Engineering and Science
University of South Wales
CF37 1DL Newport, U.K.
muhammad.usman@southwales.ac.uk

MANUEL ROVERI, *Guest Editor*
Dipartimento di Elettronica e Informazione
Politecnico di Milano
Piazza Leonardo da Vinci, 32 I-20133 Milano, Italy
manuel.roveri@polimi.it

MICHAEL SHENG, *Guest Editor*
Department of Computing
Macquarie University
Sydney, NSW 2113, Australia
michael.sheng@mq.edu.au

MARIMUTHU PALANISWAMI, *Guest Editor*
Department of Electrical and Electronic Engineering
The University of Melbourne
Parkville, VIC 3010, Australia
palani@unimelb.edu.au

KRISHNA KANT, *Guest Editor*
Department of Computer and Information Sciences
Temple University
Philadelphia, PA 19122, USA
kkant@temple.edu

Alireza Jolfaei (Senior Member, IEEE) received the Ph.D. degree in applied cryptography from Griffith University, Gold Coast, QLD, Australia. He is the Program Leader of Master of IT in cyber security with Macquarie University, Sydney, NSW, Australia. His main research interests include cyber and cyber-physical systems security. He has participated in several projects involving different aspects of Cyber Security. On these topics, he has authored or coauthored more than 100 papers appeared in journals, conference proceedings, and books. Before Macquarie University, he has been a Faculty Member with Federation University Australia and Temple University, Philadelphia, PA, USA. He was the recipient of multiple awards for Academic Excellence, University Contribution, and Inclusion and Diversity Support. He was the recipient of the prestigious IEEE Australian Council Award for his research paper published in the IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY. He was 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 was a Guest Associate Editor for IEEE journals and transactions, including the IEEE IOT JOURNAL and IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS. He was a Program Co-Chair and a Technical Program Committee Member, for main conferences in cyber security, including IEEE TrustCom. He is a Distinguished Speaker of the Association for Computing Machinery (ACM) on the topic of Cyber Security.

Muhammad Usman received the M.S. degree (first-class) in computer science from Pir Mehr Ali Shah Arid Agriculture University, Rawalpindi, Pakistan, and the Ph.D. degree from the School of Information and Communication Technology, Griffith University, Brisbane, QLD, Australia. He is currently a Senior Lecturer of cyber security with the University of South Wales, U.K. He was a Postdoctoral Research Fellow of cyber security and machine learning with the University of Surrey, Guildford, U.K. He possesses more than 17 years of experience during which he held several academic and industrial positions in different parts of the globe, including Australia, Asia, and Europe. He has authored more than 50 research papers in international journals and conferences, including prestigious journals, such as the IEEE TRANSACTIONS ON CONSUMER ELECTRONICS, IEEE TRANSACTIONS ON INDUSTRY APPLICATIONS, IEEE TRANSACTIONS ON EMERGING TOPICS IN COMPUTATIONAL INTELLIGENCE, IEEE TRANSACTIONS ON RELIABILITY, and a book. 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 successfully supervised more than 50 postgraduate research and undergraduate project students and supervising several Ph.D. students. Dr. Usman was the recipient of several research and travel grants. He led and acted as the Guest Editor of special issues in several IEEE transactions. He was in different leading capacities, such as a focal person, steering committee chair, 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 U.K. Parliament. He is also a Member of Computer Science Teachers Association, USA. He is a Juniper certified networking and security specialist. His research paper was the recipient of the Best Paper Award in IEEE ComTech 2017.

Manuel Roveri (Senior Member, IEEE) received the Dr.Eng. degree in computer science engineering from the Politecnico di Milano, Milano, Italy, in June 2003, the M.S. degree in computer science from the University of Illinois at Chicago, Chicago, IL, USA, in December 2003, and the Ph.D. degree in computer engineering from Politecnico di Milano, in May 2007. He is currently an Associate Professor with the Dipartimento di Elettronica, Informazione e Bioingegneria of the Politecnico di Milano. He is a Visiting Researcher with Imperial College London, U.K. He has authored or coauthored more than 70 papers in international journals, book chapters, and conference proceedings. His current research interests include adaptation and learning in non-stationary environments and intelligence for embedded systems and cognitive fault diagnosis. He is an Associate Editor for the IEEE TRANSACTIONS ON NEURAL NETWORKS AND LEARNING SYSTEMS and was the Chair and a Member in many IEEE subcommittees. He is the Chair of the IEEE Computational Intelligence Society Student Activities Subcommittee and a Member of the IEEE Computational Intelligence Society Subcommittee on Webinars and of the IEEE Computational Intelligence Society Subcommittee on Research Grants. He is the Co-Organizer of the IEEE Symposium on Intelligent Embedded Systems in 2014 and organizer and co-organizer of workshops and special sessions at IEEE-sponsored conferences.

