Digital Object Identifier 10.1109/ACCESS.2019.2940302

EDITORIAL

IEEE ACCESS SPECIAL SECTION EDITORIAL: RECENT ADVANCES IN COMPUTATIONAL INTELLIGENCE PARADIGMS FOR SECURITY AND PRIVACY FOR FOG AND MOBILE EDGE COMPUTING

Today, cloud computing services are undeniably becoming parts of modern information and communication systems in our daily lives. Cloud computing has proven to be an incredible technology for provisioning quickly deployed and scalable information technology (IT) solutions at reduced infrastructure costs. Cloud computing is unable to meet the requirements of low latency, location awareness, and mobility support. To solve this problem, researchers have introduced a trusted and dependable solution through fog and mobile edge computing (FMEC) to put the services and resources of the cloud closer to users, which facilitates the leveraging of available services and resources in the edge networks. Organizations are beginning to look at FMEC as the answer to the cloud computing problem. FMEC consists of putting micro data centers or even small, purpose-built high-performance data analytics machines in remote offices and locations in order to gain real-time insights from the data collected, or to promote data thinning at the edge, by dramatically reducing the amount of data that needs to be transmitted to a central data center. Without having to move unnecessary data to a central data center, analytics at the edge can simplify and drastically speed analysis while also cutting costs. FMEC pushes applications, data, and computing power (services) away from centralized points to the logical extremes of a network. FMEC replicates fragments of information across distributed networks of web servers, which may be vast. As a topological paradigm, edge computing is also referred to as mesh computing, peer-to-peer computing, autonomic (self-healing) computing, grid computing, and other names implying non-centralized, node-less availability.

However, FMEC services open a number of security and privacy issues and challenges. The concept of applying computational intelligence (CI) approaches in FMEC analysis for solving security and privacy issues is feasible and sound. Moreover, CI and its associated learning paradigms have played vital roles in a large number of application areas related to security and privacy in information systems. CI paradigm consists of various branches that are not limited to expert systems, artificial immune system, swarm intelligence, fuzzy system, neural network, evolutionary computing, and various hybrid systems, which are combinations of two or more of the branches. Security architects faced with these edge-heavy designs need to examine more feasible security architectures, such as boundary defense, in order to secure the edge infrastructure equipment. Security architects must also focus on the protection of data itself, often in many forms (pre-processed/processed) in order to safeguard customer-, employee-, and partner-sensitive information.

Researching the CI security, privacy, and trust components of an FMEC network—and how they differ from those corresponding modules in a traditional enterprise network—one must take into consideration how and why FMEC networks have evolved along a different evolutionary path. One of the unique qualities of an FMEC network architecture is its inherent ability to scale in order to accommodate the explosive growth of services that is expected. This Special Section starts to consider security, privacy, and trust in the context of FMEC network growth, as it is necessary to first research the security and privacy of these FMEC architectures and services. Network architectures vary depending on their purpose, for example, an enterprise network differs considerably from a data center network, in both topology and architectural design. Consequently, when we consider security in an FMEC context, the authors have to study the architectures and frameworks that are commonly in use today. The rationale behind this is simply that FMEC architectures have a different purpose than enterprise, consumer, or cloud networks. Indeed, FMEC networks can encompass features from all three, yet an FMEC network will support different devices, protocols, and purpose. There are challenges in coping with this, based on overall performance aspects of FMEC, including power consumption, connectivity, data security and privacy issues, and wireless networks, especially in sensor networks or the Internet of Things (IoT) networks. Therefore, it is helpful to take a high-level look at the evolution of the

FMEC architecture, why the topology came about and how it differs in technology and purpose to traditional network designs for service delivery.

The goal of this Special Section in IEEE Access is to bring together the state-of-art research and development on CI approaches for security and privacy of FMEC and secure FMEC services, novel attacks on FMEC services, and novel defenses for FMEC service attacks, and FMEC security analysis. We invited authors to contribute original research articles that would address the CI techniques leading to real-world FMEC challenges and future improvements for security and privacy for FMEC services. This Special Section of IEEE Access contains novel contributions aimed at fog and edge-based computing with an emphasis on security and privacy. The Special Section, with 22 articles selected on the basis of significance, originality, novelty, and presentation, is an outcome of substantial efforts from authors around the globe.

