Digital Object Identifier 10.1109/ACCESS.2021.3075818

EDITORIAL

IEEE ACCESS SPECIAL SECTION EDITORIAL: SECURITY AND PRIVACY IN EMERGING DECENTRALIZED COMMUNICATION ENVIRONMENTS

Due to the COVID-19 epidemic, face-to-face team working has changed into distanced work from home. Modern, decentralized digital communication environments are changing with the availability of new technologies and the development of new real-world applications, which lead to novel challenges in security and privacy protection. 5G/6G mobile applications, the smart Internet of Things (IoT) devices, big data applications, and cloud systems are developing to better meet new requirements. Mobile–cloud architecture is emerging as 5G /6G mobile IoT devices are generating large volumes of data which need cloud infrastructure to process. Many IoT systems and cloud systems are decentralized, and new security and privacy protection solutions are emerging in decentralized networks. The increasing interdependence of IT solutions accepted by society has led to a sharp increase in data. As a result, the chances of data leakage or privacy infringement also increase, along with the need for new solutions for digital security and privacy protection.

This Special Section in IEEE Access aims to report highlighted security and privacy research in modern decentralized digital communication environments. The Special Section invited experts and scholars in the fields of digital security, so that readers can keep abreast of the latest developments in the industry and master the latest security technologies.

This Special Section attracted a good number of submissions; 166 articles were submitted, and in total 53 articles were finally accepted.

The invited article ''Covert channels in the MQTT-based Internet of Things,'' by Velinov *et al.*, presents the first comprehensive study of covert channels in the Internet of Things (IoT) environments by studying the network information hiding patterns, which presents an emerging topic of security solutions in decentralized communication.

The article ''A lightweight privacy-preserving protocol for VANETs based on secure outsourcing computing,'' by Wei *et al.*, proposes an identity-based signature that achieves unforgeability against chosen-message attacks without random oracle, and provides anonymity, traceability, and privacy for the VANETs.

In the article ''Wireless network intrusion detection based on improved convolutional neural network,'' by Yang and Wang, the authors propose a wireless network intrusion detection method based on an improved convolutional neural network with higher detection accuracy and true positive rates, together with a lower false positive rate.

In the article ''A novel dynamic network pruning via smooth initialization and its potential applications in machine learning based security solutions,'' by Wu *et al.*, the authors develop a dynamic network pruning method which reduces the necessary number of free parameters in the convolutional neural networks, and which does not need pretraining to learn the connectivity of the network, nor does it require a long time spent fine-tuning in order to restore the performance. This can lead to better data privacy in a distributed environment due to improved learning efficiency and convergence.

The article ''Sensitive and energetic IoT access control for managing cloud electronic health records,'' by Riad *et al.*, presents a sensitive and energetic access control mechanism for managing cloud-hosted electronic health records that provide fine-grained access control, even in critical situations.

The article ''Combined wireless network intrusion detection model based on deep learning,'' by Yang *et al.*, proposes a combined wireless network intrusion detection model based on deep learning. A feature database was generated by feature mapping, one-hot encoding, and normalization processing. Then, a deep belief network (DBN) with the multi-restricted Boltzmann machine (RBM) and the back propagation (BP) network was built. The BP network layer was connected as an auxiliary layer to the end of the RBM. The back propagation algorithm was used to fine-tune the weight of the multirestricted Boltzmann machine. Finally, the support vector machine (SVM) was used to train the detection method.

The article ''A secure and efficient data integrity verification scheme for cloud-IoT based on short signature,'' by Zhu *et al.*, aims to ensure data integrity and availability in the cloud and IoT storage systems, and proposes a scheme of data integrity verification based on a short signature algorithm (ZSS signature), which supports privacy protection and public auditing by introducing a trusted third party. The computational overhead is effectively reduced by

reducing hash function overhead in the signature process. Under the assumption of the CDH difficult problem, it can resist adaptive chosen-message attacks.

