Guest Editorial Special Issue on Privacy and Security in Distributed Edge Computing and Evolving IoT

RECENT advances in artificial intelligence, edge computing, and big data have enabled extensive reasoning capabilities at the edge of the network. Edge servers are now capable of extracting meaningful intelligence from IoT nodes, which can benefit a very diverse set of IoT applications, including smart carrier and distribution networks (power, people, water, and food), smart agriculture and manufacturing, and healthcare and maintenance. Unfortunately, as the infrastructures become more intelligent, they also become more vulnerable to disruption due to cyberattacks and information leakage. Furthermore, the rich data gathering and analytics involved in driving the intelligent management substantially raise the stakes in terms of privacy violation of the people and organizations that it serves.

Data mining on genuine data could be harmful to data privacy. For example, data mining on time-series data taken from motion sensors, microphones, and GPS sensors could reveal users' activities, demographics, health conditions, relationships, attitudes, preferences, biases, etc., that they may not be willing to share otherwise. This could potentially lead to security and privacy concerns in many participatory and opportunistic crowdsensing applications, where a large group of individuals having mobile devices capable of sensing and computing collectively share data and extract information to measure, map, analyze, estimate, or infer any processes of common interest. Invariably, privacy preservation is not considered as an area of primary concern in data collection and analytics. This provides a fertile ground for malicious adversaries who are willing and often are incentivized to the game and exploit edge processing vulnerabilities.

This special issue was organized to provide a multiaspect up-to-date reference for solutions that leverage techniques and insights from the domains of artificial intelligence, edge computing, and big data to address privacy and security challenges in distributed edge computing and evolving IoT applications. We received in total 64 original submissions from various institutions all over the world. After a rigorous review process, 19 articles were accepted and are presented for inclusion in this special issue of the IEEE INTERNET OF THINGS JOURNAL. In the following, we introduce these articles and highlight their main contribution.

The special issue starts with the article titled "PAAL: A framework based on authentication, aggregation, and local differential privacy for Internet of Multimedia Things." This work adopts a three-layer privacy-preserving framework based on a multilevel edge computing architecture for IoT multimedia applications. The article shows that the proposed framework outperforms the existing frameworks in terms of node management, privacy preservation of sensitive information, and protection of the underlying network.

The article titled "Dynamic edge access system in IoT environment" addresses the existing problems in protocol library management, compilation services for access programs, and heterogeneous device node reconfigurations by making use of a novel dynamic edge access system. It shows that the proposed method has less redundancy and significantly reduced hardware costs compared to conventional systems.

An IoT architecture for smart homes is outlined in the article titled "Security and privacy of smart home systems based on the Internet of Things and stereo matching algorithms." The authors evaluate the data communication in smart home systems from both hardware and software point of view using a stereo matching algorithm. To enhance the security and privacy of users, the overall structure of a smart home is revised. The author's design has a low cost and high accuracy. It not only optimizes the performance of smart home systems but also improves the safety factor.

The article titled "Secure brain-to-brain communication with edge computing for assisting post-stroke paralyzed patients" investigates the security and privacy issues in the brain-to-brain communications and highlights the limitations of the existing systems. The authors suggest the use of a lightweight symmetric encryption algorithm to secure the transmission of the patient's brainwave information to the caregiver. The proposed method is computationally inexpensive.

To solve the security and privacy problem posed by the evolving mobile IoT applications, a real-time detection system for Android malware interacting with the native library is adopted in the article titled "SoProtector: Safeguard privacy for native SO files in evolving mobile IoT applications." The authors claim that compared to most tools of static analysis and most applications, the adopted system is able to detect more Android malware threats.

The problem of encrypted data retrieval in Industrial Internet of Things (IIoT) is addressed in the article titled "Privacy-preserving and pairing-free multirecipient certificateless encryption with keyword search for cloud-assisted IIoT." The authors propose a scheme for maintaining the privacy of the multirecipient keyword search function. They formally

Digital Object Identifier 10.1109/JIOT.2020.2980103

prove that their scheme achieves the indistinguishable security against keyword guessing attacks in the random oracle model. The authors claim that compared to the current literature, their scheme is more efficient in terms of computation efficiency.