1. In the article "A fog based middleware for automated compliance with OECD privacy principles in Internet of Healthcare Things," Elmisery *et al.* provide a holistic privacy middleware for Internet of Healthcare Things (IoHT)-based healthcare services using fog nodes (personal gateways) as privacy enforcement points. Counting on this, a novel approach is where sensitive health data have two copies: a concealed version, which is located on the cloud-based healthcare recommender service side, and a plain version that is stored on the user's side or in his/her fog node. More precisely, the authors' approach for enhancing the user's privacy is to utilize the personal gateways at the end-user side as intermediate fog nodes between IoHT devices and cloud-based healthcare services. These fog nodes will host the proposed holistic privacy middleware and user's health profiles. The user's health data can be either kept private on his/her side, or released in a concealed form. The latter implies that health data is shared in a private manner after concealing it using a two-stage concealment process. The non-resource constrained feature of these fog nodes will unburden the constrained IoHT devices from performing intensive privacy-preserving processes.
2. In the article "From cloud to fog computing: a review and a conceptual live VM migration framework," Osanaiye *et al.* describe a fog computing architecture and review its different services and applications by discussing the security and privacy issues in fog computing, focusing on service and resource availability. Virtualization is a vital technology in both fog and cloud computing that enables virtual machines (VMs) to coexist in a physical server (host) to share resources. These VMs could be subject to malicious attacks or the physical server hosting it could experience system failure, both of which result in unavailability of services and resources. Therefore, a conceptual smart pre-copy live migration approach is presented for VM migration. Using this approach, the authors estimate the downtime after each iteration to determine whether to proceed to the stop-and-copy stage during a system failure or an attack on a fog computing node. This will minimize both the downtime and the migration time to guarantee resource and service availability to the end users of fog computing.
3. The article "Biometric security through visual encryption for fog edge computing," by Wadood *et al.* is concerned with developing a biometric security solution for face images, using visual cryptography and zero-watermarking, which does not adversely impact the visual quality of the image. The original face image is not modified through the zero-watermarking and visual encryption procedures and this in turn does not adversely impact the recognition rate. The problems related to security and privacy of biometric content are simpler to solve through edge computing resulting in improved security and privacy of biometric and other critically private information. Zero-watermarking has been proposed as a solution to help protect the ownership of multimedia content that is easy to copy and distribute. Visual cryptography is another approach to secure data shared through generating multiple shares.
4. In the article "Enabling far-edge analytics: performance profiling of frequent pattern mining algorithms," by Alam *et al.*, far-edge analytics enable data reduction in mobile environments, hence reducing the data transfer rate and bandwidth utilization cost for mobile-edge communication. In addition, far-edge analytics facilitate local knowledge availability to enable personalized mobile data stream mining applications. Existing literature mainly addresses classification and clustering problems in far-edge mobile devices, but the problem of frequent pattern mining (FPM) remains unexplored. This research presents the results of an experimental study on the performance profiling of FPM algorithms. The authors developed a real mobile application for performance analysis and profiling of 21 FPM algorithms with various real data sets in terms of execution time, storage complexity, sparsity, density, and data set size. According to the experimental results, large-sized data sets with high sparsity increase computational and storage cost in far-edge mobile devices. To address these issues, the authors propose a framework and discuss the relevant research challenges for seamless execution of FPM algorithms in MECC systems.
5. In the article "SAIDR: a new dynamic model for SMS-based worm propagation in mobile networks," Xiao *et al.* propose a worm propagation model based on short message service (SMS), named susceptible-affected-infectious-suspended-recovered. To accurately predict the worm propagation via SMS, first the affected state is added to represent the state

of users who have received the messages but have not clicked the malicious links. Second, since an infected node does not always send malicious messages to others, a novel state, the suspended state, is introduced to describe this situation. Furthermore, related stabilities of the worm-free equilibrium and the endemic equilibrium are studied. The worm-free equilibrium is locally and globally asymptotically stable if the basic reproduction number R0 < 1, whereas the endemic equilibrium is locally asymptotically stable if R0 > 1. Finally, comprehensive experiments were done to support the authors' conclusions and confirm the rationality.

