Guest Editorial Introduction to the Special Issue on Deep Learning Models for Safe and Secure Intelligent Transportation Systems

THE autonomous vehicular technology is approaching a level of maturity that gives confidence to end-users in many cities around the world for their usage so as to share the roads with manual vehicles. Autonomous and manual vehicles have different capabilities which may result in surprising safety, security, and resilience impacts when mixed together as a part of the intelligent transportation system (ITS). For example, autonomous vehicles can communicate electronically with one another, make fast decisions and associated actuation, and generally act deterministically. In contrast, manual vehicles cannot communicate electronically, are limited by the capabilities and slow reaction of human drivers, and may show some uncertainty and even irrationality in behavior due to the involvement of humans. At the same time, humans can react properly to more complex situations than autonomous vehicles. Unlike manual vehicles, the security of computing and communications of autonomous vehicles can be compromised thereby precluding them from achieving individual or group goals.

Given the expected mixture of autonomous and manual vehicles that is expected to persist for many decades, safety and security issues for a mixture of autonomous and manual vehicles are crucial to investigate before autonomous vehicles enter our roadways in numbers. To improve the safety and security of the transportation system, artificial intelligence (AI)-based techniques and deep learning models have extensively been applied to the data-driven ITS model. Despite the pioneering works on the integration of ITS data with deep learning techniques, such techniques still require more accurate perception since the false positives generated during the execution of the algorithms can perturb the utility of real-time data analytics particularly for safety applications in ITS. More importantly, the recent breakthrough in generative adversarial networks in machine learning better demonstrates the criticality of the safety problems in ITS in the presence of advanced persistent threats as that adversarial models can be generated at an accelerating pace. Therefore, it is crucial to understand how both types of vehicles will fare in terms of safety (avoidance of dangerous situations), performance (acceptable delays and throughput), and resilience (fast recovery from dangerous situations) under a variety of uncertain situations without and with attacks on autonomous vehicle communications in the presence of hidden adversaries who exploit machine learning security loopholes.

Despite the existing research on cyber-attacks on the functions of individual vehicles, the focus on the interplay of different types of vehicles under the influence of cyber-adversaries is missing. To address the abovementioned challenges, there is a need for new algorithmic developments beyond traditional topics in big data, deep neural networks, and cybersecurity.

This Special Issue of the IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS captures the most recent advances and technologies pertaining to the theoretical development of deep-learning models and techniques for improving security and safety in ITS. We received so many articles from different research groups and a variety of perspectives for this Special Issue. After a thorough evaluation of the articles by reviewers, the editorial board chose 47 high-quality research articles which cover a range of topics from the special issue theme, as specified in the call. These articles are representative solutions that attempt to present novel applications of deep learning models for safe and secure intelligent transportation systems and collectively reflect the advances, challenges, and directions for current and future research. The articles have been organized in the following categories to facilitate their reading:

- optimizing safety in ITS using deep learning (ten articles);
- deep learning based security, integrity and privacy solutions for ITS (ten articles);
- deep learning based intrusion detection and prevention techniques (nine articles);
- deep learning based solutions to tackle traffic congestion (six articles);
- deep learning based crowd sensing solutions for ITS (four articles);
- future applications of deep learning models in ITS (eight articles).

The Special Issue opens with the article entitled "Vehicle detection and tracking in adverse weather using a deep learning framework" by Hassaballah *et al.*, which addresses the problem of vehicle detection and tracking under adverse weather conditions by introducing a visibility restoration

Digital Object Identifier 10.1109/TITS.2021.3090721

method to improve images' quality. To maintain the safety of vehicles in adverse weather, the authors propose an online vehicle tracking scheme using the YOLOv3 architecture for overcoming problems caused by missed detection, false positives, and occlusions. To ensure the safety of trains in adverse weather, Liu *et al.* propose a model named Multiple Attention Layer-based Multi-Instance Learning (MAL-MIL), which estimates the possibility that the actual wind speed exceeds the safety threshold, in the article entitled "Short-term strong wind risk prediction for high-speed railway." In the article entitled "ReViewNet: A fast and resource optimized network for enabling safe autonomous driving in hazy weather conditions," Mehra *et al.* propose a fast and lightweight deep learning model named ReviewNet for haze removal, thus making higher level tasks like object detection, segmentation, and decision making faster and more accurate.