The article ''Storage mechanism optimization in blockchain system based on residual number system,'' by Mei *et al.*, proposes a storage optimization mechanism based on a residual number system to reduce the storage volume on each node. In addition, the recovery procedure of CRT-II (the new Chinese remainder theorem) is used to detect garbled data from devil nodes to provide strong fault tolerance capability.

The article ''Secure identity authentication of community medical Internet of Things,'' by Cheng *et al.*, reports an efficient community medical IoT node secure two-way identity authentication method and proposes a secure and reliable mechanism updating authentication keys and session keys. These measures can effectively ensure the legality of nodes and communication security in the community medical IoT system.

The article ''Joint data hiding and compression scheme based on modified BTC and image inpainting,'' by Liu *et al.*, presents the first joint data hiding and compression (JDHC) scheme on block truncation coding (BTC) compression domain. For the smooth blocks, according to the current embedding bit, either image inpainting or block search order coding (BSOC) is used to embed secret data and compress blocks simultaneously while maintaining acceptable compression performance. According to the image compression codes that are provided as output, image decompression and secret bits extraction procedures can be conducted simultaneously.

The article ''Cloud-assisted EHR sharing with security and privacy preservation via consortium blockchain,'' by Wang *et al.*, proposes a blockchain-based secure and privacy-preserving EHR sharing protocol. The data requester can search for desired keywords from the data provider to find relevant EHRs on the EHR consortium blockchain and get the re-encryption ciphertext from the cloud server after obtaining the data owner's authorization. The scheme implements searchable encryption and conditional proxy re-encryption for data security, privacy preservation, and access control. Proof of authorization is designed as the consensus mechanism for the consortium blockchain in order to guarantee the system's availability.

The article ''An authentic-based privacy preservation protocol for smart e-healthcare systems in IoT,'' by Deebak *et al.*, proposes a secure and anonymous biometric-based user authentication scheme to ensure secure communication in healthcare applications. The authors prove that through the use of this scheme, an adversary cannot impersonate a legitimate user to illegally access or revoke the smart handheld card. A formal analysis based on the random-oracle model and resource analysis is provided to show security and resource efficiencies in medical application systems.

The article ''A secured and efficient communication scheme for decentralized cognitive radio-based Internet of Vehicles,'' by Yao *et al.*, proposes a secured and efficient communication scheme for a decentralized CR-based IoV (CIoV) network. In this scheme, the roadside unit (RSU) senses the spectrum using an energy detection method. Each vehicle independently predicts the primary user (PU) activity pattern using a hidden Markov model (HMM). Once a vehicle detects a licensed channel free from the PUs, it informs the RSU to store the channel in a database alongside the dedicated direct short-range communication (DSRC) channels for data transmission. The RSU and vehicles are registered with a trusted authority, and they mutually authenticate each other. Upon mutual authentication, the RSU assigns communication channels to the vehicles on the road based on their density. When the density of the vehicles is high, the detected licensed channels are used; otherwise, the DSRC channels are used.

The article ''A privacy protection scheme of microgrid direct electricity transaction based on consortium blockchain and continuous double auction,'' by Zhang *et al.*, proposes a privacy protection scheme of microgrids direct electricity transaction based on consortium blockchain and the continuous double auction to reduce costs and improve the efficiency of transactions. Pseudonyms and pseudonym certificates are generated by fair blind signature technology to realize identity privacy in the continuous double auction. Decentralization and user identity traceability are achieved using (t, n) threshold secret sharing technology, which distributes and recovers the private key of a trusted third party.

The article ''A privacy-preserving method based on server-aided reverse oblivious transfer protocol in MCS,'' by Long *et al.*, proposes a privacy-preserving method based on server-aided (or cloud-assisted) reverse oblivious transfer (ROT) protocol containing a cloud server which can compute the results of the encrypted sensing data to avoid the full trust in the sensing platform and enhance the computing efficiency in MCS.

The article ''Reliable access control for mobile cloud computing (MCC) with cache-aware scheduling,'' by Jamal *et al.*, proposes an agent-based ABE access control method for the mobile cloud environment to deal with the single point of failure in the certification authority. Furthermore, the authors upgraded the cache-based scheduling algorithm to improve the response time of user jobs.

