Guest Editorial Introduction to the Special Section on AI-Driven Cybersecurity for Healthcare Cyber Physical Systems

WITH the gradual integration of Internet of Things (IoT), healthcare industry has become ubiquitous, complex, sophisticated, efficient and autonomous. With this technological shift, remote patient monitoring, smart sensing and seamless integration of medical equipments has become a reality. Thus, the modern day cyber physical systems (CPS) encompassing healthcare devices, medical equipments, intelligent implantable medical devices (IMDs), smart sensors, wearables, etc., have gained the attention of both the academia and industry. The CPS specific to healthcare systems are characterised by bundle of opportunities for both the pro-consumers (patients and their relatives) and the service providers (doctors and hospitals). The major advantages range from proactive treatment, faster disease diagnosis, and improved treatment to cost reduction, error reduction, and easier equipment and drug management.

Nevertheless, the integration of IoT with healthcare is not just limited to the above mentioned opportunities, but is also bounded by various deficiencies namely interoperability, security and high assurance. Amongst these challenges, one of the most concerning threat facing the healthcare-based CPS is implementing apt security measures. This is because the connected CPSs capture heterogeneous and humongous data including the sensitive content (such as names, social security numbers, home addresses and dates of birth); which in turn requires deployment of intelligent and sophisticated security solutions. Sharing the secure data with other medical devices further exaggerates the challenges for IT professionals. Further, the risks associated with IoT have witnessed a major surge particularly in the healthcare space; relative to any other consumer spaces.

Because of these reasons, both the IT and healthcare administrators still remain vigilant in extending the concept of IoT to healthcare domain. For instance, hackers are leveraging latest and creative ways to surface different attack vectors and compromise the medical equipments. One of the widely used methods is exploiting the error messages for gaining deeper insights about the healthcare CPSs and connected devices. Another prevalent technique is discovering and launching zero day attacks. These attack vectors are predominantly known for their unknown behaviour with latest signatures often unavailable in the attack database. Thus, the installation of conventional intrusion detection and prevention system (IDS/IPS) with access control mechanisms often fall short to detect such life threatening attacks. Sometimes, the breach of sensitive medical records could mean the difference between life and death. While at other instances, it may manifest identity theft attacks by revealing the highly sensitive data to the hackers. Such attack vectors may allow an adversary to gain illegitimate access to person's health insurance data and thereby exposing the risk to obtain expensive medical services, prescription medications, equipments, etc.

Thus, to ensure highly secure and uninterrupted services in the healthcare-based CPSs, it is essential to devise more advanced and intelligent techniques. One of the latest trends involves artificial intelligence (AI)-driven technologies that allow seamless management of heterogenous data while designing highly decisive attack patterns to accurately foresee hacker's behaviour. Additionally, game-theoretic approaches have also surfaced as eminent candidates for cyber defence to optimally address complex decision making problems. These problems involve appropriate classification of participating agents (known as players) as legitimate or illegitimate entities. This special section aims to bring together leading researchers, both from academia and industry, to share their visions, challenges, recent findings and advances related to the application of AI-based cyber security for Big Data-driven smart healthcare ecosystem. It is interesting to note that the call for papers received an especially strong response from the community, further attesting the rapid development of this scientific area. We hope these articles will show their value over time, while being immediately helpful for our current readership. We summarize the accepted articles in this editorial as follows.

The work "A Novel Homomorphic Encryption and Consortium Blockchain-based Hybrid Deep Learning Model for Industrial Internet of Medical Things", by Ali et al. proposes a hybrid-deep learning based homomorphic encryption model for industrial internet of medical things using consortium blockchain, providing the facility to train the data in the cloud and deploy the train model into the blockchain edge app.

The paper "An Efficient Hybrid Deep Learning Model for Denial of Service Detection in Cyber Physical Systems" by Ankita et al. uses convolutional layers combined with bidirectional long short term memory (LSTM) for detecting and classifying DoS attacks.

The paper "Intelligent Task Scheduling Approach for IoT Integrated Healthcare Cyber Physical Systems" by Nagarajan et al. presents an IoT-based healthcare cyber-physical system framework that uses multi-objective heuristic approach to provide effective resource utilization and task scheduling

Digital Object Identifier 10.1109/TNSE.2023.3293694

methodology while minimizing execution cost in Fog-cloud based healthcare setup.