Connected and automated vehicles are prominent innovations of the emerging smart world and they have significantly improved in recent years. In the article entitled "Toward safe and smart mobility: Energy-aware deep learning for driving behavior analysis and prediction of connected vehicles," Xing *et al.* propose an energy-aware driving pattern analysis and motion prediction system for connected vehicles using a deep learning-based time-series modeling approach. To improve the accuracy of traffic prediction and also to reduce the data transmission delay, Lv *et al.* propose an efficient routing strategy using deep learning methods in the article entitled "Solving the security problem of intelligent transportation system with deep learning." In the article entitled "Anomaly detection in automated vehicles using multistage attention-based convolutional neural network," Javed *et al.* propose a combination of a multi-stage attention mechanism with a Long Short-Term Memory (LSTM)-based Convolutional Neural Network (CNN) and a weight-adjusted fine-tuned ensemble to detect anomalies in connected and automated vehicles. The proposed method is capable of detecting various single and mixed anomaly types.

Traditional vehicle location methods, such as the Global Position System (GPS), can only locate the 1-D Direction Of Arrivals (DOAs) estimation of target vehicles. The super-resolution cannot be achieved when two vehicles are too close, which means that safety incidents exist when autonomous vehicles are deployed in future ITS. To address the problem, Wan *et al.* propose a massive multi-input multi-output, reconfigurable, intelligent surface using deep learning in the article entitled "Deep learning based autonomous vehicle super resolution DOA estimation for safety driving." In the article entitled "Deep learning for safe autonomous driving: Current challenges and future directions,"Muhammad *et al.* explain the potentials of deep learning architectures in terms of reliability and efficient real-time performance and overview the state-of-the-art strategies for safe autonomous driving using this family of modeling approaches, including their major achievements and limitations.

In the article entitled "Deep learning-based traffic safety solution for a mixture of autonomous and manual vehicles in the 5G-enabled intelligent transportation system," Yu *et al.* propose a deep learning-based traffic safety solution for a mixture of autonomous and manual vehicles in a 5G-enabled ITS. In the article entitled "A novel deep Q-learning based air-assisted vehicular caching scheme for safe autonomous driving," Shi *et al.* propose a deep Q-learning based air-assisted vehicular caching scheme to respond to the driving safety-related content requests of vehicle users. The method uses a three-layered content response architecture, where an airship is leveraged to take charge of the scheduling of vehicles to improve the content response. Deep Q-learning is applied to solve the multi-objective problem by learning from the history content requests of vehicle users.

The feature matching used in Vehicular Ad Hoc Networks (VANETs) has seriously threatened personal safety and caused considerable economic loss due to the disclosure of users' privacy. In the article entitled "Oblivious transfer for privacy-preserving in VANET's feature matching," Wang *et al.* propose an oblivious transfer protocol and a private set intersection protocol to protect users' privacy in the situation of VANET's feature matching. The proposed scheme does not use complex calculations and resists quantum attacks. To ensure the accuracy of task assignment while protecting the privacy of vehicles' locations, Qian *et al.* propose a task protection mechanism which meets the requirements on privacy protection in the article entitled "Optimal location privacy preserving and services quality guaranteed in vehicle-based crowdsensing networks."

In the article entitled "SPEED: A deep learning assisted privacy-preserved framework for intelligent transportation systems," Usman *et al.* propose a framework named SPEED to manage multimedia data and preserve the privacy using a multilevel edge computing architecture and machine learning algorithms in ITS. The proposed method helps in addressing issues like data redundancy and privacy-preserving in end-to-end communications. To identify the network attacks and to reduce the security concerns in the VANETs, a Secure and Private-Collaborative Intrusion Detection System (SP-CIDS) is proposed by Raja *et al.* in the article entitled "SP-CIDS: Secure and private collaborative IDS for VANETs." In the article entitled "Stochastic modeling and integration of plug-in hybrid electric vehicles in reconfigurable microgrids with deep learning-based forecasting," Dabbaghjamanesh *et al.* investigate the impact of uncoordinated, coordinated, and smart charging of plug-in hybrid electric vehicles on the optimal operation of microgrids incorporating the dynamic line rating security constraint. The authors propose a deep learning gated recurrent unit technique to forecast renewable power output for mitigating the uncertainties in renewable energy components.

In the article entitled "A deep learning-based blockchain mechanism for secure Internet of Drones environment," Singh *et al.* propose a blockchain-based security mechanism for the Internet of Drones Environment, where the miner node is selected using a deep learning-based approach using features like computational resources, the available battery power, and flight time of the drone. In the article entitled "Robust, resilient and reliable architecture for Vehicle to Everything (V2X) communication," Khan *et al.* propose a robust, resilient, and reliable architecture for V2X communications. They also propose a blockchain-based transaction that ensures reliability.