The article ''Detecting steganography in inactive voice-over-IP frames based on statistic characteristics of fundamental frequency,'' by Tian *et al.*, presents a new steganalysis method based on statistic characteristics of fundamental frequency, employs the statistics to characterize the frame-level dynamic characteristic of speech signals, utilizes the average values of Mel-frequency cepstral coefficients (MFCCs) to represent the invariant characteristic of inactive frames, and proposes a support-vector-machine-based steganalysis for inactive speech frames. The proposed method can provide accurate detecting results using only a very small quantity of inactive frames in real-time speech streams.

The article ''Quantum searchable encryption for cloud data based on full-blind quantum computation,'' by Liu *et al.*,

proposes a multi-client universal circuit-based full-blind quantum computation (FBQC) model. In order to meet the requirements of multiclient accessing or computing encrypted cloud data, all clients with limited quantum ability outsource the key generation to a trusted key center and upload their encrypted data to the data center. By combining the multi-client FBQC model and Grover searching algorithm, the authors propose a quantum searchable encryption scheme for cloud data. It solves the problem of multi-client access mode under searchable encryption in the cloud environment and has the ability to resist some quantum attacks. The security of this scheme is analyzed from two aspects: external attacks and internal attacks. The result indicates that it can resist such kinds of attacks and also guarantee the blindness of data and computation.

The article ''Efficient verifiable key-aggregate keyword searchable encryption for data sharing in outsourcing storage,'' by Wang *et al.*, proposes an efficient verifiable key-aggregate keyword searchable encryption (EVKAKSE) scheme. In this scheme, the data owner distributes only one aggregate key to users for keyword search, decryption, and verification, who can use the aggregate key to generate a single trapdoor for keyword search over shared files.

The article ''Integrated functional safety and security diagnosis mechanism of CPS based on blockchain,'' by Gu *et al.*, proposes a functional safety and information security protection mechanism based on blockchain technology. An effective communication judgment mechanism based on a functional safety error threshold is proposed, which is stored and judged by a smart contract. In addition, a refund transaction with a clock is proposed to ensure the effective execution of the functional safety error threshold mechanism.

In the article ''Traceability in permissioned blockchain,'' by Mitani and Otsuka, the authors achieve privacy protection and high transparency in a permissioned blockchain. To improve the transparency of the permissioned blockchain under privacy protection, this article considers traceability in the permissioned blockchain consisting of the following three properties: trade privacy (who trades with whom and at what asset amount), preservation (the total amount inside the permissioned blockchain, including deposits and withdrawals to the permissionless blockchain, is immutable), and noninvolvement (some members in the permissioned blockchain are not involved in some trades, and it is possible to prove that specified members performed the transaction). This is the first to achieve both preservation and noninvolvement while protecting the privacy of transactions. The method models traceability based on the hidden Markov model. Because the proof of traceability requires the calculation of more than quadratic degrees, this model is encrypted by homomorphic encryption. The number of participants in the permissioned blockchain corresponds to the number of additions in the model. The encrypted model is constructed by employing homomorphic encryption. The establishment of the original model is verifiable by applying the noninteractive zero-knowledge proof of the knowledge that the plaintext is equal to zero.

The article ''A digital watermarking encryption technique based on FPGA cloud accelerator,'' by Cao *et al.*, adopts discrete cosine transform (DCT) to transform the given image from spatial domain to frequency domain for adding watermark information. In order to meet the demands of image watermarking batch processing and cloud processing, this article optimizes the DCT algorithm and successfully deploys the designed accelerator kernel on the FPGA cloud platform to speed up the processing of watermarking. The cloud-based implementation makes digital watermarking applications highly extensible, widely shareable, and more secure. The whole system implements a series of complete cloud processes including image decoding, image pre-processing, watermarking embedding, and watermarked image encoding. The watermarking algorithm is accelerated by the efficient parallel computing capabilities of FPGA.

