Guest Editorial: Privacy-Preserving Federated Machine Learning Solutions for Enhanced Security of Critical Energy Infrastructures

I. Introduction

CRITICAL energy infrastructure (CEI) is specific engineering information about proposed or existing critical infrastructure. Modern critical infrastructures are increasingly turning into distributed, complex cyber-physical systems that need proactive protection and fast restoration to mitigate physical or cyber incidents or attacks. Most importantly, combined cyber-physical attacks are much more challenging and are expected to become the most intrusive attack. This is particularly true for the CEIs. During 2015, the Industrial Control Systems Cyber Emergency Response Team in the Unites States responded to more than 245 incidents; the energy sector tops the list with 32% incidents. Considering the importance of energy in our daily lives and its influence on other critical infrastructures, CEI requires significant attention comparatively. For example, the wind-turbine system is considered one of the most complex cyber-physical infrastructures, causing huge cascading effects to other CEIs, such as electrical power and energy systems and transportation, healthcare sector, communications, industry, and finance. Wind turbines are mainly composed of condition monitoring and operational data (i.e., supervisory command and data acquisition), including air temperature, air pressure, voltage, and power with multiple parameters and periodic characteristics.

Utilize less expensive and scalable IoT that enables data monitoring in near real-time conditions. However, the main limitations regarding wind-turbine data monitoring still pertain. An innovative approach is to adopt privacy-preserving federated machine learning solutions in order to detect any possible anomalies in such infrastructures. Instead of centralizing the wind-turbine data into a common server, federated machine learning allows the data to remain on-premise in the infrastructure. This enables the responsible authorities to consider the advantages of machine learning and simultaneously protect their privacy. Federated learning (FL) can train a model using data stored at multiple wind-turbine stations without the data leaving the station's premises.

The guest editor team (Imran Razzak, Muhammad Khurram Khan, and Guandong Xu) hope that the articles in the Special Issue can contribute to the body of knowledge on enhancing the security of critical infrastructure in developing the machine learning solutions and benefiting our future fighting against cyber threats in critical infrastructure. Based on the reviewers' feedback and editors' evaluations, seven articles were selected from more than 46 submissions in this particular section. The seven articles, which cover broad topics, are introduced briefly as follows.

Access control is the key security concern that needs to be ensured for any IIoT infrastructure. Recently, various access control solutions have been presented for IoTs. However, only few of these are applicable for IIoTs. Kumar *et al.* [A1] presented a blockchain-based framework that uses role-based access controls and accounts for the transaction, ensuring the authenticity of each data process. A private blockchain environment is used, which can be extended to public or consortium blockchain for geographically distributed dependency.

Despite the practical application, FL has received widespread attention. How to allocate tasks in asynchronous FL effectively is largely ignored—minimizing the gradient staleness on edge nodes with heterogeneous computing and communication capacities may result in unbalanced allocation in a limited pool of participants, which is highly unfair to worse off participants. Existing fairness frameworks (Max–Min, Kalai–Smorodinsky, and proportional fairness) are based on collective fairness, i.e., once a participant feels unfair, he may leave to achieve higher benefits, which will affect the system sustainability. Lu *et al.* [A2] designed fairness-aware time-sensitive task allocation approach in asynchronous FL for CEI that formulate the task allocation issue by addressing two typical scenarios where learning accuracy, time, and individual fairness is considered concurrent. An optimal multidimensional contract where the optimal contract value is guarantees reliability, honesty, and fairness, which helps maximize the learning accuracy.

Without any knowledge of attackers, differential privacy has strong capabilities of protecting privacy. It has been widely applied in various areas, such as healthcare and Internet of Vehicles. Pan *et al.* [A3] designed a joint protection framework for energy security and information privacy by leveraging FL and differential privacy for healthcare. In order to avoid privacy leakage, a differential privacy-enabled information preserving method is presented, and a customized demand-based privacy-preserving method is designed to perturb sensitive information. Besides, a noncooperative game-based incentive mechanism is presented to optimize the utility of each ETs and encourage participation of ETs, and balance the joint energy-information security.