6. The article, ''An attribute-based encryption scheme to secure fog communications,'' by Alrawais *et al.* discusses how fog computing is deemed as a highly virtualized paradigm that can enable computing at the Internet of Things devices, residing in the edge of the network, for the purpose of delivering services and applications more efficiently and effectively. Since fog computing originates from and is a non-trivial extension of cloud computing, it inherits many security and privacy challenges of cloud computing, causing extensive concerns in the research community. To enable authentic and confidential communications among a group of fog nodes, in this article, the authors propose an efficient key exchange protocol based on cipher text-policy attribute-based encryption (CP-ABE) to establish secure communications among the participants. To achieve confidentiality, authentication, verifiability, and access control, they combine CP-ABE and digital signature techniques. The authors analyze the efficiency of the protocol in terms of security and performance and also implement their protocol and compare it with the certificate-based scheme to illustrate its feasibility.
7. In the article ''Towards a secure mobile edge computing framework for Hajj,'' Rahman *et al.* discuss the cloud computing paradigm facing the challenges of providing low latency, high availability, and real-time location-aware services, where millions of people are mobile with respect to time and geographic location. In this article, the authors propose a mobile edge-computing framework that can support real-time, location-aware personalized services to a very large crowd. The framework uses a hybrid of cloud at the server end and fog computing terminals (FCTs) at the crowd edge. The concept of FCT is realized by adding a middle layer acting as a proxy between the user end and cloud infrastructure. Each FCT node covers a geographic zone and provides a subset of services and resources based on the geographic location of a mobile user. When a user moves from one FCT-covered zone to another, the secure handshaking of metadata about the user is shared with the new FCT node. The communication between mobile users' terminals, such as smartphone and the FCT, is assumed as 4G/5G networks, while the communication between the FCT and cloud is based on a high speed, always available, and reliable Internet connection. The location of each mobile user is made secure and shared according to a novel privacy policy paradigm. The framework is designed to switch between FCT and cloud, depending on the task, network condition, geographic nearness, and resources available within the client unit. The authors have implemented the framework to support context-aware services to millions of pilgrims that gather together in a very small area of land each year.
8. In the article, ''A survey on C-RAN security,'' Tian *et al.* discuss how 5G has initiated its full development to satisfy an increasing demand on mobile data traffic and big data bandwidth. Centralized data processing, collaborative radio, real-time cloud infrastructure, and cloud radioaccess network (C-RAN), along with their excellent advantages, are being sought by more and more operators to meet end-user requirements. As a promising mobile wireless network architecture, compared with traditional RAN, C-RAN has incomparable advantages in terms of low power consumption, reduced base station (BS) numbers, and economic capital and operating expenditure. It can also improve network capacity and BS utilization rate. Recently, C-RAN security has aroused special attention and concern. However, the literature still lacks an overall review on it in order to guide current and future research. In this article, the authors first overview the architecture, deployment scenarios, and special characteristics of C-RAN. The authors then provide a thorough review on the existing security studies in the field of C-RAN based on its three logic layers and corresponding security threats and attacks. Finally, the authors discuss whether the current literature can satisfy the expected security requirements in C-RAN.
9. In the article ''A secure trust model based on fuzzy logic in vehicular ad hoc networks with fog computing,'' Soleymani *et al.* explain how in vehicular ad hoc networks (VANETs), trust establishment among vehicles is important to secure integrity and reliability of applications. In general, trust and reliability help vehicles to collect correct and credible information from surrounding vehicles. On top of that, a secure trust model can deal with uncertainties and risk taking from unreliable information in vehicular environments. However, inaccurate, incomplete, and imprecise information collected by vehicles as well as movable/immovable obstacles have interrupting effects on VANET. In this article, a fuzzy trust model based on experience and plausibility is proposed to secure the vehicular network. The proposed trust model executes a series of security checks to ensure the correctness of the information received from authorized vehicles. Moreover, fog nodes are adopted as a facility to evaluate the level of accuracy of event's location.

The analyses show that the proposed solution not only detects malicious attackers and faulty nodes, but also overcomes the uncertainty and imprecision of data in vehicular networks in both line-of-sight and non-line-of-sight environments.