Michael Sheng (Member, IEEE) received the B.E. degree in information systems from Beihang University, Beijing, China, in 1993, and the Ph.D. degree in computer science from the University of New South Wales, Sydney, NSW, Australia, in 2006. He is currently a Full Professor and the Head of the Department of Computing, Macquarie University, Sydney, NSW, Australia. He has more than 20 years' research and development experience in the Internet of Things and related areas such as service-oriented computing, radio frequency identification, sensor networks, and Big Data analytics. He has authored or coauthored more than 400 publications in these areas and is one of the top-ranked authors in the Internet of Things research area according to AMiner and one of the most impactful authors in services computing according to Microsoft Academic. He was the recipient of a number of prestigious awards, including ARC Future Fellowship in 2014, Chris Wallace Award for Outstanding Research Contribution (2012), and Microsoft Research Fellowship (2003).

Marimuthu Palaniswami (Life Fellow, IEEE) received the Ph.D. degree from the University of Newcastle, Callaghan, NSW, Australia. He is an internationally recognized expert in Internet of Things (IoT), Sensor Networks, Automated Learning, and Computational Intelligence in large-scale complex systems. He is a named Distinguished Lecturer of the IEEE Computational Intelligence Society over the period 2013–2015. He is currently the Professor with the Department of Electrical and Electronic Engineering. He has a demonstrated track record in leading large research initiatives. In particular, he is the Founder and Director of the ARC Research Network on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), which has become an internationally recognized constellation of researchers, partner universities and industry organisations in the area of sensor networks. He is also a Co-Founder of the European Centred IoT forum. He has authored or coauthored more than 500 scientific papers including books and edited volumes in related topics in IEEE TRANSACTIONS ON IoT JOURNAL, *Cybernetics*, *Fuzzy Systems*, *Neural Networks*, *Power Systems*, *Communications Magazine*, *Computational Intelligence Magazine*, *Information and Forensic Society*, *Mobile Computing*, *Automatica Control*, *ACM Transactions on Sensor Networks Pattern Recognition*, *Computer Vision and Image Understanding (CVIU)*, *Automatica*, IEEE JOURNAL OF BIOMEDICAL AND HEALTH INFORMATICS (JBHI), *PLoS ONE*, *Frontiers in Physiology*, and Medical and Biological Engineering and Computing. His research has focused on translational aspects of his research and he has a fantastic track record in working with diverse industry sectors, from defence to environment, from telecom to biomedical and from health to local government domains. He was the General Chair of more than ten IEEE Sponsored International conferences with a focus on Sensor Networks and Internet of Things (IoT). His extensive publication and citation record is a clear testament to his technical leadership spanning Internet flow control, cloud computing, computational tools for analytics, image processing, sensor network architectures, sensor data fusion, autonomous tracking, sensor network security and control engineering.

Krishna Kant (Life Fellow, IEEE) received the Ph.D. degree in mathematical sciences from the University of Texas at Dallas, Richardson, TX, USA, in 1981. He is currently a Professor with the Computer and Information Science Department, Temple University in Philadelphia, PA, USA, where he directs the IUCRC Center on Intelligent Storage. Earlier, he was a Research Professor with the Center for Secure Information Systems, George Mason University, Fairfax, VA, USA. From 2008 to 2013, he was the Program Director with 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 was with industry for 18 years (at Intel, Bellcore, and Bell Labs) and ten years in academia (at Penn State and Northwestern University). He carries a combined 40 years of experience in academia, industry, and government. He has authored or coauthored 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.