Deep Learning Driven Secure Communication for Cyber Physical Systems

Wei Wei

Ching-Hsien Hsu

Vincenzo Piuri

Ammar Rayes

The proliferation of industrial cyber physical systems (CPSs) is changing our lives. CPS applications are often associated with sensitive data, core infrastructures, and assets, making them attractive in terms of vulnerability, data breach, and denial of services. Moreover, the heterogeneity in terms of protocols, operating systems, and devices combined with poor adoption of standard solutions create insecure design, architectures, and deployments. In addition, due to the use of wireless technologies, secure communication is strongly needed to protect valuable information. Therefore, secure communication management has become a crucial aspect of developing trustworthy systems with the preservation of security and privacy for CPSs. Deep learning (DL) has strong potential to overcome this challenge via data-driven solutions and improve the performance of CPSs while utilizing limited spectrum resources. DL is a more powerful method of data exploration to learn about "normal" and "abnormal" behavior according to how CPSs' components and devices interact with one another. The input data of each part of a CPS can be collected and investigated to determine normal patterns of interaction, thereby identifying malicious behavior at early stages. Moreover, DL can be important in predicting new attacks, which are often mutations of previous attacks, because they can intelligently predict future unknown attacks by learning from existing examples. Consequently, CPSs must have a transition from merely facilitating secure communication among devices to security-based intelligence enabled by DL methods for effective and secure systems.

However, the challenge in applying DL for secure communication in CPSs has yet to be addressed. Such challenges include but are not limited to risks and regulatory issues as well as other associated factors related to processing, storage, and availability for secure communication. Therefore, this Special Issue (SI) aims to bring together researchers from different sectors to focus on understanding security challenges of CPSs, and architect innovative solutions with the help of cutting edge DL related technologies. Based on the reviewers' feedback, as well as the evaluations of the Editors, 10 papers were selected for this SI from more than 90 submissions. The 10 articles, which cover broad topics, are introduced briefly as follow.

The article "Deep Learning Powered Adversarial Sample Attacks Approach for Security Detection of DGA Domain Name in Cyber Physical Systems" authored by Shen *et al.* proposes a domain name detection system to solve this security issue in CPSs. In the system, a DL-powered adversarial sample attacks approach is embedded to improve its performance. The experimental results prove that the proposed system achieves better performance in the malicious domain name recognition task.

The article "Deep Federated Learning-Enhanced Secure POI Microservices for Cyber Physical Systems" authored by Guo *et al.* proposes a deep federated-learning-based framework for secure POI microservices under CPSs. In order to enhance data security, the system architecture is designed by isolating the cloud center from accessing user data at edge nodes, and an interactive training mechanism is introduced between the cloud center and edge nodes. The experimental results prove that this proposal achieves optimal scheduling performance, which demonstrates its practical utility.

The article "An Ultra-Lightweight Data-Aggregation Scheme with Deep Learning Security for Smart-Grid" authored by Gope *et al.* proposes a DL-based ultra-lightweight data aggregation scheme for smart-grids. Unlike existing data aggregation schemes, the proposed solution does not require storing any secret but can still ensure a higher level of security. Also, to the best of the authors' knowledge, it is the first aggregation scheme that can ensure physical security of the smart meter.

The article "Attack Detection and Data Generation for Wireless Cyber-physical Systems Based on Self-Training Powered Generative Adversarial Networks" authored by Huang *et al.* proposes a self-training powered generative adversarial network (ST-GAN) to detect attacks in wireless CPSs. The proposed ST-GAN system solves the issue of limited data in the field of security for wireless CPSs, which is caused by confidentiality as well as the number of attacks. Experimental results prove that the proposed system can effectively detect attacks in wireless CPSs.

The article "Distributed Q-Learning Enabled Multi-Dimensional Spectrum Sharing Security Scheme for 6G Wireless Communication" authored by Ding *et al.* proposes a distributed Q-learning enabled multi-dimensional spectrum sharing security scheme for the millimeter-wave frequency band. To prove this scheme, the authors use simulations to verify the performance of the proposed distributed Q-learning algorithm for solving the spectrum sharing optimization problem. Results prove that the proposed multi-dimensional spectrum sharing security scheme can significantly reduce the access delay of users, increase the number of unauthorized users that can be accommodated, and improve the throughput while achieving good security performance of the network.

