Guest Editors' Introduction to the Joint Special Section on Secure and Emerging Collaborative Computing and Intelligent Systems

Yuan Hong, *Senior Member, IEEE*, Valerie Issarny, *Member, IEEE*, Surya Nepal, *Senior Member, IEEE*, and Mudhakar Srivatsa

The Internet coupled with recent advances in computing and information technologies, such as IoT, mobile edge/cloud computing, cyber-physical-social systems, and artificial intelligence/machine learning/deep learning, have paved the way for creating next-generation smart and intelligent systems and applications that can have transformative impact in our society while accelerating rapid scientific discoveries and innovations. Unprecedented cyber-social and cyber-physical infrastructures and systems that span geographic boundaries are possible because of the Internet and the growing number of collaboration-enabling technologies. With newer technologies and paradigms getting increasingly embedded in the computing platforms and networked information systems/infrastructures that form the digital foundation for our personal, organizational, and social processes and activities, it is increasingly becoming critical that the trust, privacy, and security issues in such digital environments are holistically addressed to ensure the safety and well-being of individuals as well as our society.

This joint special section of IEEE Transactions on Emerging Topics in Computing (TETC) and IEEE Transactions on Dependable and Secure Computing (TDSC) focuses on the security, privacy and trust of the emerging collaborative computing and intelligent systems. It includes 11 high quality peer-reviewed papers (3 articles in TETC and 8 articles in TDSC) on various emerging topics: cryptographic protocol, differential privacy, blockchain security, cloud security, machine learning robustness, authorizations, mobile computing, and deep learning for blockchain applications. The 11 papers in this joint special section are listed as below:

1) Towards the AlexNet Moment for Homomorphic Encryption: HCNN, the First Homomorphic CNN on Encrypted Data with GPUs (in TETC).
2) Bitcoin Transaction Forecasting with Deep Network Representation Learning (in TETC).
3) SDLSC-TA: Subarea Division Learning Based Task Allocation in Sparse Mobile Crowdsensing (in TETC).
4) Robust Deep Learning Ensemble against Deception (in TDSC).
5) An Optimal Noise Mechanism for Cross-correlated IoT Data Releasing (in TDSC).
6) Differentially Private k-Means Clustering with Convergence Guarantee (in TDSC).
7) VMGuard: State-based Proactive Verification of Virtual Network Isolation with Application to NFV (in TDSC).
8) Quantify Co-Residency Risks in the Cloud through Deep Learning (in TDSC).
9) Fee-Free Pooled Mining for Countering Pool-Hopping Attack in Blockchain (in TDSC).
10) Sustainable Ensemble Learning Driving Intrusion Detection Model (in TDSC).
11) Stochastic Workflow Authorizations with Queueing Constraints (in TDSC).

In this special section, there is an increasing trend for research focusing on security and privacy in deep learning, as well as applying deep neural networks to emerging applications. Besides two papers (on privacy in deep learning and deep learning for the blockchain applications) in TETC, another paper entitled "*Robust Deep Learning Ensemble against Deception*", proposes XEnsemble, a diversity ensemble verification methodology for enhancing the adversarial robustness of DNN models against deception caused by either adversarial examples or out-of-distribution inputs. It builds diverse input denoising verifiers, develops a disagreement-diversity ensemble learning methodology for guarding the output of the prediction model against deception, and provides a suite of algorithms to combine input verification and output verification to protect the DNN prediction models from both adversarial examples and out of distribution inputs.

This special section also includes two papers on differential privacy. The first work, entitled "*An Optimal Noise Mechanism for Cross-correlated IoT Data Releasing*" proposes a novel Correlated noise mechanism for Cross-correlated Data Privacy (CCDP), which can be used to protect cross correlation privacy within correlated datasets, such as trajectories from

- *Yuan Hong is with the Department of Computer Science, Illinois Institute of Technology, Chicago, IL 60616 USA. E-mail: yuan.hong@iit.edu.*
- *Valerie Issarny is with Inria, 33405 Talence, France. E-mail: valerie.issarny@inria.fr.*
- *Surya Nepal is with the CSIRO's Data61, Sydney, NSW 2015, Australia. E-mail: Surya.Nepal@data61.csiro.au.*
- *Mudhakar Srivatsa is with IBM Research, Yorktown Heights, NY 10598 USA. E-mail: msrivats@us.ibm.com.*

Digital Object Identifier no. 10.1109/TDSC.2021.3076120

1545-5971 © 2021 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.
See https://www.ieee.org/publications/rights/index.html for more information.

smartphones and smart meters data in smart grids. They perform rigorous mathematical analysis of the CCDP and prove that it satisfies ϵ-Pufferfish privacy, and also prove that the CCDP can achieve the optimal data utility for a given privacy budget ϵ, which has been experimentally validated on three types of datasets: computer-generated data, real-world trajectory data, and smart meter data. The other work, entitled "*Differentially Private k-Means Clustering with Convergence Guarantee*" addresses the non-convengence problem of the existing solutions for differentially private k-means clustering, by proposing a novel framework for injecting differential privacy into the real centroids in the interactive setting. The authors have also validated the superiority of the proposed algorithms in clustering quality to the state-of-the-art results through extensive experiments on six widely used real-world datasets.

