Guest Editorial: Configuration Security for Industrial Automation and Control Systems

THE INDUSTRIAL automation and control systems include supervisory control and data acquisition systems, distributed control systems, and other control system configurations such as programmable logic controllers, which are typically used in industries such as electric, water and wastewater, oil and natural gas, transportation, chemical, pharmaceutical, food and beverage, and discrete manufacturing, examples of which are automotive, aerospace, and durable goods. These systems are highly interconnected and mutually dependent in complex ways, both physically and through information and communications technologies, and they support a diverse set of services for the management of critical infrastructure by making use of a wide variety of Internet of Things (IoT) devices for sensing and actuation.

The industrial automation and control services operate by defining a set of rules that specify appropriate control actions for each important set of events. The rules involve events based on the real-time data reported by the IoT devices. The actions initiated by the service controllers could occasionally lead to conflicts or undesirable, unsafe outcomes both due to inadvertent misconfiguration, attacks on the configuration state, and poorly understood dependencies. From consumer IoT devices developed with minimal built-in security, which are often co-opted by malware to launch large distributed denial of service attacks on Internet infrastructure, to remote attacks on industrial control devices; these newly connected, composed systems provide a vast attack surface. To this end, more secure configurations should be developed to address system vulnerabilities and minimize attack surfaces while maintaining expected functionality and performance.

This Special Section on "Configuration Security for Industrial Automation and Control Systems" of the IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS highlights the main research challenges and solutions for improving configuration security in the context of industrial automation and control systems by taking into consideration various challenges faced by industrial applications.

We received many papers from different research groups and a variety of perspectives for this section. After a thorough evaluation of the papers by reviewers, the editorial board chose eleven high-quality research articles which cover a wide 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 address configuration security in industrial automation and control systems and collectively reflect the advances, challenges, and directions for current and future research.

This Special Section opens with the article "A Novel Method to Prevent Misconfiguration of Industrial Automation and Control Systems" by Zhang *et al.*, which addresses the detection and correction of configuration errors in the industrial automation and control systems. The authors propose a streaming algorithm to keep a history of changes in configurations in a limited memory space. Once a new change in the configuration happens, it is cross-referenced and validated using similar historical changes, while overcoming the inherent unbounded-memory bottleneck. The author's experiments with real and synthetic datasets confirm the theoretical analyses and demonstrate the effectiveness of the proposed method in preventing misconfigurations.

Scalability and security-aware industrial control for real-time, cloud-based industrial applications is another important area addressed by Meng *et al.* in the article "Security-Aware Dynamic Scheduling for Real-Time Optimization in Cloud-Based Industrial Applications." A requirement for reliable operations in cloud-based industrial applications is to maintain a tight time latency and enable real-time processing. The authors propose a three-level security model for a two-tier heterogeneous cloud architecture consisting of the cloud and edge computing nodes. In particular, a security-aware scheduling method based on a distributed, particle swarm optimization is presented for resource allocation with security concerns. To deal with the dynamics of edge resources and mobile industrial applications, the authors propose a scheduling mechanism based on a dynamic workflow model for real-time optimization. The article shows that the proposed scheduling control policy achieves a good balance between security and scheduling performance.

In recent years, there has been a rise in the use of electric vehicles and the charging of such vehicles may impact the load profile of the electric grid, which could lead to a cascaded failures. In the article "Reinforcement Learning-Based Load Forecasting of Electric Vehicle Charging Station Using Q-Learning Technique," Dabbaghjamanesh *et al.* investigate the charging problem of electric vehicles. They propose a Q-learning based forecasting technique for the electric vehicle charging station loads. The authors show the effectiveness of their load demand prediction through extensive experimentation under three

Digital Object Identifier 10.1109/TII.2020.3036114

charging scenarios for plug-in hybrid electric vehicles, that is, smart, uncoordinated, and coordinated charging.

In the article "Secure Storage Auditing With Efficient Key Updates for Cognitive Industrial IoT Environment," Zheng *et al.* propose a secure storage auditing to support efficient key updates, which can also be used in cognitive industrial IoT environments. The proposed auditing method can be extended to support batch auditing that is suitable for multiple end devices to audit their data blocks simultaneously. The article shows that the proposed method can identify the location of data blocks about 40% faster than previous methods.