In the article entitled "Deep learning based semi-supervised control for vertical security of maglev vehicle with guaranteed bounded airgap," Sun *et al.* propose a semi-supervised controller based on a deep belief network algorithm for Maglev vehicle in the presence of unknown external disturbances. An output-constrained controller is designed by a backstepping method, and the estimated value of extended state observer is introduced to ensure that the output airgap is constrained within a bounded range.

A large scale fast-growing data generated in ITS has become a ponderous burden on the coordination of heterogeneous transportation networks, which makes the traditional cloud-centric storage architecture no longer satisfy new data analytics requirements. Meanwhile, the lack of storage trust between ITS devices and edge servers could lead to security risks in the data storage process. However, a unified data distributed storage architecture for ITS with intelligent management and trustworthiness is absent in the previous works. To address these challenges, in the article entitled "Trustworthy edge storage orchestration in intelligent transportation systems using reinforcement learning," Qiao *et al.* propose a distributed trustworthy storage architecture with reinforcement learning, which also promotes to support edge services.

Existing statistical non-learning based models for measuring the trust level of a driverless are not so effective because of not being able to capture the extremely distributed, dynamic, and complex nature of the traffic systems. In the article entitled "Assessing trust level of a driverless car using deep learning," Karmakar *et al.* propose two deep learning-based models for measuring the trustworthiness of a driverless car and assessing the trust level of its major on-board unit components. Despite the rapid development of the Internet of vehicles, connected vehicles, autonomous vehicles, and autonomous driving technologies, the automotive controller area networks are still suffering from various intrusion attacks. To address the problem, In the article entitled "Threat analysis for automotive CAN networks: A GAN model-based intrusion detection technique," Xie *et al.* propose an enhanced deep learning generative adversarial network (GAN) model using controller area network message blocks and an enhanced GAN discriminator. In the article entitled "An evolutionary deep learning based anomaly detection model for securing vehicles," Kavousi-Fard *et al.* propose a deep-learning-based attack detection based on a GAN classification to assess the message frames transferring between the electric control unit (ECU) and other hardware inside the vehicle.

An ITS pervasively deploys thousands of video cameras. Analyzing live video streams from those cameras is of significant importance to public safety. To address the problem, Wan *et al.* propose a long video event retrieval algorithm based on superframe segmentation in the article entitled "An intelligent video analysis method for abnormal event detection in intelligent transportation systems." In the article entitled "A two-phase anomaly detection model for secure intelligent transportation ride-hauling trajectories," Belhadi *et al.* propose a two-phase based approach for identifying individual and group taxi frauds. A parallel version of the algorithm is also proposed using a sliding window-based GPU approach to boost the runtime performance. In the article entitled "Novel deep learning-enabled LSTM autoencoder architecture for discovering anomalous events from intelligent transportation systems," Ashraf *et al.* propose a deep learning-based intrusion detection system for ITS to discover suspicious network activity of In-Vehicle Networks (IVN), Vehicle to Vehicle (V2V) communications, and Vehicle to Infrastructure (V2I) networks.

In the article entitled "Collaborative intrusion detection for VANETs: A deep learning based distributed SDN approach," Shu *et al.* propose a collaborative intrusion detection system for VANETs using a deep-learning-based, distributed Software-Defined Networking (SDN) approach to detect abnormal network behaviors under local sub-networks rather than the entire VANET. In the article entitled "Airborne LiDAR assisted obstacle recognition and intrusion detection towards unmanned aerial vehicle: Architecture, modelling and evaluation," Miao *et al.* propose an obstacle recognition and intrusion detection algorithm for Unmanned Aerial Vehicle (UAV)-based on an Airborne LiDAR (ALORID). In the article entitled "Information-centric content management framework for software defined Internet of Vehicles towards application specific services," Manogaran *et al.* propose an information-centric content management framework for effective information utilization in the vehicular networks. This framework performs data acquisition, smoothing, and management process for effective information analysis and better offloading. The proposed framework incorporates the functions of linear vector quantization for classifying acquired information and segregating it for maximum utilization. This quantization is recurrent in both continuous and alternating learning process to improve the reliability of information handling and management.