In cloud security, an accepted paper, entitled "*VMGuard: State-based Proactive Verification of Virtual Network Isolation with Application to NFV*" proposes VMGuard, a state-based proactive approach for efficiently verifying large-scale virtual infrastructures in cloud and Network Functions Virtualization (NFV) against network isolation policies. They have implemented VMGuard based on OpenStack, and evaluated it on both real and synthetic data. The results demonstrate the performance and efficiency, e.g., less than five milliseconds to perform incremental verification on a dataset with more than 25,000 VMs and less than two milliseconds with the proactive module enabled. Another paper, entitled "*Quantify Co-Residency Risks in the Cloud through Deep Learning*" proposes a fine-grained model to quantify the risk level caused by co-residency in the cloud through deep learning. Using a large scale dataset collected from Microsoft Azure Platform, the authors profile the behavior patterns of normal service subscribers (tenants) using the proposed feature metrics, and cluster tenants into multiple categories. A classification component and a quantification component are constructed to dynamically quantify the co-residency risks for a specific virtual machine.

To improve the blockchain security, one paper "*Fee-Free Pooled Mining for Countering Pool-Hopping Attack in Blockchain*" addresses the Pool-Hopping Attack for the Blockchain. They apply the zero-determinant (ZD) theory to design a novel pooled mining which offers an incentive mechanism for motivating miners not to switch in pools strategically by economic means without fee charged. The proposed pooled mining has three unique features: (1) fee-free: no fee is charged if the miner does not hop, (2) wide applicability: it can be employed in both prepaid and postpaid mechanisms, and (3) fairness.

Finally, two other papers design learning models to solve security problems. The first paper "*Sustainable Ensemble Learning Driving Intrusion Detection Model*" proposes a model based on sustainable ensemble learning to improve accuracy for intrusion detection systems, by considering the accumulation and reuse of historical knowledge, as well as the sensitivity of the detection model to different types of attacks. They have conducted experiments to validate the detection accuracy, false alarm, stability and robustness by benchmarking with the existing solutions. The second paper "*Stochastic Workflow Authorizations with Queueing Constraints*" studies the authorization model under the more realistic dynamic settings to secure cloud-based workflow architecture, which can be widely used in e-science, e-business, smart city, and others, to automate business processes and improve their flexibility and maintainability.

As guest editors, we would like to thank all the authors who submitted their quality work to this joint special section, and also would like to thank all the anonymous reviewers for their valuable time and constructive comments. Finally, we would like to thank the Editor-in-Chiefs of IEEE TETC (Dr. Paolo Montuschi and Dr. Cecilia Metra) and Editor-in-Chief of IEEE TDSC (Dr. Jaideep Vaidya), and all the staff of two journals for their guidance and support.

Yuan Hong (Senior Member, IEEE) received the PhD degree in information technology from Rutgers University, New Brunswick, New Jersey. He is currently an assistant professor with the Department of Computer Science, Illinois Institute of Technology, Chicago, Illinois. His research primarily focuses on differential privacy, secure multiparty computation, adversarial machine learning, mechanism design, and optimization. He received the NSF CAREER Award in 2021.

Valerie Issarny (Member, IEEE) is currently a director of research with Inria, French Institute for Research in Digital Sciences. Her research focuses on middleware solutions easing the development of distributed collaborative services, including mobile services deployed over smartphones and interacting with sensors and actuators. She has published more than 200 technical papers. She is an associate editor of the *ACM Transactions on the Internet of Things*, *IEEE Transactions on Services Computing*, and *IEEE Transactions on Software Engineering*. She is an editor in chief of the *ACM Transactions on Autonomous and Adaptive Systems*. For more deatails please visit: http://valerie-issarny.me/.

Surya Nepal (Senior Member, IEEE) is currently a senior principal research scientist with CSIRO Data61. He currently leads the Distributed Systems Security Group comprising more than 30 research staff and more than 50 postgraduate students. His main research focus is in the development and implementation of technologies in the area of cybersecurity and privacy, and AI and cybersecurity. He has more than 250 peer-reviewed publications to his credit. He is a member of the editorial boards of the *IEEE Transactions on Service Computing*, *ACM Transactions on Internet Technology*, *IEEE Transactions on Dependable and Secure Computing*, and *Frontiers of Big Data- Security Privacy, and Trust*. He is currently a theme leader of Cybersecurity Cooperative Research Centre (CRC), a national initiative in Australia.

Mudhakar Srivatsa is currently a distinguished research staff member and manager with the Distributed AI Department, IBM T. J. Watson Research Center. His work is focused on distributed machine learning and edge intelligence on spatial and temporal data gathered from heterogeneous data sources while being robust under adversarial settings. He is an IBM master inventor, authored more than 100 research papers, 75 granted US patents and and has transitioned major software artifacts to various commercial product offerings.

▷ **For more information on this or any other computing topic, please visit our Digital Library at** www.computer.org/csdl.