The article "A Deep Learning Assisted Software Defined Security Architecture For 6G Wireless Networks: IIoT Perspective" authored by Rahman *et al.* studies the security challenges on 6G networks posed by the recent convergence of operational technology and information technology networks, and proposes distributed DL-assisted software-defined security for 6G wireless networks that will autonomously detect, localize, and isolate security threats via security function virtualization.

The article "Deep-Learning Based Mobile Group Intelligence Perception Mechanism Oriented to User Privacy and Data Security in the Internet of Things" authored by Hu *et al*. proposes a mobile group intelligence perception mechanism oriented to user privacy and data security. This mechanism uses DL as its core algorithm to handle big data cases. It can provide authenticity and reliability guarantees for the subsequent data application on the premise of protecting user privacy. Experimental results prove that this proposed mechanism meets the security requirements, and its user-end computing overhead is small.

The article "Federated Learning Driven Secure Internet of Medical Things" authored by Fan *et al.* proposes a federated learning driven Internet of Medical Things (FLDIoMT) framework, which aims to support flexible deployment of IoMT services and address the privacy and security issues at the same time. Results prove the feasibility of the proposed FLDIoMT framework by implementing a novel sleep monitoring system called iSmile.

The article "Toward Industrial Private AI: A Two-Tier Framework for Data and Model Security" authored by Khowaja *et al.* proposes a federated learning and encryption-based private (FLEP) AI framework that provides two-tier security for data and model parameters in an Industrial Internet of Things environment. Experimental results prove that the proposed framework achieves better encryption quality at the expense of slightly increased execution time.

The article "Blockchain and Federated Deep Reinforcement Learning-Based Secure Cloud-Edge-End Collaboration in Power IoT" authored by Zhang *et al.* proposes a blockchain and AI-based secure cloud-edge-end collaboration Power Internet of Things architecture to ensure data security and intelligent computation offloading. Its advantages in flexible resource allocation, secure data sharing, and differentiated service guarantee are elaborated. Numerical results verify its excellent performance in total queuing delay and consensus delay.

The Guest Editors would like to thank all the authors who submitted their papers and anonymous reviewers who carefully reviewed and helped evaluate these papers. We would also like to extend our sincere thanks to the Editor-in-Chief, Yi Qian, and Associate Editor-in-Chief, Nirwan Ansari, for their support in the publication of this SI.

Biographies

Wei Wei [SM] works at Xi'an University of Technology, China. He received his Ph.D from Xi'an Jiaotong University. His research interests include the Internet of Things, wireless sensor networks, image processing, mobile computing, distributed computing, pervasive computing, smart city, artificial intelligence, sensor data clouds, and more. He has over 200 papers published or accepted by international conferences and journals (e.g., *IEEE Transactions on Services Computing*, *IEEE Transactions on Industrial Informatics*, *IEEE Transactions on Computational Social Systems*, *IEEE Communications Magazine*, *IEEE Transactions on Parallel and Distributed Systems*, and the *IEEE Internet of Things Journal*). He is an Associate Editor of *IEEE Access*. He is also an editorial member of *Future Generation Computer Systems*, *Neural Computing and Applications*, the *Journal of Network and Computer Applications*, *Ad Hoc & Sensor Wireless Networks*, *IEICE Transactions on Information and Systems*, and *KSII Transactions on Internet and Information Systems*. He has also been lead Guest Editor of *IEEE Transactions on Industrial Informatics*, *ACM Transactions on Internet Technology*, *IEEE Intelligent Systems*, *Image and Vision Computing*, *Computer Communications*, the *International Journal of Distributed Sensor Networks*, *IEEE Access*, *Mathematical Biosciences and Engineering*, *Personal and Ubiquitous Computing*, the *Computing Journal*, *Design Automation for Embedded Systems*, the *Journal of Ambient Intelligence and Humanized Computing*, and the *Journal of Internet Technology*. He has been a TPC member of many conferences and a regular reviewer for *IEEE Communications Magazine*, *IEEE Transactions on Parallel and Distributed Systems*, *IEEE Transactions on Image Processing*, *IEEE Transactions on Mobile Computing*, *IEEE Transactions on Wireless Communications*, *IEEE Transactions on Industrial Informatics*, and *IEEE Transactions on Industrial Electronics*. He has participated in many funded research projects as Principal Investigator and technical member. He is a Senior Member of CCF.