The Cognitive Internet of Vehicles (CIoV) is an intelligent network that embeds the cognitive mechanism in the Internet of Vehicles (IoV) to sense the environment and observe the network states to learn the optimal policies adaptively. However, one of the key challenges in CIoV systems is to design a smart agent that can smartly schedule the packet transmission for ultra-reliable low latency communication under extreme random and noisy network conditions. In the article entitled "A generative adversarial network enabled deep distributional reinforcement learning for transmission scheduling in the Internet of Vehicles," Naeem *et al.* propose a GAN-Scheduling algorithm, that is, an SDN based scheme that leverages a generative adversarial network-powered deep distributional Q network for learning the action-value distribution for intelligent transmission scheduling.

In the article entitled "Topological graph convolutional network based urban traffic flow and density prediction," Qiu *et al.* propose an intelligence traffic prediction system to efficiently allocate the V2X communication resources. This system is built based on combining the topological graph convolutional network with a sequence-to-sequence framework. In the article entitled "A convolution bidirectional long short-term memory neural network for driver emotion recognition," Du *et al.* propose a deep learning framework named Convolution Bidirectional Long Short-term Memory Neural

Network (CBLNN) to effectively recognize drivers' emotions. The proposed method predicts the emotions based on the geometric features extracted from facial skin information and the heart rate extracted from changes in RGB components.

In the article entitled "AI empowered communication systems for intelligent transportation systems," Lv *et al.* use a back-propagation neural network model to improve the predictions of the number of vehicles passing at intersections. In the article entitled "ICN-based enhanced cooperative caching for multimedia streaming in resource constrained vehicular environment," Gupta *et al.* propose a cooperative caching scheme in hierarchical network architecture that jointly considers cache location as well as combined content popularity and predicted future rating score while making a caching decision. The proposed scheme uses modified weighted clustering algorithms for the selection of cluster heads which are then used to decide cache location. A probability matrix is used to compute content caching probability which considers both popularity and predicted future rating of content.

With the advancement of communication technology and location acquisition technology in the context of modern smart cities, the sharing bike systems offer users great autonomy and convenience for the last/first-kilometer trip. However, due to the skewed and imbalanced bike usages for stations located at different places, it is of great significance yet very challenging to predict the potential destinations of each individual trip beforehand so that the service providers can better schedule manual bike re-dispatch in advance. To address this issue, Wang *et al.* propose an attention-based deep learning framework for trip destination prediction in the article entitled "An attention-based deep learning framework for trip destination prediction of sharing bike." In the article entitled "Short-term prediction of urban rail transit passenger flow based on LSTM-LGB-DRS," Jing *et al.* propose an LGB-LSTM-DRS model for short-term prediction of urban rail transit passenger flow in an external passenger transport hub. The model selects DRS as the dynamic regression device to fuse the Long-Short-Term Memory (LSTM) network model and the lightweight implementation of the algorithm GBM to achieve a local optimal fusion prediction.

Over the past decade, along with a widespread adoption of smartphones, crowdsourced navigation has become a prevalent automobile navigation solution. In the article entitled "Sybil attack identification for crowdsourced navigation: A self-supervised deep learning approach," Yu proposes a deep generative model based on Bayesian deep learning for the detection of Sybil attacks. The proposed model exploits time-series features to embed trajectories in a latent distribution space, which serves as a basis for identifying ones generated by Sybil attacks. In the article entitled "Reinforcement learning based advertising strategy using crowd sensing vehicular data," Lou *et al.* investigate a dynamic advertising problem for digital roadside billboards. To deal with the dynamic advertising problem, the authors consider many factors including potential customers' mobility patterns and their preferences, which are extracted using crowd sensing vehicular data. The proposed advertising strategy based on multi-agent reinforcement learning can train each digital billboard to switch different advertisements for different situations so that the influence of advertisements can be improved and the advertiser could obtain maximal commercial profit.

In the article entitled "A deep learning-based mobile crowd sensing scheme by predicting vehicle mobility," Zhu *et al.* address the problem of vehicle recruitment by proposing a deep learning-based scheme to collect sensing data in the urban environment and deep-learning-based offline algorithm to predict vehicle mobility in a future time period. The method uses a greedy online algorithm to recruit a subset of vehicles with a limited budget. In the article entitled "AI-enabled fingerprinting and crowd source-based vehicle localization for resilient and safe transportation systems," Shit *et al.* propose a crowdsource-based localization system to address the radio map building problem in fingerprinting localization system. In this method, the first initial radio map is constructed from the path-loss RSS model, followed by the update of the fingerprints with crowdsourcing. Finally, the vehicle location is estimated from the RSS sample by matching it with an updated radio map with a deep-learning algorithm.