The article ''Using granule to search privacy preserving voice in home IoT systems,'' by Li *et al.*, proposes a novel personalized search scheme of encrypting voice with privacy-preserving by the granule computing technique. First, mel-frequency cepstrum coefficients (MFCC) are used to extract voice features. These features are obfuscated by an obfuscation function in order to protect them from being disclosed the server. Second, a series of definitions are presented including fuzzy granule, fuzzy granule vector, ciphertext granule, operators, and metrics. Third, the AES method is used to encrypt voices. A scheme of searchable encrypted voice is designed by creating the fuzzy granule of obfuscation features of voices and the ciphertext granule of the voice.

The article ''Joint energy-saving scheduling and secure routing for critical event reporting in wireless sensor networks,'' by Feng *et al.*, investigates a joint energy-saving scheduling and secure routing algorithm for critical event reporting in WSN. When a critical event has been detected, the notification must be safely sent to the sink node through the uplink transmission, and the sink node needs to broadcast the alarm messages to the whole network through the downlink transmission. In the uplink, a joint power allocation and secure routing strategy (JPASR) has been proposed to maximize the routing secure connection probability (RSCP) under the constraint of power. Meanwhile, combined with the level-by-level sleeping scheduling method, the energy-saving and secure uplink transmission can be guaranteed. In the downlink, an energy-first multi-point relays set selection mechanism (EFMSS) is designed to choose the backbone nodes to broadcast messages, and the backbone nodes are woken up by the same level-by-level sleeping scheduling method as the uplink transmission. With the two-step procedure, the critical events are appropriately dealt with and the responses are broadcast to the whole network.

The article ''Plenoptic face presentation attack detection,'' by Zhu *et al.*, presents a passive presentation attack detection method based on a complete plenoptic imaging system, which

can derive the complete plenoptic function of light rays using a single detector.

The article ''Stern-brocot-based non-repudiation dynamic provable data possession,'' by Tian *et al.*, discusses that a provable data possession (PDP) scheme can effectively help users to verify the integrity of data stored remotely in the cloud. The authors proposed a non-repudiable dynamic PDP scheme based on the Stern–Brocot tree (Stern–Brocot-based non-repudiation dynamic provable data possession, abbreviated as SB-NR-DPDP) in view of the problem that the existing PDP scheme pays less attention to the clients deceiving the cloud server.

The article ''An effective encrypted scheme over outsourcing data for query on cloud platform,'' by Tang *et al.*, discusses that users' data privacy was likely to be disclosed to the cloud server when their encrypted data was updated on cloud platforms. To address these problems, the authors proposed an effective encrypted query scheme over outsourcing data on cloud platforms.

The article ''Multi-layer network local community detection based on influence relation,'' by Li *et al.*, discusses how the discovery of local communities in multi-layer networks has become an active research field of complex systems. In this article, based on the homogeneity drive of multi-layer network and the influence relation index of multi-layer path length measurement, the authors proposed a local community detection model based on the influence relation of the multi-layer network.

The article ''SGX-based secure indexing system,'' by Xu *et al.*, discusses that the encrypted data rendered keyword indexing is more difficult to achieve, and the way to specify the plain-text keywords for the cipher-text data also revealed the privacy of the data owner to the untrusted service provider. To solve these problems, the authors proposed an SGX-based secure indexing solution based on the combination of hardware and software and using Intel's Software Guard Extensions (SGX) technology.

The article ''Group key agreement protocol based on privacy protection and attribute,'' by Qikun *et al.*, discusses that the identity authentication, privacy protection, and information sharing access control (different access rights may exist for different sensitivity of information) are key issues to be solved in group key agreement. Aiming at these problems, the authors proposed a group key agreement protocol based on privacy protection and attribute authentication (GKA-PPAA).

