Guest Editorial: Security and Privacy in Industry 4.0

INDUSTRIES, governments, and scientific communities are increasingly drawing special attention to competitive advantages that Industry 4.0 can bring to business sustainability and economy of a country. The tendency to couple information technologies (ITs) with the existing operational technologies (OTs) adds new opportunities to improve and optimize operational processes, products, and services in which multiple stakeholders (e.g., end-users) can interact with the new industrial ecosystems to speed up and customize processes. In this sense, Industry 4.0 constitutes a relevant investment source composed of a complex technological showcase in which multiple connections and accesses can arise, seriously impacting on the good performance of the different production and distribution chains associated with smart factories and manufacturing, smart grid systems, smart transportation, or smart health environments.

This way of connecting entities with the "smart world" and the interconnection of different Industry 4.0 domains based on the new paradigms and heterogeneous technologies such as cyber–physical systems, industrial Internet of Things (IIoT), or edge computing infrastructures (cloud/fog computing systems), certainly, opens the door to coexistence problems and novel exploitations. Diverse vulnerabilities and risks may significantly grow according to the new adaptations and the participation of stakeholders, generating a need to further research protection issues required to safeguard the operational processes and ensure a secure, resilient, and dependable cohesion between IT and OT systems, including physical entities.

The aim of this special section is, therefore, is to bring together researchers from diverse interdisciplinary areas of computing and security to cover, from a holistic point of view, the topics related to secure coupling of the new ITs with operational networks, without discarding aspects on privacy. Indeed, Hao *et al.* [1] present a novel privacy-enhanced federated learning (PEFL) scheme for industrial artificial intelligence. This scheme adds noniterative properties in each secure aggregation so as to prevent privacy leakage from the local gradients as well as the shared parameters even when an adversary colludes with multiple entities. The article includes experiments with real-world data, and performs a detailed security analysis to show that PEFL provides postquantum security and guarantees aggregator oblivious security.

One of the greatest issues within Industry 4.0 is precisely how to manage massive redundant data without impacting the integrity of the systems, privacy of user data, and added costs. Liang *et al* [2]. address this aspect providing a secure data storage and recovery scheme making use of blockchain and a local regenerative code for local repairs. This approach together with both technologies offers multiple benefits for real-time monitoring and management of storage systems since the approach adds support for dynamic storage, fast repair, and update of distributed data in the data storage system of industrial nodes.

Continuing with blockchain, Huang *et al.* [3] apply the Ethereum technology together with mobile crowd sensing (MCS) to foster mobility and scalability in Industry 4.0 domains, resulting in the blockchain-based MCS system. The approach verifies the sensory data and activates a dynamic reward ranking incentive mechanism through miners, and detects anomalies by integrating a sensory data quality detection scheme. Li *et al.* [4] also explore the benefits of Ethereum for energy trading in IIoT so as to satisfy energy demands and optimize efficiency in Industry 4.0. Through this technology, the authors propose FeneChain to supervise and manage the energy trading process by applying anonymous authentication and a timed commitments-based mechanism to guarantee the verifiable fairness during energy trading.

Rubio *et al.* [5] study the role of the opinion dynamics in IIoT domains and explore its deployment over different IIoT architectures to detect advanced persistent threats, specifying a common framework for data acquisition considering the computational constraints of the IIoT devices. Through experiments and a comprehensive analysis about the feasibility of the opinion dynamics, the authors show its utility when it is applied for IIoT infrastructures. To protect the IIoT communications, Yang *et al.* [6] propose a lightweight authenticated key agreement protocol to establish a session key between devices combined with perfect forward secrecy techniques. The approach is fast thanks to a new dynamic authentication credential framework that does not require public-key cryptographic primitives.

As for use cases and associated with critical environments, Ma *et al.* [7] propose a novel biometrics-based remote authentication scheme on the operator's portable devices for smart grid, denoted as Eye-movement and Iris recognition based Authentication (EmIr-Auth). EmIr-Auth applies the recorded eye-movement trajectory and randomly selected iris image to authenticate human operators. For the experiments, the Burrows–Abadi–Needham approach is applied to demonstrate the authentication capacity of the approach (EmIr-Auth) and how it is able to cope with several threats.