In the article entitled "Online performance prediction of perception DNNs by multi-task learning with depth estimation," Klingner *et al.* propose an online performance prediction method for DNNs carrying out computer vision tasks in ITS. In the article entitled "Enhancing transferability of deep reinforcement learning-based variable speed limit control using transfer learning," Ke *et al.* utilize transfer learning to enhance the transferability of a deep reinforcement learning-based variable speed limits control strategy aiming to reduce freeway travel time. In the article entitled "MASR: Multi-aspect-aware session-based recommendation for intelligent transportation services," Zhang *et al.* propose a multi-aspect aware session-based recommendation for comprehensively and accurately capturing the user intention. In the article entitled "Optimal distribution of workloads in cloud-fog architecture in intelligent vehicular networks," Abbasi *et al.* optimize the power consumption of edge systems and reduce delays in the processing of workloads using a genetic algorithm.

In the article entitled "A highly efficient vehicle taillight detection approach based on deep learning," Li *et al.* propose an end-to-end framework that locates the rear brake and turn signals from a video stream in real-time. The system adopts the fast YOLOv3-tiny as the backbone model and makes three improvements to increase the detection accuracy on taillight semantics; that is, additional output layer for multi-scale detection, spatial pyramid pooling module for richer deep features, and focal loss for alleviation of class imbalance and hard sample classification. Since understanding the surrounding scenes is one of the fundamental tasks in ITS, Zhang *et al.* conduct an extensive empirical study on the performance of state-of-the-art scene text detection and recognition algorithms, in the article entitled "Street view text recognition with deep learning for urban scene understanding in intelligent transportation systems."

In the article entitled "N^2C: Neural network controller design using behavioral cloning," using a deep learning framework, Azam *et al.* propose a robust controller using behavioral cloning and motion planning of autonomous vehicle. In the

article entitled "Efficient and secure routing protocol based on artificial intelligence algorithms with UAV-assisted for vehicular *ad hoc* networks in intelligent transportation systems," Fatemidokht *et al.* propose a routing protocol by studying the operation of UAVs in ad hoc mode and their cooperation with other vehicles in VANETs.

As Guest Editors, we would like to convey our heartiest gratitude to all the authors who submitted their contributions and to the highly qualified anonymous reviewers for dedicating their efforts in completing timely and constructive reviews. We would also like to thank Prof. Azim Eskandarian, the Editor-in-Chief (EiC) of the IEEE Transactions on Intelligent Transportation Systems, for giving us the opportunity to organize this Special Issue and for all the encouragement, help, and support given throughout the process. Finally, a special thank you goes to Miriam Snyder, the Assistant to the EiC of the IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, for her continuous suggestions and technical support. We hope that this Special Issue will serve as a good reference for researchers, scientists, engineers, and academics in the fields of deep learning and intelligent transportation systems.

ALIREZA JOLFAEI, *Lead Guest Editor*
Department of Computing
Macquarie University
Sydney, NSW 2113, Australia
e-mail: alireza.jolfaei@mq.edu.au

NEERAJ KUMAR, *Guest Editor*
Department of Computer Science
and Engineering
Thapar Institute of Engineering and Technology
Patiala 147004, India
e-mail: neeraj.kumar@thapar.edu

MIN CHEN, *Guest Editor*
School of Computer Science and Technology
Huazhong University of Science and Technology
Wuhan 430074, China
e-mail: minchen@ieee.org

KRISHNA KANT, *Guest Editor*
Department of Computer and Information Sciences
Temple University
Philadelphia, PA 19122 USA
e-mail: kkant@temple.edu

Alireza Jolfaei (Senior Member, IEEE) received the Ph.D. degree in applied cryptography from Griffith University, Gold Coast, Australia. He has been a Faculty Member with Federation University Australia and Temple University, Philadelphia, PA, USA. He is currently the Program Leader of Master of IT in Cyber Security at Macquarie University, Sydney, Australia. He has participated in several projects involving different aspects of cybersecurity. On these topics, he has published over 80 articles appeared in journals, conference proceedings, and books. His main research interests include cyber and cyber-physical systems security. He has received multiple awards for academic excellence, University contribution, and inclusion and diversity support. He received the prestigious IEEE Australian Council Award for his research article published in the IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY. He served as the Chairman for the Computational Intelligence Society in the IEEE Victoria Section and for Professional and Career Activities for the IEEE Queensland Section. He has served as the Program Co-Chair and a Technical Program Committee Member for major conferences in cybersecurity, including IEEE TrustCom. He has served as a Guest Associate Editor for IEEE journals and TRANSACTIONS, including the IEEE INTERNET OF THINGS JOURNAL (IoT-J) and IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS. He is a Distinguished Speaker of the Association for Computing Machinery (ACM) on the topic of cybersecurity.