The article ''Physical layer security performance analysis of the FD-based NOMA-VC system,'' by Xie *et al.*, discusses the secrecy outage probability (SOP) of a cooperative non-orthogonal multiple access (NOMA) vehicular communication (VC) system, where the relay was working in either half-duplex (HD) or full-duplex (FD) mode. The authors assumed that all these links experience Nakagami-m fading. Some closed-form analytical expressions for the SOP performance of the FD/HD cooperative NOMA-VC system were derived.

The article ''Network security situation prediction based on MR-SVM,'' by Hu *et al.*, discusses that the support vector machine (SVM) was verified to be effective for predicting cyber security situations; however, the long training time of the prediction model was a drawback to its use. To address this, the authors proposed a cyber security situation prediction model based on MapReduce and the SVM.

The article ''Low-power AES data encryption architecture for a LoRaWAN,'' by Tsai *et al.*, discusses that for battery powered IoT end nodes, the AES encryption process consumes some amount of power, owing to the involvement of multiple cycles of repetition. To solve this problem, in this study, the authors proposed a low power consumed AES encryption architecture, called Low-Power AES Data Encryption Architecture (LPADA), which reduced the power consumed by the AES for data encryption by using low power SBox, power gating techniques, and power management methods.

The article ''An efficient outsourced privacy preserving machine learning scheme with public verifiability,'' by Hassan *et al.*, discusses that the cloud servers engaged through a third party cannot be fully trusted by multiple data users. Some recent outsourcing machine learning schemes have been proposed in order to preserve the privacy of data providers. The authors presented an efficient privacy-preserving machine learning scheme for multiple data providers.

The article ''Crowdsourcing approach for developing hands-on experiments in cybersecurity education,'' by Wang *et al.*, discusses that operational skills are essential for cybersecurity practitioners, and how hands-on experiments can be utilized to train their practical skills. The authors propose a framework called RC 2 F by adopting the crowdsourcing approach, which acted as a platform for the engineers and the faculties, as well as channels between them for resource exchanging.

The article ''An efficient multi-message and multi-receiver signcryption scheme for heterogeneous smart mobile IoT,'' by Qiu *et al.*, discusses that due to the inherent heterogeneity, distribution, intensive communication, and resource constraints of SM-IoT, efficient security and privacy communication protocols become a significant critical challenge. The authors proposed a signcryption scheme to achieve efficient secure multi-message and multi-receiver communication for the heterogeneous and distributed SM-IoT.

The article ''User behavior clustering scheme with automatic tagging over encrypted data,'' by Gao *et al.*, discusses that most of the existing methods of user behavior have problems such as weak generality and the lack of tags of clustering. Based on clustering algorithm, homomorphic encryption technology, and information security, in this article, the authors proposed a user behavior clustering scheme that supports automatic tags on ciphertext.

The article ''A high-imperceptibility and histogram-shifting data hiding scheme for JPEG images,'' by Li *et al.*,

discusses the data hiding of JPEG images realized by the histogram shift, where the secret message bits are embedded in the high-frequency coefficients to ensure a higher embedding rate, and the high-frequency coefficients are obtained by histogram distribution. The authors demonstrated that the proposed solution outperformed the most advanced technology in terms of embedding rate and visual quality.

The article ''Prototyping flow-net logging for accountability management in Linux operating systems,'' by Xiao *et al.*, discusses how to implement operating system accountability via accountable logging mechanisms in Linux operating systems. The authors designed and implemented a prototype of a flow-net accountable logging framework, which can be applied to both normal Linux operating systems and Internet of Things (IoT)-based Android operating systems. The authors demonstrated that the flow-net prototype only introduced a small overhead when compared with existing logging methods but provided much better operating system accountability.

The article ''A two-way VoLTE covert channel with feedback adaptive to mobile network environment,'' by Zhang *et al.*, proposes a two-way VoLTE covert channel over mobile network, which includes a sender-to-receiver covert timing channel that modulates covert message through actively dropping packets during the silence periods, and a reverse covert storage channel that hides the acceptance of the covert message as feedback information into the feedback control information field of the real-time transport control protocol packet. The proposed approach is demonstrated to remain undetectable and robust.