Ching-Hsien Hsu [SM] is Chair Professor and Dean of the College of Information and Electrical Engineering, Asia University, Taiwan. His research includes high-performance computing, cloud computing, parallel and distributed systems, big data analytics, and ubiquitous/pervasive computing and intelligence. He has published 200 papers in top journals such as *IEEE TPDS*, *IEEE TSC*, *ACM TOMM*, *IEEE TCC*, *IEEE TETC*, the *IEEE Systems Journal*, *IEEE Network*, top conference proceedings, and book chapters in these areas. He is the Editor-in-Chief of the *International Journal of Grid and High Performance Computing* and the *International Journal of Big Data Intelligence*, and serves on the Editorial Boards of a number of prestigious journals, including *IEEE Transactions on Service Computing*, *IEEE Transactions on Cloud Computing*, the *International Journal of Communication Systems*, the *International Journal of Computational Science*, and the *AutoSoft Journal*. He has been an author/co-author or an editor/co-editor of 10 books from Elsevier, Springer, IGI Global, World Scientific, and McGraw-Hill. He was awarded six times talent awards from Ministry of Science and Technology, Ministry of Education, and nine times distinguished award for excellence in research from Chung Hua University, Taiwan. Since 2008, he has been serving as executive committee of IEEE Technical Committee of Scalable Computing; IEEE Special Technical Co mmittee Cloud Computing; Taiwan Association of Cloud Computing. He is a Fellow of the IET (IEE), and Chair of the IEEE Technical Committee on Cloud Computing and the IEEE Technical Committee on Scalable Computing.

Vincenzo Piuri [F] received his Ph.D. in computer engineering from Politecnico di Milano, Italy, in 1989. He has been a full professor in computer engineering at the Università degli Studi di Milano, Italy, since 2000. He was an associate professor at Politecnico di Milano, and a visiting professor at the University of Texas at Austin and George Mason University. His main research interests are: artificial intelligence, computational intelligence, intelligent systems, machine learning, pattern analysis and recognition, signal and image processing, biometrics, intelligent measurement systems, industrial applications, digital processing architectures, fault tolerance, and cloud computing infrastructures. Original results have been published in 400+ papers in international journals, proceedings of international conferences, books, and book chapters. He is a Distinguished Scientist of ACM and a Senior Member of INNS. He was President of the IEEE Systems Council (2020–2021), IEEE Vice President for Technical Activities (2015), IEEE Director, President of the IEEE Computational Intelligence Society, Vice President for Education of the IEEE Biometrics Council, Vice President for Publications of the IEEE Instrumentation and Measurement Society and the IEEE Systems Council, and Vice President for Membership of the IEEE Computational Intelligence Society. He was Editor-in-Chief of the *IEEE Systems Journal* (2013–2019). He is an Associate Editor of *IEEE Transactions on Cloud Computing* and has been an Associate Editor of *IEEE Transactions on Computers*, *IEEE Transactions on Neural Networks*, *IEEE Transactions on Instrumentation and Measurement*, and *IEEE Access*. He received the IEEE Instrumentation and Measurement Society Technical Award (2002). He is an Honorary Professor at: Obuda University, Hungary; Guangdong University of Petrochemical Technology, China; Northeastern University, China; Muroran Institute of Technology, Japan; and Amity University, India.

Ammar Rayes has authored over 100 publications in refereed journals and conferences on advances in software and networking related technologies, 4 books, and over 35 U.S. and international patents. He is the Founding President and board member of the International Society of Service Innovation Professionals (www.issip.org), an adjunct professor at San Jose State University, Editor-in-Chief of the *Advances of Internet of Things Journal*, Senior Editor of the *IEEE Journal on Selected Areas in Communications*, and an Editorial Board member of the *IEEE Blockchain Newsletter*, *Transactions on Industrial Networks and Intelligent Systems*, the *Journal of Electronic Research and Application*, and the European Alliance for Innovation — Industrial Networks and Intelligent Systems. He has served as an Associate Editor of *ACM Transactions on Internet Technology and Wireless Communications* and the *Mobile Computing Journal*, a Guest Editor of multiple journals and over half a dozen *IEEE Communications Magazine* and *IEEE Network* issues, co-chaired the Frontiers in Service Conference, and appeared as a keynote speaker at several IEEE and industry conferences (https://sites.google.com/view/ammarrayes/home). At Cisco, he is the founding Chair of Cisco Services Research and the Cisco Services Patent Council. He received the Cisco Chairman's Choice Award for IoT Excellent Innovation & Execution. He received his B.S. and M.S. Degrees in EE from the University of Illinois at Urbana and his Ph.D. degree in EE from Washington University in St. Louis, Missouri, where he received the Outstanding Graduate Student Award in Telecommunications.