10. In the article, ''HIBS-KSharing: hierarchical identity-based signature key sharing for automotive,'' Wei *et al*. propose a novel and secure key-sharing system named hierarchical identity-based signature key sharing (HIBS-KSharing), which consists of key generation, key transmission, and key management (e.g., remote issuing, revocation of access rights, and their delegation to other users or sharers). The authors implemented a proposed system based on Nexus smartphones and near-field communication devices. Compared with existing key-sharing schemes of car rental/sharing, the proposed HIBS-KSharing system is secure and easily extended.
11. In the article ''An ensemble random forest algorithm for insurance big data analysis,'' Lin *et al*. exploit a heuristic bootstrap sampling approach combined with the ensemble learning algorithm on large-scale insurance business data mining, and propose an ensemble random forest algorithm that uses the parallel computing capability and memory-cache mechanism optimized by Spark. The authors collected the insurance business data from China Life Insurance Company to analyze the potential customers using the proposed algorithm. The authors use F-measure and G-mean to evaluate the performance of the algorithm. Experimental results show that the ensemble random forest algorithm outperformed support vector machine (SVM) and other classification algorithms in both performance and accuracy within the imbalanced data, and it is useful for improving the accuracy of product marketing compared to the traditional artificial approach.
12. The article, ''Fog intelligence for real-time IoT sensor data analytics,'' by Raafat *et al*., discusses the evolution of the Internet of Things and how the continuing increase in the number of sensors connected to the Internet imposes big challenges regarding the management of the resulting deluge of data and network latency. Uploading sensor data over the web does not add value. Therefore, an efficient knowledge extraction technique is needed to reduce the amount of data transfer and to help simplify the process of knowledge management. Homoscedasticity and statistical features extraction are introduced in this article as novelty detection enabling techniques, which help extract the important events in sensor data in real time when used with neural classifiers. Experiments have been conducted on a fog computing platform. System performance has also been evaluated on an occupancy data set and showed promising results.
13. In the article ''Hash based encryption for keyframes of diagnostic hysteroscopy,'' Hamza *et al*. address the problem of confidentiality of keyframes, which are extracted from diagnostic hysteroscopy data using video summarization. The authors propose an image color coding method aimed at increasing the security of keyframes extracted from diagnostic hysteroscopy videos. In this regard, the authors use a 2-D logistic map to generate the cryptographic key sequences, which relies on mixing and cascading the orbits of chaotic map in order to generate the stream keys for the encryption algorithm. The encrypted images produced by their proposed algorithm exhibit randomness behavior, providing a high level of security for the keyframes against various attacks. The experimental results and security analysis from different perspectives verify the superior security and high efficiency of the proposed encryption scheme compared to other state-of-the-art image encryption algorithms. Furthermore, the proposed method can be combined with mobile-cloud environments and can be generalized to ensure the security of cloud contents as well as important data during transmission.
14. In the article ''Fog computing over IoT: a secure deployment and formal verification,'' Zahra *et al*. discuss how fog computing, being an extension of cloud computing, has addressed some issues found in cloud computing by providing additional features, such as location awareness, low latency, mobility support, and so on. Its unique features have also opened a way toward security challenges, which need to be focused to make it bug-free for the users. This article focuses on overcoming the security issues encountered during the data outsourcing from fog client to fog node. The authors have added Shibboleth, also known as security and crossdomain access control protocol, between fog client and fog node for improved and secure communication between the fog client and fog node. Furthermore, to prove whether Shibboleth meets the security requirement needed to provide the secure outsourcing, the authors have also formally verified the protocol against basic security properties using high-level Petri net.
15. In the article ''A hesitant fuzzy based security approach for fog and mobile-edge computing,'' Rathore *et al*. introduce a soft hesitant fuzzy rough set (SHFRS) to solve multi-criteria decision-making problems. SHFRS is introduced as an innovative extension of the hesitant fuzzy rough set theory by fusing it with the hesitant fuzzy soft set. The authors describe the inverse hesitant fuzzy soft set that defines the inverse hesitant fuzzy relation to determine the SHFRS upper and lower approximation operators of any hesitant fuzzy subset in the given set of parameters. The authors also present different special cases of SHFRS upper and lower approximation operators and discuss some fundamental theorems based on approximation operators. In addition, the authors propose a novel solution

to multi-criteria decision-making problems based on SHFRS. Finally, the authors assess the proposed solution by applying it to a real-time multi-criteria decision-making problem of appropriate security service selection for FMEC in the existence of multi-observer hesitant fuzzy information.