The article ''An graph-based adaptive method for fast detection of transformed data leakage in IoT via WSN,'' by Yu *et al.*, discusses data leakage prevention (DLP) in the Internet of Things (IOT), where the confidentiality of data changes frequently. The authors propose an adaptive feature graph update (AFGU) model based on mapping features of confidential data to the feature graph and demonstrated the proposed method can effectively and efficiently detect confidential data.

The article ''A novel solutions for malicious code detection and family clustering based on machine learning,'' by Yang *et al.*, discusses a malware identification problem, where the complexity of malware is increasing and malicious code is continuously produced. The authors proposed a malware classification model-based ensemble model, as well as a malware family clustering-based feature visualization, and demonstrated that the proposed methods outperformed existed individual models in accuracy or adaptation ability.

The article ''Attacking black-box image classifiers with particle swarm optimization,'' by Zhang *et al.*, discusses two variants of the PSO algorithm as approaches for generating black-box adversarial examples while requiring fewer black-box queries and feedback information. The authors proposed an efficient and effective adversarial examples generation algorithm for both targeted and non-targeted attacks in the black-box environment and demonstrated that the proposed algorithm outperformed other generation algorithms for image misclassification.

The article ''Secure mining of association rules in distributed datasets,'' by Han *et al.*, discusses secure association rule mining in the background that transactions come from multiple data centers. The authors proposed an association rules mining approach that preserve differential privacy. In the mining process, each party's raw transactions are well protected no matter how strong the attacker's background knowledge is. Simulation results prove the security and efficiency of the proposed approach.

The article ''DT-CP: A double-TTPs based contract-signing protocol with lower computational cost,'' by Xu *et al.*, discusses contract signing protocol, where the involved parties exchange their private signature with each other via two double trusted third parties in a secure way, while preventing malicious external parties and minimizing the computational cost as much as possible during the execution of the protocol. The authors proposed an efficient and secure contract signing protocol for the IoT and demonstrated that the proposed protocol outperformed other related protocols.

The article ''Cooperative secondary encryption for primary privacy preserving in cognitive radio networks,'' by Wang *et al.*, discusses secure cognitive communication, where a primary system directly transmits private messages or employs pre-transmitted secure secondary messages to encrypt the primary privacy information, and the secondary system acquires a fraction of the interference-free licensed spectrum. The authors studied the primary secure transmission for the non-buffer scenario and the buffer-aided scenario and demonstrated that the proposed scheme outperformed other standard protocols.

The article ''Vulnerability analysis of instructions for SDC-causing error detection,'' by Gu *et al.*, discusses the reliability of IoT devices, where the extracted instruction features were investigated to analyze the vulnerabilities of programs or instructions for detecting the silent data corruption (SDC) error. The authors proposed a method of SDC-causing error detection based on support vector regression (SED-SVR) for fully exploiting the correlation between data features and demonstrated that the proposed method outperformed other standard detection methods.

The article ''A security protocol for route optimization in DMM-based smart home IoT networks,'' by Shin *et al.*, discusses secure IoT smart home communication, where the involved devices directly communicate with each other in a secure way while minimizing the possibility of information leakage during data transmission. The authors proposed a secure route optimization protocol for distributed IP mobility management (DMM)-based smart home systems and demonstrated that the proposed system outperformed other standard protocols.

In the article titled ''An optimized static propositional function model to detect software vulnerability,'' by Han *et al.*, the authors propose a static detection model based on the proposition function for software vulnerability detection.

At the same time, a new program intermediate representation, vulnerability executable path set (VEPS), was also proposed to optimize the designated model. Their experiments show that the proposed detection method is effective and efficient.

In the article ''Using AI to attack VA: A stealthy spyware against voice assistances in smart phones,'' by Zhang *et al.*, a novel attack approach, Vaspy, was proposed. The proposed artificial intelligence-based attack method could craft the users' ''activation voice'' by silently listening to users' phone calls. Once the activation voice was formed, Vaspy could select a suitable occasion to launch an attack.