The article titled "CB-CAS: Certificate-based efficient signature scheme with compact aggregation for Industrial Internet of Things environment" addresses the source authentication and message integrity issues in IIoT environments by making use of digital signature schemes. The authors use a compact aggregation to create a fixed-length compressed signature. Thus, an increase in the number of signatures does not affect the length of the compressed final signature. The article shows that the proposed scheme is computationally less expensive than other competitive schemes.

The article titled "IoT sensor numerical data trust model using temporal correlation" deploys a trust assessment model for numerical data of IoT sensors considering the temporal variation and correlation among data. The model uses a deep neural network with two different DCT-based feature sets and calculates the trust scores by fusing the classification decision and decision uncertainty using the Dempster–Shefar theory. The authors claim that their model outperforms a contemporary correlation-based approach and can accurately and consistently estimate trust scores for numerical data from IoT sensors.

The article titled "Highly anonymous mobility-tolerant location-based onion routing for VANETs" adopts a novel onion-based anonymous routing protocol for vehicular *ad hoc* networks. It works based on vehicle-to-vehicle communications and satisfies source, destination, and route anonymity. The proposed protocol introduces the concept of location-based dynamic relay groups. In this concept, vehicles dynamically form groups around specific locations to act as onion relays. The algorithm outperforms the classic onion-based solutions in terms of delivery ratio, delay, and the number of retransmissions.

The article titled "REVAMP^{2}T: Real-time edge video analytics for multicamera privacy-aware pedestrian tracking" adopts an integrated end-to-end IoT system to enable decentralized edge cognitive intelligence for situational awareness. The authors' experimental results show that the method outperforms the current state of the art in terms of accuracy and efficiency.

A new development for a recent reversible data hiding method for video synthetic aperture radar (ViSAR) sensors is presented in the article titled "Reliable data aggregation in Internet of ViSAR Vehicles using chained dual-phase adaptive interpolation and data embedding." The method makes data communications in ViSAR aerial networks more efficient, reliable, and faster.

The article titled "TGM: A generative mechanism for publishing trajectories with differential privacy" attempts to provide privacy guarantee for location-based services. Experiments show that the method is highly efficient particularly when the data cover a large metropolitan area.

The article titled "Joint optimization of offloading utility and privacy for edge computing enabled IoT" addresses the offloading problem by reducing the resource utilization of edge computing units and the time cost for task execution. This work describes a two-phase offloading strategy to obtain a tradeoff between utility and privacy.

The next article, titled "On the integration of blockchain to the Internet of Things for enabling access right delegation" addresses the issue of access right delegation for large-scale IoT systems using the blockchain technology. The proof of the concept prototype is tested using Ethereum blockchain. The evaluation results show the practical feasibility of the models for transferring of access rights in a secure and fine-grained level.

The article titled "Differentially private high-dimensional data publication in Internet of Things" presents a compressed sensing mechanism to address the challenges in differentially private high-dimensional data publication. This mechanism can minimize the overall error of query results under ϵ-differential privacy by injecting the minimum amount of noise into the compressed data. The authors claim that their proposed compressed sensing mechanism significantly outperforms the state-of-the-art differentially private mechanisms for high-dimensional data publication.

The article titled "Enabling efficient privacy-assured outlier detection over encrypted incremental data sets" presents a privacy-preserving outlier detection protocol targeting the encrypted incremental data set. The protocol leverages advanced cryptographic primitives to build several secure and efficient modules. In addition, it adopts a sliding window technique to ensure a practical performance during the update phase with new arrival data points. The authors provide a performance evaluation based on a real-world data set and demonstrate the accuracy and efficiency of their protocol.

The article titled "Lightweight privacy-preserving training and evaluation for discretized neural networks" explores a lightweight privacy-preserving training and evaluation scheme for discretized neural networks. In this scheme, the authors utilize a single key fully homomorphic data encapsulation mechanism, through which a series of atomic operations are devised as a building block. The formal security proof and performance evaluation confirm the efficiency and accuracy of the method.

The article titled "Preserving balance between privacy and data integrity in edge-assisted Internet of Things" addresses the balance between the data security tasks and computational efforts for performing security tasks by fulfilling three requirements of the IoT network, that is, preserving the privacy of the device users, the data integrity, and the low cost of computation in the edge-assisted IoT networks. The method is based on an extraction method and a biometric elliptic curve cryptography-based authentication algorithm.