In the article "Lightweight Searchable Encryption Protocol for Industrial IoT," Zhang *et al.* propose an attribute-based encryption scheme for secure data sharing and searching for IoT applications. The article shows that the proposed encryption scheme is quite efficient and can be extended to multiauthority scenarios.

In the article "A Practical Model Based on Anomaly Detection for Protecting Medical IoT Control Services Against External Attacks," Fang *et al.* propose an anomaly detection system for the detection of unusual behavior in medical IoT systems, where adversaries can use device configuration vulnerabilities to hijack devices and control services. The proposed mechanism, which is based on a rough set theory and a fuzzy core vector machine, is able to analyze the data gathered from medical IoT devices, learn operation rules autodidactically, and alert management personnel when a device is in an abnormal operation state to ensure the safety and reliability of the control services. The authors showed the effectiveness of their anomaly detection system through extensive experimentation.

In the article "A Decision-Making Model for Securing IoT Devices in Smart Industries," Rathee *et al.* propose an intelligent decision-making model for the industrial IoT. The proposed model, which is based on the Technique for Order Preference by Similarity to the Ideal Solution, is able to examine the data collected from IoT devices in a secure, efficient, and structured way. The results obtained from the simulations and experiments reveal that compared to baseline methods, the proposed model can more effectively detect malicious nodes from where denial-of-service threats could occur.

In the article "Efficient and Lightweight Data Streaming Authentication in Industrial Control and Automation Systems," Xu *et al.* discuss the authentication issues in industrial control and automation systems. While verifiable data streaming methods can provide the authentication, such methods are computationally expensive and unsuitable for real-time use. To address this challenge, the paper proposes a chameleon authentication tree with prefixes, which is extended from a chameleon authentication tree and shows that such a scheme can satisfy both security and responsiveness requirements in data streaming authentication.

In the article "An Attribute-Based Access Control for Cloud Enabled Industrial Smart Vehicles," Gupta *et al.* discuss the vast attack surface available to adversaries through which they can remotely exploit and control the critical mechanics in the smart vehicles, including engine and brake systems. To address access control issues in the Internet of Vehicle ecosystem, the authors propose a formal attribute-based access control system based on the notion of groups. The proposed method takes individual privacy preferences together with system-wide policies in order to accept or reject notifications from different participating parties. The experimental analysis confirms the effectiveness of the model.

In the article "Fuzzy and Real Coded Chemical Reaction Optimization for Intrusion Detection in Industrial Big Data Environment," Ding *et al.* propose a cluster analysis approach with feature selection for detecting intrusions in a big data platform. To improve accuracy and convergence, the cluster analysis uses a real coded chemical reaction optimization, which initiates fuzzy c-mean over optimized cluster centers. To avoid the processing of a large number of features, the model uses a flexible mutual information feature selection approach.

In the article "Intelligent Internet-of-Things System for Smart Home Optimal Convection," Zielonka *et al.* propose an IoT convection installation for a small house. It uses a remote platform control system that adjusts the convection system based on an optimization model. The experimental results show an increased comfort level with smaller changes in the temperature inside the house.

Acknowledgment

The Guest Editors would like to thank all the authors who have submitted their contributions and to the highly qualified anonymous reviewers. The Guest Editors would also like to thank Prof. R. Luo, the Editor-in-Chief of the IEEE Transactions on Industrial Informatics for giving them the opportunity to organize this Special Section and for all the encouragement, help, and support given throughout the process. They are also grateful to the IEEE Transactions on Industrial Informatics staff for the professional support provided.

Alireza Jolfaei, *Guest Editor*
Department of Computing
Macquarie University
Sydney, NSW 2109, Australia

Mian Ahmad Jan, *Guest Editor*
Department of Computer Science
Abdul Wali Khan University
Mardan
Mardan 23200, Pakistan

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

Muhammad Usman, *Guest Editor*
School of Science, Engineering and
Information Technology
Federation University Australia
Ballarat, VIC 3355, Australia

Alireza Jolfaei (Senior Member, IEEE) received the Ph.D. degree in applied cryptography from Griffith University, Gold Coast, QLD, Australia, in 2016.

