IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Date of current version August 19, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3014416

EDITORIAL

IEEE ACCESS SPECIAL SECTION EDITORIAL: SECURITY AND TRUSTED COMPUTING FOR INDUSTRIAL INTERNET OF THINGS: RESEARCH CHALLENGES AND OPPORTUNITIES

Industrial IoT (IIoT) interconnects critical devices and sensors in critical infrastructure sectors with existing Internet of Things (IoT) devices and applications. Generally, IIoT deployment allows organizations and users to gain invaluable insights into industrial processes and achieve high-productivity gains while reducing cost. Their role will be increasingly important as we move toward Industry 5.0. Hence, it is also crucial to understand and address any security and privacy risks that may arise, including those discussed in the articles accepted in this Special Section.

A typical IIoT system has up to tens of thousands of interconnected devices and sensors, where information/data are exchanged in real-time. Analysis and mining of such (rich) data allow organizations and governments to gain situational awareness and invaluable insights into industrial processes, which in turn informs policy-making and strategy formulation. There are, however, underpinning security and privacy risks since these interconnected devices and sensors are now potential attack vectors that can be exploited (i.e., a significantly expanded attack base).

The objective of this Special Section is to report existing research efforts dedicated to strengthening the security foundations of IIoT systems, and the broader ecosystems where they are deployed (e.g., smart cities). Specifically, a total of 80 high-quality submissions were received and each manuscript was critically reviewed by at least two independent reviewers. The manuscripts were evaluated for their rigor and quality, as well as their relevance to the theme proposed in this Special Section. After a rigorous review process, 26 high-quality articles were accepted to be included in this Special Section (i.e., acceptance rate of 32.5%).

We will now briefly introduce the accepted articles.

In the article titled ''MIAEC: Missing data imputation based on the evidence chain,'' Xu *et al.* developed a missing value imputation algorithm based on evidence chain, namely, MIAEC, in order to facilitate security investigations in an IIoT environment.

In the article titled ''Malware threats and detection for industrial mobile-IoT networks,'' Sharmeen *et al.* focused on malware targeting devices deployed in an IIoT environment, where they analyzed approaches based on static, dynamic, and hybrid detection.

In the article titled ''A user-friendly privacy framework for users to achieve consents with nearby BLE devices,'' Cha *et al.* proposed a privacy preference expression framework for low-energy Bluetooth applications. Specifically, they defined specifications and guidelines for users and operators in order to achieve mutual agreement on privacy practices.

In the article titled ''Sensitivity analysis of an Attack-pattern discovery based trusted routing scheme for mobile Ad-Hoc networks in industrial IoT,'' Jhaveri *et al.* investigated a trusted routing scheme with pattern discovery (TRS-PD) for values of different parameters in IIoT scenarios.

In the article titled ''An effective high threating alarm mining method for cloud security management,'' Meng *et al.* proposed a self-adapting threat degree calculation method to qualify the threat degree of the alarms in an IIoT environment.

In the article titled ''Secrecy outage performance analysis for energy harvesting sensor networks with a jammer using relay selection strategy,'' Vo Nhan *et al*. attempted to enhance the secrecy of the IIoT systems. Specifically, they developed a near-optimal energy-harvesting time algorithm.

In the article titled ''A DDoS attack detection and mitigation with software-defined Internet of Things framework,'' Yin *et al.* proposed a general framework for software-defined IoT, which consists of a controller pool software-defined-IoT controllers, switches, and IoT devices.

In the article titled ''A reliable and lightweight trust computing mechanism for IoT edge devices based on multi-source feedback information fusion,'' Yuan *et al.* proposed a reliable lightweight trust mechanism for IoT edge devices, based on multi-source feedback information fusion.

Data encryption is a relatively mature research area but it is still of ongoing interest in IIoT, as evidenced by the article titled ''A novel efficient pairing-free CP-ABE based on elliptic curve cryptography for IoT.'' Specifically, Ding *et al.* proposed a pairing-free data access control scheme based on the ciphertext-policy attribute-based encryption (CP-ABE) using elliptic curve cryptography.

In the article titled "Secure APIT localization scheme against sybil attacks in distributed wireless sensor networks," Yuan *et al.* developed a lightweight Sybil-free algorithm, which is designed to mitigate Sybil attacks in approximate point in triangular test (APIT) algorithm.

In the article titled "An integrated method for anomaly detection from massive system logs," Liu *et al.* proposed an integrated method using K-prototype clustering and kNN classification algorithms to facilitate anomaly detection unentitled massive logs.

In the article titled "A new threat intelligence scheme for safeguarding industry 4.0 systems," Moustafa *et al.* addressed the challenges in Industry 4.0 and proposed a threat intelligence technique based on beta mixture-hidden Markov models (MHMMs) for discovering anomalous activities against both physical and network systems.