The article titled "Decentralized self-enforcing trust management system for social Internet of Things" evaluates the trustworthiness of IoT devices as well as the users to prevent malicious entities from disseminating malicious content or causing network disruption. The proposed system adopts a homomorphic encryption system with the properties of decentralization, self-enforcement, and privacy preservation. The proposed system assures correct computation, privacy,

and security of users even in the presence of malicious parties and colluding users.

While these 19 accepted articles made a significant contribution to various topics related to privacy and security in distributed edge computing and evolving IoT, numerous challenges remain, given the evolving nature of these topics that need to be addressed. As guest editors, we would like to convey our heartiest gratitude to all the authors who have submitted their knowledgeable contributions and to the highly qualified anonymous reviewers. We would also like to thank Prof. H. Wang, the Editor-in-Chief (EiC) of the IEEE INTERNET OF THINGS JOURNAL, and the former EiC Prof. S. Shen for giving us the opportunity to organize this special issue and for all the encouragement, help, and support given throughout the process.

ALIREZA JOLFAEI
Department of Computing
Macquarie University
Sydney, NSW 2109, Australia

POUYA OSTOVARI
Charles W. Davidson College
of Engineering
San Jose State University
San Jose, CA 95192 USA

MAMOUN ALAZAB
College of Engineering,
IT and Environment
Charles Darwin University
Casuarina, NT 0810, Australia

IQBAL GONDAL
School of Science, Engineering
and Information Technology
Federation University Australia
Mt. Helen, 3355 VIC, Australia

KRISHNA KANT
Department of Computer
and Information Sciences
Temple University
Philadelphia, PA 19122 USA

Alireza Jolfaei (Senior Member, IEEE) received the Ph.D. degree in applied cryptography from Griffith University, Gold Coast, QLD, Australia.

He is a Lecturer (Assistant Professor in North America) and a Program Leader of cyber security with Macquarie University, Sydney, NSW, Australia. Before this appointment, he worked as an Assistant Professor with Federation University Australia, Ballarat, VIC, Australia, and Temple University, Philadelphia, PA, USA. He has authored over 70 peer-reviewed articles on topics related to cyber security. His current research areas include cyber and cyber–physical systems security.

Dr. Jolfaei received the prestigious IEEE Australian Council Award for his research paper published in the IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY. He received a recognition Diploma with a cash award from the IEEE Industrial Electronics Society for his publication at the 2019 IEEE IES International Conference on Industrial Technology. He is the Founding Chair of the Federation University IEEE Student Branch. He served as the Chairman of the Computational Intelligence Society in the IEEE Victoria Section and also as the Chairman of Professional and Career Activities for the IEEE Queensland Section. He has served as the Guest Associate Editor for IEEE journals and transactions, including the IEEE SENSORS JOURNAL, the IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, the IEEE TRANSACTIONS ON INDUSTRY APPLICATIONS, the IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, and the IEEE TRANSACTIONS ON EMERGING TOPICS IN COMPUTATIONAL INTELLIGENCE. He has served over ten conferences in leadership capacities, including the Program Co-Chair, the Track Chair, the Session Chair, and a Technical Program Committee Member, including IEEE TrustCom and IEEE INFOCOM. He is a Distinguished Speaker of the ACM on the topic of cyber security.

Pouya Ostovari received the B.S. degree in software engineering from Shahid Beheshti University, Tehran, Iran, the M.S. degree from Amirkabir University of Technology (Tehran Polytechnic), Tehran, and the Ph.D. degree in computer and information sciences from Temple University, Philadelphia, PA, USA, in 2015.

He was an Assistant Professor of computer and information sciences with Temple University. He is currently an Assistant Professor with the College of Engineering, San Jose State University, San Jose, CA, USA. He published papers in distinguished journals and conferences, such as the IEEE/ACM TRANSACTIONS ON NETWORKING, the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, and IEEE International Conference on Mobile Ad Hoc and Sensor Systems. His current research interests include network coding, wireless networks, video streaming, IoT, and distributed systems.

