Guest Editorial
Special Issue on Security and Privacy Protection for Big Data and IoT

WITH the proliferation of the Internet of Things (IoT), wireless sensor networks, mobile social networks, crowdsensing applications, and beyond, huge amounts of data are being explosively generated every day. While big data and IoT bring well-understood benefits to increase knowledge and improve the quality of our daily lives, they also face wide attacking surfaces, and thus raise critical concerns on notions of trust, security, and privacy. One of the fundamental questions is how to collect, store, and process the huge amounts of data in a secure and privacy-preserving manner, without compromising the potential of capitalization on big data and IoT.

This problem, also known as security and privacy protection for big data and IoT, has received wide attentions in recent years, where noteworthy progress has been made. However, existing solutions are still far from sufficient to address all the security and privacy issues, given the new challenges brought by the unique features of big data and IoT, such as data volume, velocity, variety, and veracity. This Special Issue aims to provide a venue for interested researchers and practitioners to share their novel ideas and latest findings on research of big data and IoT, with focus on various aspects of trust, security, and privacy. The purpose is to advocate further efforts from research communities so as to push forward the frontiers of big data security research, especially in the context of IoT.

The response to our Calls for Papers on this Special Issue was satisfactory, with 17 submissions from around the globe. During the review process, each paper was assigned to and reviewed by at least three experts in the relevant areas, with a rigorous two-round review process. In the following, let us introduce these papers and highlight their main contributions.

In the paper "The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved," in order to understand the essential reasons of new IoT threats more clearly, the concept of "IoT features" is proposed. The authors discuss the security and privacy effects of eight IoT features, as well as the relative threats, summarize existing solutions to known threats, and list many research challenges yet to be solved.

In order to conduct privacy leakage analysis in cloud specifically, the authors of "A Multigranularity Forensics and Analysis Method on Privacy Leakage in Cloud Environment" propose a multigranularity privacy leakage forensics method to analyze privacy violations caused by malware in cloud environment. With simulations in the target virtual machine environment, the proposed method can detect privacy leakage behaviors of malware without touching user's privacy data. The combination between continuous RAM mirroring technology and dynamic taint analysis assists the forensics investigation.

Since it is observed that the train-trackside channels for video dissemination can be easily accessible to anyone, the video traffic is vulnerable to attacks which may cause deadly tragedies. In "Situation-Aware Authenticated Video Broadcasting Over Train-Trackside WiFi Networks," a situation-aware authenticated video broadcasting scheme is proposed in the railway network, which consists of train, on-board sensor, trackside global system for mobile communications-railway device, WiFi access point, and train control center. The proposed scheme ensures the codestream authenticity and provides high quality of service in the lossy subway WiFi environment.

In the paper "E-AUA: An Efficient Anonymous User Authentication Protocol for Mobile IoT," the authors design an efficient anonymous user authentication protocol between the users and servers based on multiserver architectures, which contain multiple servers to address the problem of network congestion in mobile IoT. In addition, it proposes a dual-message mechanism with strong anti-attack ability, lower communication, and computation cost.

Narrowband IoT technology has been introduced into the 3GPP standards. In the paper "Fast Authentication and Data Transfer Scheme for Massive NB-IoT Devices in 3GPP 5G Network," a fast mutual-authentication and data transfer scheme for massive NB-IoT devices, by integrating the access authentication and secure data transmission process, is proposed. The proposed scheme can effectively achieve the authentications and data transmissions for a group of NB-IoT devices at the same time.

In efficient and privacy-preserving online medical primary diagnosis framework, users can access online medical primary diagnosing service accurately without divulging their medical data. In the paper "CINEMA: Efficient and Privacy-Preserving Online Medical Primary Diagnosis With Skyline Query," new mechanisms for privacy-preserving skyline query are proposed, based on fast secure permutation and comparison technique. The encrypted user's query can be directly operated at the service provider without decryption, and the diagnosis result can only be decrypted by the user. Meanwhile,

Digital Object Identifier 10.1109/JIOT.2019.2908460

the diagnosis model in service provider can also be protected.

In order to provide better electricity services, service providers utilize wireless sensor networks to collect the electricity consumption data for data clustering analysis. In the paper "Enhancing Privacy and Availability for Data Clustering in Intelligent Electrical Service of IoT," the authors propose a novel data clustering scheme. It ensures the availability of data clustering results under the premise of security, through improving the selection of the initial cluster centers and finding the outliers via calculating the density of every data point.