16. In the article, ''A lightweight authenticated encryption scheme based on chaotic SCML for railway cloud service,'' by Zheng *et al*., the authors propose a lightweight authenticated encryption scheme with associated data based on a novel discrete chaotic S-box-coupled map lattice (SCML), which avoids the dynamic degradation of the digital chaotic system and low efficiency of the chaos-based cryptosystem. Based on the chaotic SCML, an authenticated encryption scheme that protects the confidentiality and integrity in one pass is presented in detail. The security analysis and performance simulations in software and hardware show that the proposed scheme is efficient and provides adequate security through authentication and encryption. Such a scheme could be used for applications in a railway cloud service that requires moderate security and low-cost implementations.
17. The article, ''K-anonymity location privacy algorithm based on clustering,'' by Zheng *et al*., discusses how the accuracy of user location information is inversely proportional to the user's privacy-preserving degree k, and is proportional to quality of query service. In order to balance the conflict between privacy-preserving security and query quality caused by the accuracy of location information, a clustering algorithm aiming at eliminating outliers based on the k-anonymity location privacy-preserving model is proposed, which is used to realize the establishment of anonymous group in the anonymous model. The distribution of the user in the anonymous group is optimized. The idea of replacing the user location query by the center of the anonymous group is proposed. The number of repeated queries is reduced, and the quality of query service is improved on the premise of ensuring security through the experimental analysis and comparison with other schemes.
18. In the article ''Joint cell activation and selection for green communications in ultra-dense heterogeneous networks,'' Zhou *et al*. discuss how the densification of small cells in heterogeneous networks (HetNets) causes huge energy consumption and severe network interference. To fully exploit the potential of new network architecture, the cell selection (CS) in such HetNets should couple with reducing power consumption and network interference. To this end, the authors jointly perform cell activation and selection (CAS) to maximize the network energy efficiency (EE) under users' long-term rate constraints. The formulated problem is in a mixed-integer fractional form and hard to tackle. It needs to be transformed into a parametric subtractive form, by which its solution is reached through a three-layer iterative algorithm. The first layer searches an EE parameter using a bisection method; the second layer alternately optimizes CAS indices; the third layer solves CS and cell activation (CA) problems using dual decomposition and fixed point iteration, respectively. At last, the authors give some complexity and convergence analyses for the designed algorithm, and investigate the impacts of different network parameters on system performance. The simulation results show that the CA introduced in CS is a good option to reduce energy consumption and network interference.
19. The article, ''A new algorithm for enumerating bent functions based on truth tables and run length,'' by Zhao *et al*., provides some properties of truth tables of bent functions. Bent functions are a class of Boolean functions with the maximum nonlinearity and strict avalanche criterion. Bent functions can effectively resist the optimal affine approximation attack and the differential attack, which play an important role in the design of various security infrastructures, such as S-box, stream ciphers, data security, etc. Furthermore, an upper bound of truth table's run length of a bent function is presented. Based on these results, the authors propose a new algorithm for enumerating bent functions. Finally, the authors find that their algorithm requires lower storage complexity and is easier to implement with parallel/distributed computing infrastructures by comparing with some known searching algorithms.
20. The article, ''Multi-semi-couple super-resolution method for edge computing,'' by Yang *et al*., discusses how video analyses based on edge computing typically need high-resolution video images, while, in practice, the resolutions of captured video images may not be high enough. Thus, super-resolution techniques are a possible solution with the input of low-resolution images. Sparse-coding-based super-resolution methods are well known for their efficiency. However, the current sparse-coding-based methods suffer from two major problems. First, the sparse coefficient of a low-resolution patch is assumed to be the same as the sparse coefficient of its corresponding high-resolution patch, which is too strict to deal with various patterns; second, the current methods only learn one pair of high-resolution and low-resolution dictionaries, while, since patches in images are diverse in the real world, it is difficult to use only one pair of dictionaries to cover all the possible patches. In this article, to overcome these two issues, the authors propose a super-resolution method to: 1) relax the assumption by linearizing the sparse coefficient of a low-resolution patch to that of a high-resolution patch and 2) minimize super-resolution errors by jointly partitioning training patches into several clusters and learning dictionaries. Experimental results validate that this algorithm achieves more faithful reconstructions.