He is leading the Master of IT in cyber security program with the Department of Computing, Macquarie University, Sydney, NSW, Australia. Before this appointment, he was an Assistant Professor with the Federation University Australia, Ballarat, VIC, Australia and Temple University, Philadelphia, PA, USA. His research interests include cyber and cyber–physical systems security.

Dr. Jolfaei 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 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 was the Chairman of the Computational Intelligence Society in the IEEE Victoria Section and also the Chairman of Professional and Career Activities for the IEEE Queensland Section. He was the Guest Associate Editor for IEEE journals and transactions, including the IEEE TRANSACTIONS ON EMERGING TOPICS IN COMPUTATIONAL INTELLIGENCE and IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS. He has served, in more than ten conferences in leadership capacities including program Co-Chair, Track Chair, Session Chair, and Technical Program Committee member, including IEEE International Conference on Trust, Security and Privacy in Computing and Communications. He is a Distinguished Speaker of the ACM on the topic of Cyber Security.

Mian Ahmad Jan received the Ph.D. degree in computer systems from the University of Technology Sydney (UTS), Sydney, NSW, Australia, in 2016.

He is currently an Assistant Professor with the Department of Computer Science, Abdul Wali Khan University Mardan, Mardan, Pakistan. His research interests include energy-efficient and secured communication in wireless sensor networks and Internet of Things, and has been actively involved in machine learning, big data analytics, smart cities infrastructure, and vehicular ad hoc networks.

Dr. Jan was the recipient of the Best Researcher Award for the year 2014 at UTS. His research has been published in the IEEE TRANSACTIONS ON MOBILE COMPUTING, IEEE TRANSACTIONS ON CLOUD COMPUTING, IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, IEEE TRANSACTIONS ON NETWORK SCIENCE AND ENGINEERING, IEEE INTERNET OF THINGS JOURNAL, IEEE JOURNAL OF SELECTED AREAS OF COMMUNICATIONS and *ACM Computing Surveys* are few to mention. He had been the recipient of various prestigious scholarships during his Ph.D. studies. He was the recipient of the International Research Scholarship at the University of Technology, Sydney, Australia, and the Commonwealth Scientific Industrial Research Organization Scholarship. He has been the Guest Editor of numerous special issues in various prestigious journals such as the IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, *Elsevier Future Generation Computer Systems*, etc.

Krishna Kant (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, 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 a Program Director of 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. Prior to NSF, he was in the 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/coauthored in a wide variety of areas in computer science, authored a graduate textbook on performance modeling of computer systems. His research interests include energy efficiency, robustness, and security in cyber and cyber-physical systems.

Muhammad Usman received the Ph.D. degree in computer systems from the School of Electrical and Data Engineering, University of Technology Sydney (UTS), Sydney, NSW, Australia, in 2018.

He is currently a Lecturer with the School of Science, Engineering, and Information Technology, Federation University Australia, Ballarat, VIC, Australia. His research interests include secure and privacy-preserved communication in wireless sensor networks, wireless multimedia sensor networks, quality of service and experience in end-to-end communication, machine learning, video streaming, Internet of Things, and Internet of Multimedia Things, and has recently been active in using edge computing and machine learning technologies to provide services like data management, security and privacy, for smart city applications.

Dr. Usman had been the recipient of various prestigious scholarships and awards during his Ph.D. studies. He was the recipient of International Research Scholarship at the UTS. He was the recipient of the Best Researcher Award twice for the years 2016–2017 at the UTS. His research has been published in various well-reputed international journals like the IEEE TRANSACTIONS ON MULTIMEDIA, IEEE TRANSACTIONS ON CLOUD COMPUTING, IEEE TRANSACTIONS ON MOBILE COMPUTING, IEEE INTERNET OF THINGS JOURNAL, IEEE JOURNAL OF SELECTED AREAS OF COMMUNICATIONS, IEEE ACCESS, *ACM Computing Surveys*, *Elsevier Future Generations Computer Systems*, *Elsevier Information Sciences*, and *Elsevier Journal of Network and Computer Applications*. Also, he has authored/coauthored in high-ranked conferences such as the IEEE International Conference on Trust, Security and Privacy in Computing and Communications and IEEE PCS. He has been an organizing committee member of Springer/EAI 2nd Edition of International Conference on Future Intelligent Vehicular Technologies 2017, 11th International Conference on Computational Collective Intelligence 2019, and IEEE Global Communications Conference 2019.