The paper "Secure and Privacy-Preserving Human Interaction Recognition of Pervasive Healthcare Monitoring" authored by Yang et al. proposes a framework of the skeleton-based Human Interaction Recognition of Pervasive Healthcare Monitoring (HIR-PHM) under secure Edge-Fog-Cloud computing (EFCC) to manage the computation and storage resources allocation, latency, cyber-attack, and privacy-preserving simultaneously.

The paper "When Collaborative Federated Learning Meets Blockchain to Preserve Privacy in Healthcare" authored by Abou El Houda et al. presents design a decentralized and secure collaborative framework for healthcare system. First, the authors developed an approach that uses Secure Multiparty Computation (SMPC) scheme to securely aggregate local model updates. Then, they have proposed blockchain based scheme to facilitate/maintain the collaboration among clinician collaborators in a fully decentralized, trustworthy, and flexible way.

The paper "Blockchain-Enabled Cybersecurity Efficient IIoHT Cyber-Physical System for Medical Applications" by Lakhan et al. introduced a cost-efficient blockchain task scheduling cyber physical system with different heuristics where all the tasks are sorted, scheduled, and stored in a secure form to detect any kind of known or unknown attack in the blockchain network.

The paper "Semantic-driven Efficient Distributed Service Network towards Smart Healthcare System in Intelligent Fabric" by Xiao et al. presents a safety and healthcare system based on intelligent fabric, which supports the safe transmission of information flow in fabric space constructed by a variety of flexible sensors. Here, a semantic communication network for healthcare data flow was established that can encode information for different monitoring applications in order to protect the original data.

The article titled "Data Analytic for Healthcare Cyber Physical System" by Gan et al. proposes a contiguous negative sequential pattern mining algorithm called CNSPM to discover and analyze insightful and meaningful negative sequential patterns from the data collected by AI-powered healthcare CPS. Different from the current negative sequential pattern mining algorithms, CNSPM not only consider the time event time continuity, but also take account into the tolerance and concern interval.

The paper "Blockchain-Powered Tensor Meta-Learning-Driven Intelligent Healthcare System with IoT Assistance" by Ren et al. proposes a blockchain-powered tensor meta-learning-driven intelligent healthcare system with the aid of IoT devices to achieve secure and intelligent healthcare services. To alleviate the problem of limited labeled healthcare data, a tensor-prototype graph network was devised to capture the distribution of few-shot data.

The work "Smart Collaborative Evolvement for Virtual Group Creation in Customized Industrial IoT" by Song et al. predicted an intelligent and flexible medical professional network, which integrated two different fields of network structure and community detection. From device location algorithm to location data fusion, the relation of devices was further depicted, and the virtual community analysis was constructed.

The paper "Resource-Efficient Authenticated Data Sharing Mechanisms for Smart Wearable Systems" by Tanveer et al. present an authenticated key encryption scheme, which uses hash function and elliptic curve cryptography for protecting the information. The proposed scheme provides information security and users' anonymity by utilizing a session key between users and cloud server.

The paper "Recurrent Semantic Learning-driven Fast Binary Vulnerability Detection in Healthcare Cyber Physical Systems" by Yi et al. proposes a vulnerability detection scheme for Healthcare cyber physical systems (HCPS) Software. In this method, the logical representation of the program execution state of each HCPS software was defined as "programframe". On this basis, a Cascaded Long Short Time Memory network was designated to learn the program frame semantic features of the software, which implements recurrent semantic learning. And also, a fully connected neural network was trained to efficiently classify these program frame features into corresponding vulnerability types.

The paper "A secure information transmission protocol for healthcare cyber based on quantum image expansion and Grover search algorithm" by Qu et al. presents a new information security transmission protocol for healthcare, which can be used for large-scale data transmission. Here, the quantum image expansion technology and Grover search algorithm were used to ensure the large capacity of the protocol.

The paper "IRS-driven Cybersecurity of Healthcare Cyber Physical Systems" by Ji et al. proposes a basic framework of medical data privacy protection based on cloud platform and solves the problem of improving the confidentiality rate by deploying passive Intelligent reflective surface (IRS) to enhance wireless network transmission in the medical and healthcare field.

