Guest Editorial: Security, Privacy, and Trust for Industrial Internet of Things

THE INDUSTRIAL Internet of Things (IIoT) is a sensory construction connected to the Internet that contains several types of machinery to supervise and control several and critical functions, such as the oil and gas platforms, power plants, smart cities, and healthcare technology. IIoT networks security and privacy is a serious issue, as the network nodes are used to be open to the Internet. Data encryption is the cornerstone of the IIoT safeguarding, however, there is always a tradeoff between security from one side and usability from the other side. Therefore, it is required to attain a balanced and secure system. Encryption should be offered at the far end of the upper layers to safeguard all subsequent layers [item 1) of the Appendix]. However, data encryption has its relative high expenses in terms of computational and storage requirements. Therefore, current security solutions are insufficient since they do not cover large heterogeneous networks with constrained and limited resources. Lightweight and fast encryption is needed to achieve the adapted safety for IIoT; though, lightweight encryption still needs to consider new formally verified methods over the modern cryptography. On the other hand, key management in terms of authenticated key agreement with key confirmation (AKC) protocols need to be present in a new customization for the IIoT context to achieve fast rekeying and nodes addition and revocation. Further research is required to develop and design appropriate IIoT security mechanisms, including novel and innovative solutions that are resilient to the current IIoT cyberattacks, for example, and not limited to, node capture, side-channel analysis, eavesdropping, man-in-the-middle, and distributed denial-of-service (DoS) attacks [item 2) of the Appendix]. An essential part of IIoT is the operational technologies (OT) that require a deep security consideration. Existent OT is susceptible to cyberattacks, and an enhancement of the Modbus, Profibus, Fieldbus, and Hart protocols with digital authentication should promise the corresponding confidentiality, integrity, availability, and dynamic group management for OT. If IT/OT merging is achieved properly, this will assure that IoT be fully maintained by both fields. This offers the best scenario for both of them, where robust industrial control systems reside on an open, integrated, and protected technology basis [item 3) of the Appendix]. IIoT context has specific necessities when it comes to trustworthiness, such as the following.

1) Short and limited-time response is essential for constant manufacturing processes. These industrial operations are supervised and organized over broad sensing and actuation systems to be interruptions free in a reliable and secure routine.
2) Reliability is one of the main challenges for IIoT as it is controlled in hard and threatening conditions of critical safety consequences.
3) Power dependence and battery lifetime, IIoT networks need to be operated over long periods before doing a battery replacement/charging. Power dependence presents a critical factor in achieving a reliable IIoT system.
4) Security is a severe and critical issue for all IoT systems; yet, industrial applications put more restrictions in achieving robust and reliable security solutions.
5) Scalability for IIoT networks needs a smooth nodes' addition and revocation to support numerous of new sensors and actuators [item 4) of the Appendix].

Moreover, industrial usages need more robust procedures due to their safety implications. All these limitations must be considered during the security protocols design process.

This Special Section on "Security, privacy, and trust for Industrial Internet of Things" of the IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS (TII) highlights the main research challenges in the industrial Internet of Things (IoT) security, privacy, and trust. The designated nine high-quality research articles cover a wide range of the special section theme, including innovative solutions and novel technologies.

IIoT networks produce huge amounts of valuable data in which it raises a great privacy concern for this critical information. The paper "A privacy-preserving outsourcing scheme for image local binary pattern in secure Industrial Internet of Things" by Xia *et al.* presented a new image-encryption technique by applying the following three encryption stages: block shuffling, intrablock shuffling, and pixel substitution. These encryption stages can safeguard the image content properly and also improve the direct calculation of local binary pattern (LBP) features on a single server, which makes a large security improvement. Besides, the obtained LBP features can be straightforwardly used on a cloud server for LBP-based applications.

The paper "Enhanced resilient state estimation using data-driven auxiliary models" by Anubi and Konstantinou presented an improved state estimation solution for cyberphysical systems based on IIoT networks that are vulnerable to false data injection attacks. The paper presented an integrated/combined data-driven model with the conventional compressive sensing regression issue. In the paper, it has been shown that the solution of the

Digital Object Identifier 10.1109/TII.2019.2953241

consequential constrained optimization problem retrieves the system true states. The proposed algorithm is assessed through a numerical simulation example of the IEEE 14-bus system mapped to the New York Independent System Operator grid data.

Software-defined networks (SDNs) technology is promising for IIoT networks. Sadly, SDN is exposed to distributed DoS (DDoS) attacks. Honeypots have shown great potentials in countermeasuring DDoS attacks. The paper "An SDN-enabled pseudo-honeypot strategy for distributed denial of service attacks in Industrial Internet of Things" by Du and Wang discovered a new attack that can recognize honeypots to overturn their security. Moreover, the paper showed the ideal strategies of intruders to find the best time for launching related attacks. To stop such kind of antihoneypot attacks, the authors presented a pseudohoneypot game strategy. The presented strategies provide SDN protection, as malicious attacks under the presented strategy can be effectively controlled. Completely, the presented strategies are evaluated on a testbed, and experimentally the results show that the presented strategy can efficiently resist the DDoS attacks.