In the article ''Machine learning for security and the Internet of Things: The good, the bad, and the ugly,'' Liang *et al.*, presented a detailed survey on the good, the bad, and the ugly use of machine learning for cybersecurity and CPS/IoT. They considered the numerous benefits (good use) and the vulnerabilities (bad use) that machine learning has brought, both in general and specifically for security and CPS/IoT. Moreover, the authors presented the growing trend of utilization of machine learning in the execution of cyberattacks and intrusions (ugly use). It is a timely and informative ground for researchers in the security domain.

In the article ''Proof-of-reputation based-consortium blockchain for trust resource sharing in the Internet of Vehicles,'' by Chai *et al.*, the authors proposed a consortium blockchain-based resource sharing paradigm in the Internet of Vehicles, in which the resource sharing interactions were encapsulated as transactions and recorded by road side units. The extensive security and privacy analysis, as well as simulation experiments on communication performance, demonstrated the efficiency of the proposed blockchain system.

In the article ''TIMCC: On data freshness in privacy-preserving incentive mechanism design for continuous crowdsensing using reverse auction,'' by Ma *et al.*, the authors designed the truthful incentive mechanism for continuous crowdsensing (TIMCC, in short), a privacy-preserving incentive mechanism for continuous crowdsensing. The authors introduced a metric, age of data, and adopted the reverse auction framework to model the connection between the platform and the users. Simulation results validated their theoretical analysis and the effectiveness of the proposed mechanism.

In summary, this Special Section attracted high-quality and relevant contributions. The large number of submissions shows that this topic is an active and important research area.

Finally, the Guest Editors of the Special Section are very grateful to the contributing authors, dedicated reviewers, and relevant supporting editorial staff members. The Guest Editors are especially grateful for the guidance from the Editor-in-Chief to enable the success of this Special Section.

XIAOCHUN CHENG, *Lead Editor*
Department of Computer Science
Middlesex University
London NW4 4BT, U.K.

ZHELI LIU, *Guest Editor*
College of Cyber Science and
College of Computer Science
Nankai University
Tianjin 300071, China

XIAOJIANG DU, *Guest Editor*
Department of Computer and Information Sciences
Temple University
Philadelphia, PA 19122, USA

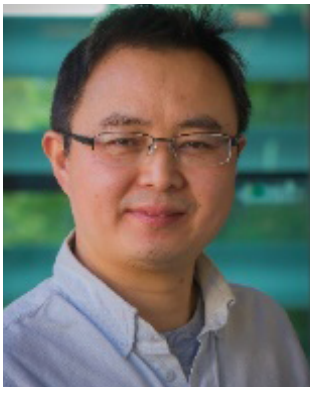
SHUI YU, *Guest Editor*
School of Computer Science
University of Technology Sydney
Ultimo, NSW 2007, Australia

LEONARDO MOSTARDA, *Guest Editor*
Computer Science Department
Università di Camerino
62032 Camerino, Italy

XIAOCHUN CHENG (Senior Member, IEEE) received the B.Eng. degree in computer engineering, in 1992, the Ph.D. degree in computer science, in 1996, and the M.B.A. degree, in 2011. He has been the Computer Science Project Coordinator of Middlesex University, since 2012. He has published with world top rank journals and international flagship conferences. He is a member of the IEEE SMC Technical Committee on Computational Intelligence, the IEEE Communications Society Communications and Information Security Technical Committee, and the BCS Information Security Specialist Group. Three of his articles are in the 2019 top 1% of the academic field based on data from essential science indicators. He has won three national competitions as well as the National Science and Technology Advance Award.