Iqbal et al. in "RThreatDroid: A Ransomware Detection Approach to Secure IoT based Healthcare Systems" proposed a novel hybrid ransomware detection method that analyzes image data, text, and application code to extract plain or encrypted threat text. The developed hybrid approach utilizes both the static and dynamic analysis along with the multi-machine learning classifier models to detect the ransomware, which was further utilized in Android platform.

Shen et al. in "DeformableGAN: Generating Medical Images with Improved Integrity for Healthcare Cyber Physical Systems" established an image generation method for GANs to eliminate checkerboard artifacts. The proposed deformable convolutional layer is interesting for the irregular shape of convolutional kernel which could benefit medical imaging for AI-driven cyber physical systems.

In "Healthcare Data Security using Lightweight Protocol for Cyber Physical System", Roy et al. proposes a lightweight data security technique for sharing information in real time. The model works in two phases: first, it fragments the original data into a random number of partitions, and second, the partition sequence is again altered with the randomized algorithm. The two working steps make it completely random for the attacker and hence tough to get the exact sequence.

The paper "Get your Foes Fooled: Proximal Gradient Split Learning for Defense against Model Inversion Attacks on IoMT data" by Khowaja et al. focuses on the privacy preservation from model inversion attacks by proposing a modified split network (PGSL). Authors used jacobian-saliency map based attacks to corrupt the input images and use proximal gradient to restore them while the training process continues. The novel part is the use of proximal gradient method to recover gradient maps and a decision-level fusion strategy to improve the recognition performance.

The paper "A N2CNN-based Anomaly Detection Method for Cardiovascular data in Cyber-Physical System" by Pal et al. proposes a novel NSGA-II based Convolution Neural Network for efficient anomaly detection on the Internet of Medical Things. The proposed method leverages the strength of a multi-objective meta-heuristic algorithm and non-dominated sorting genetic algorithm to optimize the hyper-parameters of the CNN with three objective functions namely, accuracy, precision, and recall.

The paper "Ensemble Learning-based Atrial Fibrillation Detection from Single Lead ECG Wave for Wireless Body Sensor Network" by Liu et al. proposes an ensemble learning-based algorithm which uses wireless body sensor networks (WBSN's) collected electrocardiograph (ECG) waves for atrial fibrillation (AF) detection. The developed algorithm includes two modules. First, denoised 1-D time series (ECG), time-frequency spectrum and Poincare plot are used to train three component learners through a parallel style, respectively, and each component learner produces four probability values. Then, all the outputs are combined using a weighted matrix constructed by a Bayesian optimization algorithm, which is capable of obtaining the final classification result.

The paper "QR-PUF: Design and Implementation of A RFID-based Secure Inpatient Management System Using XOR-Arbiter-PUF and QR-Code" by Gope et al. proposes an PUF-based authentication protocol for Mobile-RFID systems. To develop the protocol, they use the popup to model an XOR Arbiter-PUF inside the RFID devices and extract the PUF output to generate a secure QRCode through the mobile device attached with the RFID tag. In this way, the tag proves its legitimacy to the server.

The paper "TKAGFL: Federated Communication Framework Under Data Heterogeneity" by Pei et al. presented a new federated learning framework called TKAGFL. They used conditional GAN for data heterogeneity (processing the non-IID data), improved homomorphic encryption to balance data-sharing and privacy-protection, and AdaGard and top-K algorithm for compressing communication parameters to improve communication efficiency.

Peng et al. in "Mobility and Privacy-Aware Offloading of AR Applications for Healthcare Cyber-physical Systems in Edge Computing" investigate the computation offloading problem for AR applications in MEC-based healthcare CPSs and propose an offloading decision method based on a multi-objective algorithm to optimize time consumption, energy consumption, and load balancing.

Cao et al. in "Secure and Intelligent Service Function Chain for Sustainable Services in Healthcare Cyber Physical Systems" studies the problem of secure and dynamic SFC deployment and resource allocation based on intelligent algorithm for healthcare CPS. Then an intelligent and secure algorithm was proposed to solve the SFC deployment and resource allocation problems in the underlying healthcare CPS. The proposed intelligent algorithm was designed for dynamically coming slice requests and avoiding the effect of CPS failure.