Neeraj Kumar received the Ph.D. degree in computer science and engineering from Shri Mata Vaishno Devi University, Katra, India, in 2009. He was a Post-Doctoral Research Fellow with Coventry University, Coventry, U.K. He is currently working as a Professor with the Department of Computer Science and Engineering, Thapar Institute of Engineering and Technology (Deemed to be University), Patiala, India. He has guided many research scholars leading to Ph.D. and M.E./M.Tech. He has published more than 300 technical research articles in top-cited journals, such as IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING (TKDE), IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING (TDSC), IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS (TITS), IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS (TII), and IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY (TVT). He has edited more than ten journals special issues of repute and published four books from CRC, Springer, IET, U.K., and BPB publications. He has won the Best Papers Award from IEEE SYSTEMS JOURNAL and ICC 2018, Kansas City, in 2018. His research was supported by funding from UGC, DST, CSIR, and TCS. He is an Associate Technical Editor of *IEEE Communications Magazine* and *IEEE Network Magazine*. He is an Associate Editor of *IJCS* (Wiley), *JNCA* (Elsevier), *Computer Communications* (Elsevier), and *Security and Communication Networks* (Wiley). He has been a Guest Editor of various international journals of repute, such as IEEE ACCESS, *IEEE Communication Magazine*, *IEEE Network Magazine*, *Computer Networks* (Elsevier), *Future Generation Computer Systems* (Elsevier), *Journal of Medical Systems* (Springer), *Computer and Electrical Engineering* (Elsevier), *Mobile Information Systems*, *International Journal of Ad Hoc and Ubiquitous Computing*, *Telecommunication Systems* (Springer), and *Journal of Supercomputing* (Springer). He has more than 18 000 citations to his credit with a current H-index of 75.

Min Chen (Fellow, IEEE) was an Assistant Professor with the School of Computer Science and Engineering, Seoul National University (SNU). He was a Post-Doctoral Fellow with SNU for one and half years. He worked as a Post-Doctoral Fellow with the Department of Electrical and Computer Engineering, The University of British Columbia (UBC) for three years. He is currently a Full Professor with the School of Computer Science and Technology, Huazhong University of Science and Technology (HUST). He is also the Director of the Embedded and Pervasive Computing (EPIC) Laboratory, HUST. He has more than 300 paper publications, including more than 200 SCI papers, more than 80 IEEE TRANSACTIONS/journal articles, 18 ISI highly cited papers, and eight hot papers. He has published eight books. His Google Scholar Citations reached more than 28 000 with an H-index of 83. His top article was cited more than 2000 times. His research interests include cyber physical systems, the IoT sensing, 5G networks, mobile cloud computing, SDN, healthcare big data, media cloud privacy and security, body area networks, and emotion communications and robotics. He received the Best Paper Award from QShine 2008, IEEE ICC 2012, ICST IndustrialIoT 2016, and IEEE IWCMC 2016. He received the IEEE Communications Society Fred W. Ellersick Prize in 2017. He was selected as a Highly Cited Researcher in 2018. He is the Chair of the IEEE Computer Society (CS) Special Technical Communities (STC) on Big Data. He is the Co-Chair of IEEE ICC 2012-Communications Theory Symposium and IEEE ICC 2013-Wireless Networks Symposium. He is the General Co-Chair of IEEE CIT-2012, Tridentcom 2014, Mobimedia 2015, and Tridentcom 2017.

Krishna Kant (Fellow, IEEE) received the Ph.D. degree in mathematical sciences from The University of Texas at Dallas in 1981. He was a Research Professor with the Center for Secure Information Systems, George Mason University. He served in industry for 18 years at Intel, Bellcore, and Bell Labs, and ten years in academia at Penn State and Northwestern University. From 2008 to 2013, he served as the Program Director of the NSF, where he managed the Computer Systems Research Program and was instrumental in the development and running of NSF-wide sustainability initiative named science, engineering and education for sustainability (SEES). He carries a combined 40 years of experience in academia, industry, and government. He is currently a Professor with the Department of Computer and Information Science, Temple University, Philadelphia, PA, USA, where he directs the IUCRC Center on Intelligent Storage. He has published in a wide variety of areas in computer science and authored a graduate textbook on performance modeling of computer systems. His research interests include energy efficiency, robustness, and security in cyber and cyber-physical systems.