21. In the article, "Secure quantum steganography protocol for fog cloud Internet of Things," by Abd El-Latif *et al*., the authors present a new framework for secure information in fog cloud IoT. In the framework, the user in one location embeds his/her valuable data via the proposed quantum steganography protocol and uploads the covered data to the fog cloud. The intended receiver in another location accesses the data from the fog cloud and extracts the intended content via the proposed extraction approach. This article also presents a novel quantum steganography protocol based on hash function and quantum entangled states since, to the best of the authors' knowledge, there is no prior quantum steganography protocol that authenticates an embedded secret message. In the suggested protocol, the hash function is utilized to authenticate embedded secret messages. The presented protocol is secure against well-known attacks, such as message, man-in-the-middle, and no-message attacks. In addition, it does not consume additional channels besides the proposed one to send a secret message or verify security. The proposed approach is nominated for use in FMEC.
22. The article "A service orchestration of optimizing continuous features using big data based fog-enabled Internet of Things," by Din *et al*., discusses how video-based surveillance pedestrian detection is playing a key role in emerging technologies, such as Internet of Things and Big Data, for use in smart industries and cities. In pedestrian detection, factors such as lighting, object collisions, backgrounds, clothes, and occlusion cause complications because of inconsistent classification. To address these problems, enhancements in feature extraction are required. These features should arise from multiple variations of pedestrians. Well-known features used for pedestrian detection involve histogram of gradients, scale-invariant feature transform, and Haar built to represent boundary level classifications. Occlusion feature extraction supports identification of regions involving pedestrian detection. Classifiers, such as support vector machine and random forests, are also used to classify pedestrians. All these feature extraction and pedestrian detection methods are now being automated using deep learning methods known as convolutional neural networks (CNNs). A model is trained by providing positive and negative image data sets, and larger data sets provide more accurate results when a CNN-based approach is used. Additionally, Extensible Markup Language cascading is used for detecting faces from detected pedestrians.

We understand that the above articles cannot cover all the aspects of security and privacy for FMEC. This Special Section intends to collect the latest research findings in addressing the key challenges, such as those mentioned above, and the future directions in leveraging security and privacy for FMEC. We hope that this selection of articles will stimulate further in-depth discussions and new contributions to the related areas. Finally, we would like to thank all authors for their submissions and all reviewers for their timely and professional reviews. We also acknowledge the guidance from the former IEEE ACCESS Editor-in-Chief, Professor Michael Pecht, and other staff members of IEEE ACCESS for their continuous support and guidance.

B. B. GUPTA, *Guest Editor*
National Institute of Technology Kurukshetra
Kurukshetra, India

YOGACHANDRAN RAHULAMATHAVAN, *Guest Editor*
Loughborough University
London, U.K.

SHINGO YAMAGUCHI, *Guest Editor*
Graduate School of Science and Engineering
Yamaguchi University
Japan

TYSON BROOKS, *Guest Editor*
Syracuse University
Syracuse, NY, USA

ZHENG YAN, *Guest Editor*
School of Cyber Engineering
Xidian University
Xi'an, China

B. B. GUPTA received the Ph.D. degree in information and cyber security from IIT Roorkee, India. He has published more than 150 research articles (including four books and 20 book chapters) in international journals and conferences of high repute, including the IEEE, Elsevier, ACM, Springer, and Inderscience. He is currently an Assistant Professor with the Department of Computer Engineering, National Institute of Technology, Kurukshetra (NIT Kurukshetra), India. His research interests include information security, cyber security, mobile/smartphone, cloud computing, web security, intrusion detection, computer networks, and phishing. He is also a member of ACM, SIGCOMM, SDIWC, the Internet Society, the Institute of Nanotechnology and a Life Member of the International Association of Engineers (IAENG) and the International Association of Computer Science and Information Technology (IACSIT). His biography was selected and published in *Who's Who in the World* (Marquis, 30th Edition, 2012). He has been selected to receive the 2017 Albert Nelson Marquis Lifetime Achievement Award and the 2017 Bharat Vikas Award from the Marquis *Who's Who in the World*, USA and ISR, and India, respectively. He also received the Sir Visvesvaraya Young Faculty Research Fellowship Award, in 2017, from the Ministry of Electronics and Information Technology, Government of India. He also received the 2018 Best Faculty Award for Research Activities, the 2018 Best Faculty Award for Project and Laboratory Development from NIT Kurukshetra, and the 2018 Rula International Award for Best Researcher. He has been serving as an Associate Editor for the IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS and IEEE ACCESS and an Executive Editor for IJITCA (Inderscience). He is also leading the *International Journal of Cloud Applications and Computing* (IJCAC) (IGI Global, USA) as the Editor-in-Chief. He has been serving as a Reviewer for the journals of the IEEE, Springer, Wiley, Taylor & Francis, and so on.