The paper "A Blockchain-empowered Federated Learning in Healthcare-based Cyber Physical Systems" by Liu et al. presents a blockchain-empowered Federated Learning (FL) framework to train models without data sharing across different institutes. Specifically, a distributed ledger is maintained by a task agreement committee which is composed by the institutional representatives who execute FL tasks. This work presents the potential to recycle the computational resources in blockchain consensus network which will be wasted otherwise.

The work "Design and Testbed Experiments of User Authentication and Key Establishment Mechanism for Smart Healthcare Cyber Physical Systems" by Wazid et al. proposes a lightweight remote user authentication and key establishment scheme which uses lightweight cryptographic operations, such as cryptographic one-way hash function. It allows a legitimate registered user to access the services of the smart healthcare system after the successful completion of all the steps. The security analysis of the proposed scheme was given to prove its security for various potential attacks.

The paper "Cloud-assisted Secure and Cost-effective Authenticated Solution for Remote Wearable Health Monitoring System" by Mahmood et al. proposes an authentication protocol for Health Monitoring Systems which exploit lightweight cryptographic primitives such as Hash operations. Here, the proposed protocol is suitable for resource-constrained devices as it requires the least computational and communication costs, besides providing appropriate resilience for different well-known security attacks. The authors have also used Physically Unclonable Function (PUF) to mitigate the chances of physical or cloning attacks on wearable devices.

The paper "An AI-enabled Hybrid lightweight Authentication Scheme for Intelligent IoMT based Cyber-Physical Systems" by Adil et al. presents a hybrid authentication model to address the security concerns in digital healthcare, which is constructed form IoT base CPS. Furthermore, this model leveraged supervised machine learning technique and Cryptographic Parameter Based Encryption and Decryption (CPBE&D) scheme to ensure the validation of these devices with secure transmission over the wireless communication channel.

The paper "A Malicious Mining Code Detection Method Based on Multi-Features Fusion" by Zhang et al. proposes a malicious mining code detection method based on feature fusion and machine learning. Here, static analysis and statistical analysis methods were used to extract multi-dimensional features and n-gram model and TF-IDF were deployed to extract the feature vectors for multi-dimensional text. In this way, the best feature

vectors along with other statistic features were extracted through the classifier to train detection model.

We hope that the readers will enjoy the articles picked for this special section and this special section will stimulate and encourage researchers to continue working on this emerging and exciting area.

SAHIL GARG, *Guest Editor*
École de Technologie Supérieure
Montréal H3C 1K3, QC, Canada
sahil.garg@ieee.org

YULEI WU, *Guest Editor*
University of Exeter
Exeter EX4 4PY, U.K.
y.l.wu@exeter.ac.uk

SHAHID MUMTAZ, *Guest Editor*
InterDigital, USA
smumtaz@av.it.pt

FABRIZIO GRANELLI, *Guest Editor*
University of Trento
38122 Trento, Italy
fabrizio.granelli@unitn.it

KIM-KWANG RAYMOND CHOO, *Guest Editor*
University of Texas at San Antonio
San Antonio, TX 78260 USA
raymond.choo@fulbrightmail.org

MIN CHEN, *Guest Editor*
Huazhong University of Science and Technology
Wuhan 430074, China
minchen2012@hust.edu.cn

Sahil Garg (Member, IEEE) is currently an AI/ML Architect with Ultra Communications, Montreal, Canada, and an Adjunct Associate Professor with the École de Technologie Supérieure, Canada. Prior to this, he was a Research professional with Resilient Machine Learning Institute (ReMI), Montreal, Postdoctoral Research Fellow with ÉTS, Montreal, and a MITACS Researcher with Ericsson, Montreal. He has contributed much research in the areas of machine learning, Big Data analytics, security and privacy, Internet of Things, and cloud computing. He has more than 90 publications in highly ranked journals and conferences, including more than 60 top-tier journal papers and more than 30 reputed conference articles. He was the recipient of the 2022 IEEE HITC Early Career Researcher Award, 2021 IEEE Systems Journal Best Paper Award, 2020 IEEE TCSC Award for Excellence in Scalable Computing (Early Career Researcher), and IEEE ICC best paper award in 2018 in Kansas City, Missouri. He is currently a Managing Editor of Springer's *Human-Centric Computing* and *Information Sciences* journal. He is also an Associate Editor for IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, Elsevier's *Applied Soft Computing*, and Wiley's *International Journal on Communication Systems*. He was also an Associate Editor for other reputed journals, like Elsevier's *Future Generation Computer Systems*, *IEEE Network Magazine*, and IEEE SYSTEMS JOURNAL. In addition, he is also the Workshops and Symposia Officer for the IEEE ComSoc Emerging Technology Initiative on Aerial Communications.