One of the main issues in the critical industrial networks is the heterogeneous and real-time substation networks that are not compatible with the traditional cryptographic solutions in terms of SSL/TLS and PKI. The paper "An adaptive encryption-as-a-service architecture based on fog computing for real-time substation communications" by Zhang *et al.* proposed a new encryption architecture that offloads encryption to certain devices and issues certificate and make key management accessible over integrated web applications with the fog and cloud layers. In this article, a new algorithm, called MX-SORTS, has been presented in which it can manage the adoption of cryptographic schemes on different services to achieve a balance between the encryption lateness and real-time needs of substation networks.

The digital twin is a new industrial automation and control systems model, and it has gained interest due to abilities to perform advanced optimizations and simulations. However, digital twin security has a great security concern. The paper "A digital twin based industrial automation and control system security architecture" by Gehrmann and Gunnarsson examines the digital twin replication model and its related security architecture to facilitate data sharing and security-critical processes control. The authors identified design-driving security requirements for digital twin-based data sharing and control. The authors indicated that their presented state synchronization scheme meets the expected requirements of digital twin synchronization and gives efficient security components of the architecture. Besides, performance evaluations of a proof of concept for protected software upgrades using the proposed digital twin design have been done.

5G is a promising technology that needs solid and robust security protocols to prevent any potential security attack. Authenticated key agreement is an important feature for 5G security. Lately, quantum cryptography has received great attention due to its capability in reaching firm security solutions. The paper "A quantum-safe key hierarchy and dynamic security association for LTE/SAE in 5G scenario" by Arul *et al.* presented an authentication and key agreement (QKG-AKA) protocol for the dynamic security association using quantum cryptography. The authors implemented their new scheme in Long Term Evolution architecture without any major adjustments in the fundamental base system. Also, the presented scheme is examined against the quantum cryptanalysis. In the other sense, the related simulation showed good improvement over the related schemes.

In the same context, the physical-layer key agreement is employed to establish a shared session key between devices upon request. The characteristics of the wireless channel, which are time and location dependent, are involved in the key generation process in such schemes. Unfortunately, the physical-layer key agreement is vulnerable to active attacks. A physical-layer key agreement with user introduced randomness (PHY-UIR) is a potential solution against active attacks. The paper "A session hijacking attack against a device-assisted physical-layer key agreement" by Hu *et al.* investigated the risk of having a session hijacking attack on PHY-UIR that can help the intruder to control the established shared key. The proposed attack influences the key agreement process over a man-in-the-middle attack to force the communication's partners to run the PHY-UIR protocol with the attacker. The paper presented some experiments to indicate the impact of the proposed attack. To circumvent these weaknesses, a PHY-UIR+ protocol has been proposed, where devices instantaneously exchange information about the session keys to help them to detect the hijacking attack accordingly.

In the same perspective, the physical layer (PHY) key generation is one of the promising techniques that can be involved to protect the IoT context. Asymmetric keys generation is one of the main challenges of the PHY key generation schemes. To address this issue, the paper "A hybrid key generation and a verification scheme" by Khosroshahi *et al.* introduced a key verification scheme which is based on information reconciliation. The authors presented a hybrid key generation and key verification scheme, where the revealed information during the key verification process is useless for the intruder, in which the verified keys are equal. On the other hand, the numerical results and software-defined radio-based tests show that the proposed verification scheme attains the Internet of Industrial Things (IIoT) systems' needs.

Blockchain technology has been progressively deployed for decentralizing cloud-based IoT systems to overcome the restrictions of the centralized system. The current centralization techniques need to have external clients depending on a relay node that can communicate with the full nodes in the blockchain. Attacking such relay nodes may result in an entire security breach for the entire network. The paper "Decentralizing IoT management systems using blockchain for censorship resistance" by He *et al.* presented a new technique that includes a "diffusion" function to send all messages from sensors to all network nodes and an improved consensus protocol to detect data losses, duplicate processing outcome, and enable opportunistic outcome delivery. The authors of this paper showed an improved performance in terms of practicability and efficiency in achieving censorship resistance.

Acknowledgment

The Guest Editors would like to express their deep gratitude to all the authors who submitted their works as well as to the numerous highly qualified reviewers who provided thorough reviews and comprehensive comments, thus significantly contributing to the high-quality level of the papers that were finally accepted for publication. We would like to thank current Editor-in-Chief of the TII, Prof. R. Luo, for his support and guidance in preparing and finalizing this Special Section. We are also grateful to the TII staff for the professional support provided.