YOGACHANDRAN RAHULAMATHAVAN received the Ph.D. degree in signal and information processing from Loughborough University, London, U.K., in 2011. He was an Information Security Researcher with the City, University of London, from 2011 to 2016. He is currently a Lecturer and the Program Director of the MSc Cyber Security and Big Data Program at Loughborough University. He is also coordinating the U.K.–India project (worth £200k) among Loughborough University, IIT Kharagpur, and the City, University of London. His research interest includes developing novel security protocols to advance machine learning techniques to solve complex privacy issues in emerging applications, e.g., patient's healthcare data sharing, biometric authentication systems, and identity management in cloud. For more details, visit http://www.drrahul.uk/.

SHINGO YAMAGUCHI received the B.E., M.E., and D.E. degrees from Yamaguchi University, Japan, in 1992, 1994, and 2002, respectively. He was a Visiting Scholar with the Department of Computer Science, University of Illinois at Chicago, USA, in 2007. He is currently a Professor with the Graduate School of Sciences and Technology for Innovation, Yamaguchi University. His research interests include the area of net theory and its applications, including service science, big data analysis, the IoT, AI, and cyber security. He is also a Member at Large on the Board of Governors of the IEEE Consumer Electronics Society. He is also the Chair of the Young Professionals Committee of the IEEE Consumer Electronics Society.

TYSON BROOKS received the bachelor's degree in business administration/management from Kentucky State University, the master's degree in business administration from the Thomas More College, the master's degree in information and telecommunications systems from Johns Hopkins University, and the Ph.D. degree in information management from Syracuse University. He works for the U.S. Department of Defense (DoD). He is currently an Adjunct Professor with the iSchool, Syracuse University. He is responsible for information security, security engineering and cyber-assurance activities to identify systemic and/or critical misconfigurations, vulnerabilities, and unresolved threats to U.S. DoD networks. He is also a member of the Association of Computing Machinery (ACM), the International Information System Security Certification Consortium (ISC2), and the Information System Security Association (ISSA). He is also the Founder/Editor-in-Chief of the *International Journal of Internet of Things and Cyber-Assurance*, an Associate Editor of IEEE ACCESS, *Journal of Enterprise, Architecture*, *International Journal of Cloud Computing and Services Science* (IJ-CLOSER), and *International Journal of Information and Network Security* (IJINS), and a Reviewer of the IEEE INTERNET OF THINGS JOURNAL (IoT-J). He holds the Security+, the Certified Information System Security Professional (CISSP), the Certified Ethical Hacker (C|EH), the Certified Network Defense Architect (C|NDA), the Certified Enterprise Architect (CEA), the Certificate of Advanced Study (CAS) in Information Security Management (ISM), the Project Management Professional (PMP), and the Information Technology Infrastructure Library (ITIL) v.3. certifications.

ZHENG YAN (M'06–S'14) received the B.Eng. degree in electrical engineering and the M.Eng. degree in computer science and engineering from Xi'an Jiaotong University, Xi'an, China, in 1994 and 1997, respectively, the M.Eng. degree in information security from the National University of Singapore, Singapore, in 2000, and the Licentiate of Science and the Doctor of Science in Technology degrees in electrical engineering from the Helsinki University of Technology, Helsinki, Finland. She is currently a Professor with Xidian University, Xi'an, and a Visiting Professor and a Finnish Academy Research Fellow with Aalto University, Espoo, Finland. Her research interests include trust, security, privacy, and security-related data analytics. She also serves as the General or Program Chair for more than 30 international conferences and workshops. She is also a Steering Committee Co-Chair of the IEEE Blockchain International Conference. She is also an Associate Editor of many reputable journals, e.g., the IEEE INTERNET OF THINGS JOURNAL, *Information Sciences*, *Information Fusion*, JNCA, IEEE ACCESS, and SCN.

• • •