Biological information and medical advises are communicated over wireless to the doctor as well as to the patient. Open communication or unauthorized access is a security threat, such as impersonation, eavesdropping, or tampering with body sensors. The personal data of a user should be protected against threats during the communication among the WBAN entities. Subramani *et al.*[A4] presented a computationally efficient physically unclonable functions-based anonymous mutual authentication approach to verify the authenticity of the WBAN entities.

Attacks either do not exit or scare, which limits the applicability of the model. Besides, machine learning models are vulnerable to adversarial attacks. Cui *et al.* [A5] considered the relationship among users to prevent possible covert and adversarial attacks targeting electricity theft detection systems. First, smart grid community model vulnerabilities of existing electricity theft detection methods are presented. To address these vulnerabilities, the theft method by mimicking normal consumption patterns and comprising neighboring meters concurrently is presented, which is based on hand-crafted features extracted from the pair-wise relationship of a group of users.

Security and trust are the two main challenges in the healthcare sector. With the aim to maintain the confidentiality of the medical record, Siva Rama Krishnan *et al.* [A6] presented a blockchain-based security framework by securely accessing the patient's records in any hospital through the patient's public key as a universal identifier. The unique interplanetary file system can also be used to retrieve historical information of a patient.

Beni Prathiba *et al.* [A7] presented a migrating consignment region framework that employs SDN-assisted beaconless 5G-V2X communication to disseminate SCMs to AVs in CEI with low latency and ultrahigh reliability in the highway scenarios. The framework minimizes the overhead by creating the consignment region for each instance of data dissemination. The consignment region is created once and maintained continuously by combining consignment region, breaking consignment region, and updating consignment region algorithms, which handles AVs' high-mobility nature and delivers the SCMs efficiently.

The guest editors would like to thank all the authors who submitted their articles and anonymous reviewers who carefully reviewed and evaluated them. They would also like to extend their sincere thanks to the Editor-in-Chief of the IEEE Transactions on Industrial Informatics, Prof. Ren C. Luo, for providing the opportunity to edit this Special Issue and for his guidance throughout the process and the editorial staff for their continuous support in organizing the Special Section.

Imran Razzak, *Guest Editor*
Deakin University
Geelong, VIC 3220, Australia

Guandong Xu, *Guest Editor*
University of Technology Sydney
Broadway, NSW 2007, Australia

Muhammad Khurram Khan, *Guest Editor*
King Saud University
Riyadh 11451, Saudi Arabia

Appendix
Related Works

[A1] G. Kumar, R. Saha, and M. AlazabA, "Blockchain-based access control solution for industrial Internet-of-Things," *IEEE Trans. Ind. Informat.*, to be published, doi: 10.3390/app9102058.

[A2] J. Lu, H. Liu, Z. Zhang, J. Wang, S. K. Goudos, and S. Wan, "Towards fairness-aware time-sensitive asynchronous federated learning for critical energy infrastructure," *IEEE Trans. Ind. Informat.*, to be published, doi: 10.1109/TII.2021.3117861.

[A3] Q. Pan, J. Wu, A. K. Bashir, J. Li, W. Yang, and Y. D. Al-Otaibi, "Joint protection of energy security and information privacy for energy harvesting: An incentive federated learning approach," *IEEE Trans. Ind. Informat.*, to be published, doi: 10.1109/TII.2021.3105492.

[A4] J. Subramani, M. Azees, A. Sekar, and F. Al-Turjman, "Lightweight privacy and confidentiality preserving anonymous authentication scheme for WBANs," *IEEE Trans. Ind. Informat.*, to be published, doi: 10.1109/TII.2021.3097759.

[A5] L. Cui *et al.*, "A covert electricity-theft cyber-attack against machine learning-based detection models," *IEEE Trans. Ind. Informat.*, to be published, doi: 10.1109/TII.2021.3089976.

[A6] S. S. R. Krishnan *et al.*, "A blockchain-based credibility scoring framework for electronic medical records," *IEEE Trans. Ind. Informat.*, to be published, doi: 10.1109/GCWkshps50303.2020.9367459

[A7] S. B. Prathiba, G. Raja, A. K. Bashir, A. Ali AlZubi, and B. Gupta, "SDN-assisted safety message dissemination framework for vehicular critical energy infrastructure," *IEEE Trans. Ind. Informat.*, to be published, doi: 10.1109/TII.2021.3113130.