In the article titled "Oblivious transfer based on NTRUencrypt," Mi *et al.* investigated the fastest known 1-out-of-n oblivious transfer protocol and proposed a one-round postquantum secure OT_n^1 protocol using NTRUEncrypt.

In the article titled "Analyzing Android app privacy with GP-PP model," Kesswani *et al.* investigated app privacy issues over mobile devices by categorizing app permissions into privacy-invasive and generic permissions, and validating the classification using a Naïve Bayes classifier.

In the article titled "AES-128 based secure low power communication for LoRaWAN IoT environments," Tsai *et al.* developed a high-security, but low-power consumption communication solution using AES-128.

In the article titled "A novel collaborative task offloading scheme for secure and sustainable mobile cloudlet networks," Yang *et al.* proposed a collaborative task offloading method (CTOM) to mitigate DDoS attacks for secure mobile cloudlet networks.

In the article titled "Performance and security evaluations of identity- and pairing-based digital signature algorithms on Windows, Android, and Linux Platforms: Revisiting the algorithms of Cha and Cheon, Hess, Barreto, Libert, McCullagh and Quisquater, and Paterson and Schuldt," Zhong *et al.* examined the security performance trade-off for four existing digital signature algorithms.

Yang, *et al.* proposed a data integrity solution that can be implemented at the application layer of IIoT. The solution presented in the article titled "Compact hardware implementation of a SHA-3 core for wireless body sensor networks" is based on SHA3 for wireless body sensor networks.

In the article titled "Revocable identity-based encryption scheme under LWE assumption in the standard model," Zhang *et al.* proposed a revocable identity-based encryption scheme under learning with error (LWE) assumption from the lattice, which is shown to be secure against adaptive-ID attacks.

In the article titled "Behaviour and vulnerability assessment of drones-enabled Industrial Internet of Things (IIoT)," Sharma *et al.* proposed an N-layer hierarchical context-ware aspect-oriented Petri network model to evaluate the behavior of drones and assess the potential vulnerabilities under security policies.

In the article titled "Reliable resource provisioning using Bankers' Deadlock avoidance algorithm in MEC for Industrial IoT," Ugwuanyi *et al.* focused on a resource-constrained environment and proposed a deadlock-avoidance provisioning algorithm for IIoT. This allows one to ensure the reliability of network interactions in IIoT.

In the article titled "Data transfusion: Pairing wearable devices and its implication on security for Internet of Things," Lee *et al.* studied privacy issues relating to smartwatches and demonstrated how one can perform data extraction from such devices.

In the article titled "A secured data management scheme for smart societies in Industrial Internet of Things environment," Babar *et al.* proposed a centralized approach to achieve demand-side management over a smart-home case.

In the article titled "Privacy-aware data publishing and integration for collaborative service recommendation," Yan *et al.* improved the traditional, item-based collaborative filtering (ICF) approach by integrating the locality-sensitive hashing techniques.

In the article titled "A graph based security framework for securing Industrial IoT networks from vulnerability exploitations," George *et al.* proposed a graphical model to address the relations between vulnerability in the IIoT and a use-case was used to demonstrate the effectiveness of the proposed model.

In the article titled "A master attack methodology for an AI-based automated attack planner for smart cities," Falco *et al.* investigated the security and privacy issues in critical infrastructures, and proposed an example of automated attack generation method against cyberattacks targeting such critical infrastructures.

In this Special Section, the breadth of the topics reported demonstrates the ongoing interests of the community in ensuring the security of IIoT devices and systems. We hope that this Special Section will stimulate and encourage further research in security and related issues for IIoT.

In conclusion, we thank all researchers for submitting their work to this Special Section, and the reviewers for volunteering their time and expertise to critique and contribute to the submitted articles. We would also like to thank IEEE Access Editor-in-Chief and all staff members for their continuous support and guidance.

SHANCANG LI, *Guest Editor*
Department of Computer Science and Creative Technologies
University of the West of England
Bristol BS16 1QY, U.K.

KIM-KWANG RAYMOND CHOO, *Guest Editor*
Department of Information Systems and Cyber Security
The University of Texas at San Antonio
San Antonio, TX 78249, USA

ZHIYUAN TAN, *Guest Editor*
School of Computing, Edinburgh Napier University
Edinburgh EH10 5DT, U.K.

XIANGJIAN HE, *Guest Editor*
Department of School of Electrical and Data Engineering
University of Technology Sydney
Sydney, NSW 2007, Australia

JIANKUN HU, *Guest Editor*
School of Engineering and Information Technology
University of New South Wales
Canberra Campus, Campbell, ACT 2612, Australia

TAO QIN, *Guest Editor*
MOE Key Laboratory for Intelligent Networks
and Network Security
Xi'an Jiaotong University
Xi'an 710049, China

SHANCANG LI received the B.Sc. and M.Sc. degrees in mechanical engineering and the Ph.D. degree in computer science from Xi'an Jiaotong University, Xi'an, China, in 2001, 2004, and 2008, respectively.