Yulei Wu received the B.Sc. degree (First Class Hons.) in computer science and the Ph.D. degree in computing and mathematics from the University of Bradford, Bradford, U.K., in 2006 and 2010, respectively. He is currently a Senior Lecturer with the Department of Computer Science, College of Engineering, Mathematics and Physical Sciences, University of Exeter, Exeter, U.K. His expertise is on intelligent networking, and his main research interests include computer networks, networked systems, software defined networks and systems, network management, and network security and privacy. He has authored or coauthored more than 50 research papers in prestigious journals, including J-SAC, TPDS, TMC, TNSE, and TNSM. He is an Associate Editor for IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT, IEEE TRANSACTIONS ON NETWORK SCIENCE AND ENGINEERING, and IEEE ACCESS, and the Area Editor of *Computer Networks* (Elsevier). He also organised several special issues with J-SAC, TII, TNSE, and TCCN. He is a Senior Member of ACM, and a Fellow of the HEA (Higher Education Academy).

Shahid Mumtaz received the master's degree in electrical and electronic engineering from the Blekinge Institute of Technology, Karlskrona, Sweden, and the Ph.D. degree in electrical and electronic engineering from the University of Aveiro, Aveiro, Portugal, in 2006 and 2011, respectively. He is an IET Fellow, IEEE ComSoc, and ACM Distinguished speaker. His work resulted in technology transfer to companies and patented technology. His expertise include 5G/6G wireless technologies using AI/ML and Digital Twin(VR/XR) tools and innovation path towards industrial and academic. He was a Senior 5G Consultant at Huawei and InterDigital, where he contributed to RAN1/RAN2 and looked after the university-industrial collaborative projects. He has more than 15 years of wireless industry/academic experience. From 2002 to 2003, he was with Pak Telecom as a System Engineer and with Ericsson and Huawei at Research Labs in Sweden from 2005 to 2006. Since 2011, he has been with the Instituto de Telecomunicações, where he is currently holds the position of Principal Researcher and adjunct positions with several universities across the Europe-Asian Region. He is the author of four technical books, 12 book chapters, more than 250 technical papers more than 170 Journals and Transactions, more than 90 Conferences, two IEEE best paper awards in the area of mobile communications. He has been supervising/co-supervising several Ph.D. and Master Students. He is working closely with leading R&D groups in the industry to transition these ideas to practice. He has secured funding of around 2 M Euro. He has organized 20 workshops as the Chair of IEEE prestigious conference, 22 special Issues as the Lead Guest Editor of IEEE Communication, Wireless Magazine, and JSAC and Transaction on Vehicular Technology. Dr. Mumtaz is also the Associate Editor of several IEEE Journals, Communication Magazine, Wireless Magazine, Transactions on Industrial Informatics, Transactions on Communication, and IoT Journals. In 2013, he was Co-General Chair of the 8th International Wireless Internet Conference - Symposium on Wireless and Vehicular Communication organized in Lisbon by IEEE and EAI societies. He will also be the General Chair of IEEE CAMAD 2021 in Porto, Portugal. He has been giving invited tutorials/talks in IEEE conferences and the mobile industry and invited lectures in different foreign universities. He is a Scientific Expert and Evaluator for Research Funding Agencies, such as EU, COST, and NSF China. He was the recipient of the 'Alain Bensoussan Fellowship in 2012. He was the recipient of the NSFC Visiting Researcher Fund for Young Scientist in 2017 from China. He was the recipient of the IEEE ComSoC Young Researcher Award, Founder and EiC of the *IET Journal of Quantum Communication*, EiC of *Alexandria Engineering Journal* – Elsevier, the Vice-Chair of Europe/Africa Region- IEEE ComSoc: Green Communications & Computing society and the Vice-Chair of IEEE standard on P1932.1: Standard for Licensed/Unlicensed Spectrum Interoperability in Wireless Mobile Networks.