Imran Razzak (Senior Member, IEEE) received the Ph.D. degree in computer science from International Islamic University Islamabad, Islamabad, Pakistan, in 2012.

He has been a Senior Lecturer of Computer Science with the School of Information Technology, Deakin University, Geelong, VIC, Australia, since November 2019. He has authored or coauthored more than 120 papers in reputed journals and conferences. He is the author of one book and inventor of one patent on face recognition. He has attracted research grant of 1.2 million AUD and has successfully delivered several research projects. He has applied machine learning methods with emphasis to natural language processing and image analysis to solve real-world problems related to health, finance, social media, and biometric security. His research interests include machine learning with its application spans a broad range of topics.

Guandong Xu received the B.Sc. and M.Sc. degrees in computer science and engineering from Zhejiang University, Hangzhou, China, in 1989 and 1992 respectively, and the Ph.D. degree in computer science from Victoria University, Melbourne, VIC, Australia, in 2009.

He is currently a Professor with the School of Computer Science and Advanced Analytics Institute, University of Technology Sydney, Broadway, NSW, Australia. From 2012 to 2018, he has succeeded in three academic promotions from Lecturer to Full Professor. His research has received funding from Australian Research Council Discovery and Linkage Project, Cooperative Research Centre Program, government and industry, totaling over 5.5 million AUD in past years. He currently heads the Data Science and Machine Intelligence Research Lab, which consists of more than 15 members of academics, research fellows, and HDR students. Since November 2019, he has been directing the newly established Smart Future Research Centre, which is an across-disciplines industry engagement and innovation platform for AI and data science applications toward smart wealth and investment management, energy, food, water, living, and city. He has authored or coauthored more than 200 publications in the areas of data analytics and data science, web mining, recommender systems, text mining, social computing, and predictive analytics, including monograph books, edited conference proceedings, and dozens of journal and conference papers in top venues, e.g., IEEE Transactions on Neural Networks and Learning Systems, *ACM Transactions on Information Systems*, IEEE Transactions on Software Engineering, *ACM Transactions on Intelligent Systems and Technology*, IEEE Transactions on Services Computing, IEEE Transactions on Information Forensics and Security, *Information Sciences*, *Decision Support Systems*, IEEE-IS, *Knowledge and Information Systems*, IJCAI, AAAI, WWW, CVPR, ICDM, EMNLP, ICDE, CIKM, ASE etc.

Muhammad Khurram Khan (Senior Member, IEEE) received the Ph.D. degree in computing from Southwest Jiaotong University, Chengdu, China, in 2007.

He is currently a Professor with the Center of Excellence in Information Assurance (CoEIA), King Saud University, Riyadh, Kingdom of Saudi Arabia. From March 2009 to March 2012, he was one of the founding members of CoEIA and has served as the Manager RD. He developed and successfully managed the research program of CoEIA, which transformed the center as one of the best centers of research excellence in Saudi Arabia as well as in the region. He is a Global thought Leader and influencer in cybersecurity. He is the founder and CEO of the “Global Foundation for Cyber Studies and Research” which is an independent and nonpartisan cybersecurity think-tank based in Washington, DC, USA. He has contributed cyber policy works for the G20 in shaping a safer cyberspace for children, protection of masses in the cyberspace, and empowering and enabling women in cybersecurity profession.

Prof. Khurram has been the Editor-in-Chief of a well-esteemed international journal *Telecommunication Systems*, published by Springer-Nature, since 1993 with an impact factor of 2.314 (JCR 2021). He is also the Editor-in-Chief of *Cyber Insights Magazine*. Furthermore, he is the full-time Editor/Associate Editor of several international journals/magazines, including IEEE Communications Surveys Tutorials, *IEEE Communications Magazine*, IEEE Internet of Things Journal, IEEE Transactions on Consumer Electronics, *Journal of Network Computer Applications* (Elsevier), IEEE Access, *Security Communication Networks*, *IEEE Consumer Electronics Magazine*, *Journal of Medical Systems* (Springer), *PLoS ONE*, *Computers Electrical Engineering* (Elsevier), *IET Wireless Sensor Systems*, *Electronic Commerce Research* (Springer), *Journal of Computing Informatics*, *Journal of Information Hiding and Multimedia Signal Processing* (JIHMSP), *International Journal of Biometrics* (Inderscience), etc.