Dr. Ostovari served as the Publicity Chair of the 14th IEEE International Conference on Advanced and Trusted Computing and as a TPC Member of numerous journals and conferences, including the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, the IEEE International Conference on Computer Communication and Networks, and the International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage. He also served as a reviewer of numerous prestigious journals and conferences, such as the IEEE/ACM TRANSACTIONS ON NETWORKING, the IEEE TRANSACTIONS ON SERVICES COMPUTING, the IEEE TRANSACTIONS ON COMMUNICATIONS, the IEEE International Conference on Computer Communications, the IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks, and the International Conference on Distributed Computing Systems.

Mamoun Alazab (Senior Member, IEEE) received the Ph.D. degree in computer science from the School of Science, Information Technology and Engineering, Federation University of Australia, Ballarat, VIC, Australia.

He is an Associate Professor with the College of Engineering, IT and Environment, Charles Darwin University, Casuarina, NT, Australia. He is a cyber security researcher and a practitioner with industry and academic experience. He published more than 150 research papers in many international journals and conferences, such as the IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, the IEEE TRANSACTIONS ON INDUSTRY APPLICATIONS, the IEEE TRANSACTIONS ON BIG DATA, the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, the IEEE TRANSACTIONS ON COMPUTERS, *Computers & Security*, *Future Generation Computing Systems*, and INFOCOM. He delivered many invited and keynote speeches, 24 events in 2019 alone. He convened and chaired more than 50 conferences and workshops. He works closely with government and industry on many projects. His research is multidisciplinary that focuses on cyber security and digital forensics of computer systems with a focus on cybercrime detection and prevention.

Dr. Alazab is the Founding Chair of the IEEE Northern Territory Subsection.

Iqbal Gondal received the Ph.D. degree in power line carrier communication systems from Victoria University, Melbourne, VIC, Australia.

He is the Director of the Internet Commerce Security Laboratory (ICSL), Federation University, Ballarat, VIC, Australia. ICSL conducts research in the application of advance analytics techniques for cybersecurity and provides innovative cybersecurity solutions to the industry. He is also working as a member of the University Governing Council, a member of the engineering advisory committee for Federation University, and the Non-Executive Director of the Oceania Cyber Security Centre and University engagement for the Defence Science Institute. He has been responsible for establishing collaborative partnerships between Federation University and Australian Cyber Security Centre and Australian Federal Police. He was the Director of ICT strategy for the faculty of IT in Monash. He has served in the capacity of the Director of Postgraduate studies for six years, a member of faculty board, and a member of Monash academic board. He has received significant industry funding to support research in ICSL in the area of intelligent malware analysis, threat intelligence, fraud detection, cyber-attack triage, malware webinject detection, phishing attack identification and mitigation, and blockchain. He has published over 164-refereed conference and journal papers. To date, he has successfully supervised 19 Ph.D. students. His research interests are cyber security, remote condition monitoring, and wireless and sensor networks information processing.

Dr. Gondal has received commendation from Vice-Chancellor and Pro-Vice-Chancellor (Learning and Teaching) for his excellent teaching in Monash. He is a member of the advisory board for the *International Journal for Distributed Sensors Networks* and an Editor of the *Journal of Information Processing in Agriculture*. He is a Fellow of the Institute of Engineers Australia and a Graduate Member of the Australian Institute of Company Directors.

Krishna Kant (Fellow, IEEE) received the Ph.D. degree in mathematical sciences from the University of Texas at Dallas, Richardson, TX, USA, in 1981.

He is currently a Professor with the Computer and Information Science Department, Temple University, Philadelphia, PA, USA, where he directs the IUCRC Center on Intelligent Storage. He was a Research Professor with the Center for Secure Information Systems, George Mason University, Fairfax, VA, USA. He served in industry for 18 years (at Intel, Bellcore, and Bell Labs) and ten years in academia (at Penn State University and Northwestern University). From 2008 to 2013, he served as a Program Director with 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. He carries a combined 40 years of experience in academia, industry, and government. He has published in a wide variety of areas in computer science, authored a graduate textbook on performance modeling of computer systems. His research interests span a wide range, including energy efficiency, robustness, and security in cyber and cyber–physical systems.