ZHELI LIU received the B.Sc. and M.Sc. degrees in computer science and the Ph.D. degree in computer application from Jilin University, China, in 2002, 2005, and 2009, respectively. After a Postdoctoral Fellowship at Nankai University, he joined the College of Computer and Control Engineering, Nankai University, in 2011. He is currently the Vice Dean of the College of Computer Science and the College of Cyber Science, Nankai University. His current research interests include applied cryptography and data privacy protection. He has published more than 50 articles in well-known journals or top conferences, including IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, IEEE TRANSACTIONS ON COMPUTERS, IEEE TRANSACTIONS ON SERVICES COMPUTING, IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, and IEEE INFOCOM. He was the Chair of several international conferences, including SPNCE 2019, ICA3PP 2018, CSE 2017, SPNCE 2016, BWCCA 2015, and EIDWT 2013. He has served as a Guest Editor for many well-known journals, including *MoNET* (Springer) and IEEE ACCESS. He is an Associate Editor of *Cybersecurity* (Springer).

XIAOJIANG DU (Fellow, IEEE) received the B.S. and M.S. degrees in electrical engineering from the Automation Department, Tsinghua University, Beijing, China, in 1996 and 1998, respectively, and the M.S. and Ph.D. degrees in electrical engineering from the University of Maryland at College Park, College Park, in 2002 and 2003, respectively. He is currently a tenured Full Professor and the Director of the Security and Networking (SAN) Laboratory, Department of Computer and Information Sciences, Temple University, Philadelphia, USA. His research interests include security, wireless networks, and systems. He has authored more than 400 journal articles and conference papers in these areas, as well as a book published by Springer. He is a Life Member of ACM. He is (was) a Technical Program Committee (TPC) Member of several premier ACM/IEEE conferences such as INFOCOM (2007–2020), IM, NOMS, ICC, GLOBECOM, WCNC, BroadNet, and IPCCC. He has been awarded more than six million U.S. Dollars in research grants from the U.S. National Science Foundation (NSF), Army Research Office, the Air Force Research Laboratory, NASA, the State of Pennsylvania, and Amazon. He won the Best Paper Award at IEEE GLOBECOM 2014 and the Best Poster Runner-Up Award at the ACM MobiHoc 2014. He has served as the Lead Chair for the Communication and Information Security Symposium of the IEEE International Communication Conference (ICC) 2015 and the Co-Chair for the Mobile and Wireless Networks Track of IEEE Wireless Communications and Networking Conference (WCNC) 2015. He serves on the editorial boards for two international journals.



SHUI YU (Senior Member, IEEE) is currently a Professor with the School of Computer Science, University of Technology Sydney, Australia. He has published three monographs and edited two books and has published more than 350 technical articles in top journals and conferences, such as IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, IEEE TRANSACTIONS ON COMPUTERS, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, IEEE TRANSACTIONS ON MOBILE COMPUTING, IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, IEEE TRANSACTIONS ON EMERGING TOPICS IN COMPUTING, IEEE TRANSACTIONS ON NETWORKING, and INFOCOM. He initiated the research field of networking for big data in 2013. His H-index is 43. His research interests include big data, security and privacy, networking, and mathematical modeling. He is a member of AAAS and ACM and a Distinguished Lecturer of the IEEE Communication Society. He has been serving on a number of prestigious editorial boards, including IEEE COMMUNICATIONS SURVEYS AND TUTORIALS (an Area Editor), *IEEE Communications Magazine*, and IEEE INTERNET OF THINGS JOURNAL.

LEONARDO MOSTARDA (Member, IEEE) received the Ph.D. degree from the Computer Science Department, University of L'Aquila, in 2006. Afterward, he cooperated with the European Space Agency (ESA) on the CUSPIS FP6 Project to design and implement novel security protocols and secure geo tags. In 2007, he was a Research Associate with the Distributed System and Policy Group, Computing Department, Imperial College London, where he has been working on the UBIVAL EPRC Project in cooperation with Cambridge, Oxford, Birmingham, and UCL, for building a novel middleware to support the programming of body sensor networks. In 2010, he was a Senior Lecturer with the Distributed Systems and Networking Department, Middlesex University. He is currently an Associate Professor with the Computer Science Department, Camerino University, Italy, and the CEO of Bilancio CO2 zero. His main research interests include wireless sensor networks, middleware, and security.