M. Gidlund, *Guest Editor*
Mid Sweden University
851 70 Sundsvall, Sweden

G. P. Hancke, *Guest Editor*
City University of Hong Kong
Hong Kong

M. H. Eldefrawy, *Guest Editor*
School of Information Technology
Halmstad University
301 18 Halmstad, Sweden

J. Åkerberg, *Guest Editor*
ABB Corporate Research
722 26 Västerås, Sweden

Appendix
Related Work

1) M. Gidlund, S. Han, E. Sisinni, A. Saifullah, and U. Jennehag, "Guest editorial from industrial wireless sensor networks to industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 14, no. 5. pp. 2194–2198, May 2018.
2) S. Ahmad-Reza, C. Wachsmann, and M. Waidner, "Security and privacy challenges in industrial internet of things," *Proc. 52nd ACM/EDAC/IEEE Des. Autom. Conf.*, 2015.
3) H. David, G. Salgueiro, P. Grossetete, R. Barton, and J. Henry, "IoT fundamentals: Networking technologies, protocols, and use cases for the Internet of Things," Cisco Press, Indianapolis, IN, USA, pp. 256–261, 2017.
4) M. H. Eldefrawy, N. Pereira, and M. Gidlund, "Key distribution protocol for industrial Internet of Things without implicit certificates," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 906–917, Feb. 2019.

Mikael Gidlund (M'98–SM'16) received the M.Sc. and Ph.D. degrees in electrical engineering from Mid Sweden University, Sundsvall, Sweden, in 2000 and 2005, respectively.

Since 2014, he has been a Full Professor of Computer Engineering with Mid Sweden University. In 2005, he was a Visiting Researcher with the Department of Informatics, University of Bergen, Bergen, Norway. From 2006 to 2007, he was a Research Engineer and a Project Manager, responsible for wireless broadband communication, with Acreo AB, Kista, Sweden. From 2007 to 2008, he was a Senior Specialist and a Project Manager, with responsibility for next-generation IP-based radio solutions, with Nera Networks AS, Bergen, Norway. From 2008 to 2013, he was a Senior Principal Scientist and a Global Research Area Coordinator of Wireless Technologies with ABB Corporate Research with main responsibility to drive technology and strategy plans, standardization, and innovation in the wireless automation area. He has pioneered the area of industrial wireless sensor network and holds more than 20 patents (granted and pending applications) in the area of wireless communications, and has authored or coauthored nearly 200 scientific publications in refereed fora. His research interest are wireless communication and networks, industrial Internet of Things, access protocols, and security.

Dr. Gidlund is an Associate Editor for the IEEE Transactions on Industrial Informatics and *Journal of Information Processing Systems*. He is currently the Chair for IEEE IES Technical Committee on Cloud and Wireless Systems for Industrial Applications. He won the Best Paper Award at the IEEE International Conference on Industrial IT in 2014.

Gerhard P. Hancke received B.Eng. and M.Eng. degrees in computer engineering from the University of Pretoria, Pretoria, South Africa, in 2002 and 2003, respectively, the Ph.D. degree in computer science from the University of Cambridge, Cambridge, U.K., in 2009, and an LLB degree from the University of South Africa, Pretoria, South Africa, in 2014.

In 2013, he joined City University of Hong Kong as a faculty member, where he is currently an Associate Professor. Prior to this, he was a Researcher with the Smart Card and IoT Security Centre and as a Teaching Fellow with the Department of Information Security, both located at Royal Holloway, University of London, Egham, U.K. His research interests include system security, reliable communication, and distributed sensing for the industrial Internet of Things.

Mohamed H. Eldefrawy received the Ph.D. degree in electrical engineering from Alexandria University, Alexandria, Egypt, in 2014.

He is currently an Assistant Professor with the School of Information Technology, Halmstad University, Halmstad, Sweden. Before joining Halmstad University, he was a Postdoctoral Researcher with the Department of Information Systems and Technology, Mid Sweden University, Sundsvall, Sweden. Earlier, he was a Senior Researcher with the Center of Excellence in Information Assurance, King Saud University, Riyadh, Saudi Arabia. He has more than 20 research articles in highly reputed journals and conferences. He is currently an Inventor of two US/PCT patents in cybersecurity. One of his inventions got a Bronze Medal at the 41st International Exhibition of Inventions in Geneva, Switzerland, in April 2013. Also, he is a Technical Reviewer for many international journals and conferences. His research interests include network security, digital authentication, and information assurance.

Johan Åkerberg received the M.Sc. and Ph.D. degrees in computer science and engineering from Mälardalen University, Västerås, Sweden, in 2007 and 2011, respectively.

He is currently a Principal Scientist and a Global Research Area Coordinator for embedded systems and electronics with ABB Corporate Research, Västerås, Sweden. He is mainly working with communication for embedded real-time systems in industrial automation and is frequently invited to give talks to governmental bodies, international universities, and automation fairs. He has more than 20 years experience with ABB in various positions, such as an R&D Project Manager, Industrial Communication Specialist, and Product Manager. He holds more than 10 patents (granted and pending applications) in the area of wired/wireless industrial automation, and is an author or coauthor of numerous scientific publications in refereed conferences and journals. He is also an active IEEE Senior Member organizing special sessions, holding tutorials and acting as a TCP member in various distinguished IES conferences.