Similarly, Ding *et al.* [8] provide an identity-based metering data aggregation scheme for smart grid environments, supporting batch verification by collector and electricity service

Digital Object Identifier 10.1109/TII.2020.2990878

provider. Here, collectors are responsible for collecting and aggregating the end users' metering data in their respective administrative premises without revealing the metering value. Last but not least, Kavallieratos *et al.* [9] analyze the maritime architectural framework reference architecture to detail the environment of the cyber-enabled ship, and identify the cyber-security requirements taking into account the Secure Tropos methodology.

We would express our thanks to all the authors who responded positively to this Special Section, showing also our thanks to the experts in the area who voluntarily acted as excellent reviewers on a very tight schedule. Finally, we appreciate the support of the Editor-in-Chief of the IEEE Transactions on Industrial Informatics Journal, Prof. R. C. Luo for supporting us during the publication process without forgetting the editorial staff.

Cristina Alcaraz, *Guest Editor*
Computer Science Department
University of Malaga
29071 Malaga, Spain

Yan Zhang, *Guest Editor*
Department of Informatics
University of Oslo
0315 Oslo, Norway

Alvaro Cardenas, *Guest Editor*
Computer Science and Engineering Department
University of California, Santa Cruz
Santa Cruz, CA 95064 USA

Liehuang Zhu, *Guest Editor*
School of Computer Technology and Science
Beijing Institute of Technology
Beijing 100811, China

Appendix
Related Work

1) M. Hao, H. Li, X. Luo, G. Xu, H. Yang, and S. Liu, "Efficient and privacy-enhanced federated learning for industrial artificial intelligence," *IEEE Trans. Ind. Informat.*, vol. 16, no. 10, pp. 6532–6542, Oct. 2020.
2) W. Liang, Y. Fan, K.-C. Li, D. Zhang, and J.-L. Gaudiot, "Secure data storage and recovery in industrial blockchain network environments," *IEEE Trans. Ind. Informat.*, vol. 16, no. 10, pp. 6543–6552, Oct. 2020.
3) J. Huang, L. Kong, H.-N. Dai, W. Ding, L. Cheng, G. Chen, X. Jin, and P. Zeng, "Blockchain based mobile crowd sensing in industrial systems," *IEEE Trans. Ind. Informat.*, vol. 16, no. 10, pp. 6553–6563, Oct. 2020.
4) M. Li, D. Hu, C. Lal, M. Conti, Z. Zhang, "Blockchain-enabled secure energy trading with verifiable fairness in industrial internet of things," *IEEE Trans. Ind. Informat.*, vol. 16, no. 10, pp. 6564–6574, Oct. 2020.
5) J. E. Rubio, R. Roman, and J. Lopez, "Integration of a threat traceability solution in the Industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 16, no. 10, pp. 6575–6583, Oct. 2020.
6) Z. Yang, J. He, Y. Tian, and J. Zhou, "Faster authenticated key agreement with perfect forward secrecy for Industrial Internet-of-Things," *IEEE Trans. Ind. Informat.*, vol. 16, no. 10, pp. 6584–6596, Oct. 2020.
7) Z. Ma, Y. Yang, X. Liu, Y. Liu, S. Ma, K. Ren, and C. Yao, "EmIr-Auth: Eye-movement and iris-based portable remote authentication for smart grid," *IEEE Trans. Ind. Informat.*, vol. 16, no. 10, pp. 6597–6606, Oct. 2020.
8) Y. Ding, B. Wang, Y. Wang, K. Zhang, and H. Wang, "Secure metering data aggregation with batch verification in industrial smart grid," *IEEE Trans. Ind. Informat.*, vol. 16, no. 10, pp. 6607–6616, Oct. 2020.
9) G. Kavallieratos, V. Diamantopoulou, and S. K. Katsikas, "Shipping 4.0: Security requirements for the cyber-enabled ship," *IEEE Trans. Ind. Informat.*, vol. 16, no. 10, pp. 6617–6626, Oct. 2020.