He is currently a Senior Lecturer in security and digital forensics with the University of the West of England, Bristol, U.K. He has published over 80 technical journal articles and conference papers in reputable venues, and also four books and chapters. His current research interests include digital forensics for emerging technologies, cybersecurity, IoT security, data privacy-preserving, the Internet of Things, blockchain technology, and lightweight cryptography in resource-constrained devices. He is a member of the British Computer Society. He serves as the Chair/Co-Chain/Member of several workshops/special sessions and is in the technical program committees of different IEEE flagship conferences, including GLOBECOM and SMC. He is an editor for a number of journals.

KIM-KWANG RAYMOND CHOO (Senior Member, IEEE) received the Ph.D. degree in information security from the Queensland University of Technology, Australia, in 2006.

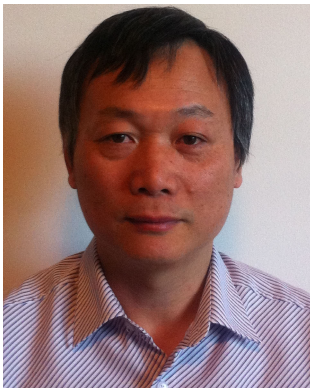
He currently holds the Cloud Technology Endowed Professorship at The University of Texas at San Antonio (UTSA). He is a Fellow of the Australian Computer Society and the Co-Chair of the IEEE Multimedia Communications Technical Committee's (MMTC) Digital Rights Management for Multimedia Interest Group. In 2015, he and his team won the Digital Forensics Research Challenge organized by Germany's University of Erlangen-Nuremberg. He was a recipient of the 2019 IEEE Technical Committee on Scalable Computing (TCSC) Award for Excellence in Scalable Computing (Middle Career Researcher), the 2018 UTSA College of Business Col. Jean Piccione and Lt. Col. Philip Piccione Endowed Research Award for Tenured Faculty, the IEEE TrustCom 2018 Best Paper Award, the ESORICS 2015 Best Research Paper Award, the 2014 Highly Commended Award by the Australia New Zealand Policing Advisory Agency, the Fulbright Scholarship in 2009, the 2008 Australia Day Achievement Medallion, and the British Computer Society's Wilkes Award in 2008.

ZHIYUAN TAN (Member, IEEE) is currently a Lecturer in cybersecurity at the School of Computing, Edinburgh Napier University, U.K.

He has been awarded The National Research Award 2017 by the Research Council of the Sultanate of Oman. He has played various chair roles in international workshops and conferences, such as the IEEE NOPE-19, SECSOC, SITN, EAI Future 5V, and EAI BD:TA 2018. He serves on the Editorial Board of the *International Journal of Computer Sciences and its Applications*. He has also recently served as a Special Issue Guest Editor for various international journals, including *Concurrency and Computation: Practice and Experience* (Wiley), *Computers and Electrical Engineering* (Elsevier), and the *International Journal of Distributed Sensor Networks* (SAGE).

XIANGJIAN HE (Senior Member, IEEE) is currently a Full Professor of computer science at the School of Electrical and Data Engineering, University of Technology Sydney, Australia.

He has been an IEEE Signal Processing Society Student Committee Member. He has been awarded the Internationally Registered Technology Specialist title by the International Technology Institute (ITI). He has played various chair roles in many international conferences, such as ACM MM, MMM, IEEE BigDataSE, IEEE TrustCom, IEEE CIT, IEEE AVSS, IEEE TrustCom, IEEE ICPR, and IEEE ICARCV. He has recently been a Guest Editor for various international journals, such as the *Journal of Computer Networks and Computer Applications* (Elsevier), *Future Generation Computer Systems* (Elsevier), and *Signal Processing* (Elsevier). He is currently an Advisor of *HKIE Transactions*.



JIANKUN HU is currently a Professor at the School of Engineering and IT, University of New South Wales (UNSW) Canberra (also named UNSW at the Australian Defence Force Academy (UNSW@ADFA), Canberra, Australia). He has many publications in top venues, including the IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE, the IEEE TRANSACTIONS ON COMPUTERS, the IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, the IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, *Pattern Recognition*, and the IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS. His research interests include cybersecurity covering intrusion detection, sensor key management, and biometrics authentication.

He has served in the Panel of Mathematics, Information and Computing Sciences (MIC), ARC ERA (The Excellence in Research for Australia) Evaluation Committee, in 2012. He serves as an Associate Editor for the IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY.

TAO QIN was a Visiting Scholar with the Department of Electrical and Computer Engineering, University of Massachusetts, Amherst, MA, USA. He is currently an Associate Professor with the Department of Computer Science and Technology, Xi'an Jiaotong University, Xi'an, China. In the past few years, he has a number of high-quality articles published in top venues, including the IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY. His research interests include traffic modelling and anomaly detection.