Fabrizio Granelli (Senior Member, IEEE) is currently a Professor with the Department of Information Engineering and Computer Science, University of Trento, Trento, Italy, and IEEE ComSoc Director for Educational Services during 2018–2019. From 2012 to 2014, he was an Italian Master School Coordinator with the Framework of the European Institute of Innovation and Technology ICT Labs Consortium. He was ComSoc Director of Online Content during 2016-2017. He was the Dean of Education of the DISI Department for the period 2015-2017, and coordinator of the research and didactical activities on computer networks within the degree in Telecommunications Engineering. He was an advisor of more than 80 B.Sc. and M.Sc. theses and eight Ph.D. theses. He was IEEE ComSoc Distinguished Lecturer for 2012-2015 and Visiting Professor with the State University of Campinas (SP, Brazil) and with The University of Tokyo (Japan). He is author or co-author of more than 200 papers published in international journals, books and conferences in networking, with particular reference to performance modeling, cross-layering, wireless networks, cognitive radios and networks, green networking and smart grid communications. Starting from January 2017, he is an Associate Editor-in-Chief of the IEEE Communications Surveys and Tutorials Journal (IF=22-the HIGHEST among all computer science and telecommunications publications!). Prof. Granelli is the Area Editor of the IEEE TRANSACTIONS ON GREEN COMMUNICATIONS AND NETWORKS. Prof. Granelli is also the Chair of the IEEE Communications Society Technical Committee on Transmission, Access and Optical Systems, and was Chair of the IEEE ComSoc Technical Committee on Communication Systems Integration and Modeling.

Kim-Kwang Raymond Choo (Senior Member, IEEE) received the Ph.D. degree in information security from the Queensland University of Technology, Brisbane, QLD, Australia. He currently holds the Cloud Technology Endowed Professorship with The University of Texas at San Antonio, San Antonio, TX, USA. He is the Founding Co-Editor-in-Chief of ACM's Distributed Ledger Technologies: Research & Practice (from June 2021), the Founding Chair of IEEE Technology and Engineering Management Society's Technical Committee (TC) on Blockchain and Distributed Ledger Technologies, and is the Department Editor of IEEE TRANSACTIONS ON ENGINEERING MANAGEMENT, and an Associate Editor for IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, and IEEE TRANSACTIONS ON BIG DATA. He is an ACM Distinguished Speaker and IEEE Computer Society Distinguished Visitor during 2021–2023, and a Web of Science's Highly Cited Researcher. He is the recipient of the 2022 IEEE Hyper-Intelligence TC Award for Excellence in Hyper-Intelligence Systems (Technical Achievement award), the 2022 IEEE TC on Homeland Security Research and Innovation Award, the 2022 IEEE TC on Secure and Dependable Measurement Mid-Career Award, and the 2019 IEEE TC on Scalable Computing Award for Excellence in Scalable Computing (Middle Career Researcher).

Min Chen (Fellow, IEEE) has been a Full Professor with the School of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan, China, since February 2012. He has more than 300 publications, including more than 200 SCI papers, more than 100 IEEE Transactions/Journal papers, 34 ESI highly cited papers and 12 ESI hot papers. He has authored or coauthored 12 books. His Google Scholar Citations reached more than 28,880 with an h-index of 83 and i10-index of 252. His top paper was cited more than 3300 times. He was selected as Highly Cited Research at 2018, 2019 and 2020. His research interests include cognitive computing, 5G Networks, wearable computing, Big Data analytics, robotics, machine learning, deep learning, emotion detection, and mobile edge computing. He was the recipient of the IEEE Communications Society Fred W. Ellersick Prize in 2017, and IEEE Jack Neubauer Memorial Award in 2019. He is an Associate Editor for IEEE TRANSACTIONS ON BIG DATA, IEEE NETWORK, and IEEE TRANSACTIONS ON COGNITIVE COMMUNICATIONS AND NETWORKING. He was the Series Editor of IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS. He was also 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.