Editorial: Industrial Internet: Security, Architectures, and Technologies

INDUSTRIAL Internet is applicable across a broad industrial spectrum, including manufacturing, aviation, road and rail transport, power, oil, and gas, healthcare, smart cities, and buildings. Some of the major impacts of the industrial Internet include the development of new and innovative services and products, which, in turn, also has economic benefits. Through predictive maintenance and safety improvements, there will be greater cost and time savings for industrial applications. Better connectivity also ensures more efficient operations, risk reduction, and scalability. The two major concerns with implementing the industrial Internet are interoperability and security. Many devices with different protocols and architectures need to be able to communicate with each other. The proliferation of connected devices also means ensuring that data are transferred securely, without compromising its integrity.

The purpose of this special issue is to bring together research studies proposing novel techniques, algorithms, models, and solutions to address challenges, such as interoperability, security, and privacy associated with industrial Internet, blockchain, and cyber-physical systems.

We accepted seven articles after two review rounds consisting of three reviews from experts in the areas. The special issue contains seven articles organized in the following categories.

1) Secure searching for edge-cloud assisted industrial Internet of Things (IoT) devices.
2) Privacy protection framework for mobile crowdsensing in Industrial Internet of Things (IIoT).
3) Content privacy for autonomous vehicles in cyber-physical system (CPS).
4) Delegated Proof of Stake (DPoS) consensus mechanism in blockchain.
5) Balancing privacy and accountability for industrial mortgage management.
6) Performance and security in wireless blockchain networks.
7) False data injection attacks in networked control systems.

The first part of this special issue is devoted to "Lightweighted Secure Searching Over Public-Key Ciphertexts for Edge-Cloud Assisted Industrial IoT Devices," which exploits the capability of the edge-cloud architecture and proposes a lightweight-designed scheme called edge-aided searchable public-key encryption (ESPE). This allows IIoT devices to delegate their costly cryptographic operations to the nearby edge for fast computing, saving energy, and guarantees that all outsourced ciphertexts are semantically secure. Consequently, Wang *et al.* show that ESPE accelerates the ciphertext corresponding procedures on edges and saves over 70.

The next part of the special issue is based on a framework for IIoT, which consists of a personalized privacy measurement algorithm, a rational uploading strategy and a privacy-preserving data aggregation scheme. Xiong *et al.* propose a personalized privacy protection (PERIO) framework based on game theory and data encryption. First, a personalized privacy measurement algorithm is designed to calculate users' privacy level, which is then combined with game theory for construction of a rational uploading strategy. Furthermore, the authors propose a privacy-preserving data aggregation scheme to ensure data confidentiality, integrity, and real-timeness. This framework satisfies the requirements of Quality of Crowdsensing Services (QoCS), improves the privacy level, and maximizes users' utility. The authors show that PERIO is effective and makes a reasonable balance between retaining high QoCS and privacy.

Another article in this part, "Achieving Personalized k-Anonymity Based Content Privacy for Autonomous Vehicles in CPS," presents a novel privacy notion of client-based personalized *k*-anonymity (CPkA). It allows a user to specify the minimum anonymity level of each query content, and different from the existing works, CPkA is carried out on the client side, such as a module in autonomous vehicles. To measure the performance of CPkA, Wang *et al.* present a privacy metric as the expected error of the optimal inference and a utility metric denoted as the expect query cost (EQC) in order to achieve the optimal CPkA in term of privacy and utility. An approach consisting of two modules to establish mechanisms, which achieve the optimal CPkA, is also presented. The first module is to build in-group mechanisms for achieving the optimal privacy within each content group. The second module includes linear programming based methods to compute the optimal grouping strategies. The in-group mechanisms and the grouping strategies are combined to establish optimal CPkA mechanisms, which achieve the optimal privacy or the optimal utility.

The fourth part of the issue presents a new improved DPoS consensus mechanism in blockchain based on vague sets voting. It makes each vote agent node more according with the human voting to solve the problem. This improves the security and fairness of blockchain and reduces the probability that malicious nodes will be selected as agent nodes. Xu *et al.* proved that

Digital Object Identifier 10.1109/TII.2020.2966589

the maximum probability of nodes after the vote of the fuzzy membership degree is 0.5. The feasibility and effectiveness of the improved consensus mechanism is also verified by examples.

The fifth part of the issue deals with “Balancing Privacy and Accountability for Industrial Mortgage Management.” This work construct a blockchain-based accountable and privacy-preserving industrial mortgage scheme (BAPIM). The proposed not only protects the privacy of honest borrowers, but also helps financial companies or financial institutions to detect the misbehavior of borrowers to achieve the borrower identity privacy and accountability at the same time. Borrower identity is concealed on the blockchain by anonymous identity credential, whereas financial institutions can still uncover the identity of a misbehaving borrower if he pledges the same asset for multiple mortgages. Xue *et al.* demonstrate that BAPIM achieves the desirable security properties and has high computational efficiency to be suitable for the industrial mortgage management.

The sixth part of the special issue discusses “How Does CSMA/CA Affect the Performance and Security in Wireless Blockchain Networks.” Cao *et al.* investigate whether the widely used media access control (MAC) mechanism, carrier sense multiple access/collision avoidance (CSMA/CA) is suitable for wireless blockchain networks or not. Based on tangle, the transaction per second and transaction loss probability of a blockchain system is analyzed by considering the impact of queuing and transmission decay caused by CSMA/CA. A stochastic model is also proposed for analysis of the security issue taking into account the malicious double-spending attack. Simulation results show that the performance would be limited by the traditional CSMA/CA protocol. Meanwhile, the authors demonstrate the probability of launching a successful double-spending attack would be affected by CSMA/CA as well.

The last part of the special issue presents “Detection and Mitigation of False Data Injection Attacks in Networked Control Systems.” Sargolzaei *et al.* propose a control scheme that enables a networked control systems to detect and mitigate false data injection attacks, and at the same time, compensate for measurement noise and process noise. The developed anomaly detection algorithm consists of a Kalman filter based observer and a neural network observer, which can detect and compensate for the adverse effects of uncertainties in the system and false data injection attacks in real time. In comparison with a traditional fault detection method, the developed anomaly detection algorithm can detect uncertainties, and false data injection attacks faster and more accurately. The Guest Editors would like to thank the authors, the Journal Editor-in-Chief Prof. R. Luo and Mrs. L. Lee EIC Secretary Office, and the reviewers. The time and efforts they have devoted to provide detailed comments and advice have contributed to significantly improving the quality of the accepted articles.

Q. Yang, *Guest Editor*
Department of Computer Science
and Engineering
University of North Texas
Denton, TX 76203 USA

R. Malekian, *Guest Editor*
Department of Computer Science
and Media Technology
Malmö University
21119 Malmö, Sweden

C. Wang, *Guest Editor*
InterDigital Communications
Wilmington, DE 19809 USA

D. Rawat, *Guest Editor*
Department of Electrical Engineering
and Computer Science
Howard University
Washington, DC 20059 USA