In the paper "Cyberspace-Oriented Access Control: A Cyberspace Characteristics-Based Model and Its Policies," a cyberspace-oriented access control model is proposed to achieve fine-grained access control for cyberspace. Taking applications in the browser–server architecture as an example, this paper presents seven atomic operations for these applications. A number of cases demonstrate that operations in these applications are combinations of introduced atomic operations.

The proposed scheme in "Smart Contract-Based Access Control for the Internet of Things" investigates the access control issue in IoT, for which they propose a smart contract-based framework to implement distributed and trustworthy access control. The framework includes multiple access control contracts to control multiple subject–object pairs in the system. There is judge contract for judging the misbehavior of the subjects during the access control, and register contract for managing the access control contracts and judge contract.

Based on the signal modulation of status LEDs, the authors of "Optical Exfiltration of Data via Keyboard LED Status Indicators to IP Cameras" propose a novel approach to build an optical covert channel. An attack model is given to build a covert communication channel with a normal IP camera by turning the LED on/off. The form of modulation and the corresponding demodulation method are designed and optimized, which implements a prototype of exfiltration malware to verify its validity.

In the live Tor network, a practical Eclipse attack and comprehensive analysis framework are proposed to evaluate the security implications. To demonstrate the feasibility of Eclipse attacks, the authors of "Towards a Comprehensive Insight Into the Eclipse Attacks of Tor Hidden Services" implement a prototype of Eclipse attacks on live Tor network. They present the first formal analysis to evaluate the extent of threat that such vulnerabilities may cause and quantify the cost of Eclipse attacks via probabilistic analysis.

In the paper "A Novel Secure and Efficient Data Aggregation Scheme for IoT," the authors define a novel problem termed $n\times 1$-out-of-n oblivious transfer, and propose a protocol combining modern cryptography and hidden permutation to efficiently solve the problem. The proposed hidden permutation can be used to implement an anonymous communication system, and the full protocol can be applied to achieve privacy-preserving data aggregation for many applications, such as smart grids, wireless sensor networks, and mobile health.

In the paper "Blockchain-Based Decentralized Trust Management in Vehicular Networks," the authors propose a decentralized trust management system for vehicular networks, which can aggregate the trust values based on ratings generated by messages receivers. Using blockchain techniques, all roadside units work together to maintain a reliable and consistent database. With the aid of the proposed system, vehicles are able to query the trust values of neighbors and then assess the credibility of received messages.

In the paper "IoT Big Data Security and Privacy Versus Innovation," the authors address the conflict in the collection, use, and management of Big Data at the intersection of security and privacy requirements and the demand of innovative uses of the data. They propose a three-part decomposition of the design space, in order to clarify requirements and constraints. By identifying several distinct objectives for the design of IoT Big Data management, they propose that more effective design and control is possible at the intersection of these forces, through an iterative process of review and redesign.

Different from the widely investigated cryptographic approaches, the authors of "Distributed Privacy-Preserving Data Aggregation Against Dishonest Nodes in Network Systems" consider how to mitigate the pollution from dishonest nodes. They propose an enhanced secure consensus-based data aggregation (E-SCDA) algorithm that allows neighbors to detect dishonest nodes, and they also derive the error bound accordingly, in case of undetectable dishonest nodes. They prove the convergence of the E-SCDA and show that the algorithm can preserve the privacy associated to nodes' initial states. Extensive simulations of the proposed algorithm has a high convergence accuracy and low complexity.

To ensure the security of IoT data, particularly those outsourced to the cloud or the edge, the authors of "Secure Range Search Over Encrypted Uncertain IoT Outsourced Data" proposed an effective indexing technique to support range searches on multidimensional encrypted data. Specifically, they use the KD-tree to organize the objects to improve the retrieval efficiency. To further support operations over ciphertext, they use an OPE and homomorphic encryption scheme to encrypt the dataset. Some positive evaluation results are also provided.

In wireless multimedia sensor network, the underlying routing protocols need to provide an acceptable level of quality-of-service support for the multimedia traffic. In the paper "SAMS: A Seamless and Authorized Multimedia Streaming Framework for WMSN-Based IoMT," a seamless and authorized multimedia streaming framework is proposed for a cluster-based hierarchical network of wireless multimedia sensors. The framework uses authentication at different levels to form secured clusters.

We express our gratitude to the authors for their excellent contributions to this Special Issue. Great thanks to all reviewers for their efforts in reviewing these papers, and valuable comments that help greatly to improve the quality of the papers. We also appreciate the great efforts and support from the Editor-in-Chief, the Editorial Board, and the administrative staff, without which this Special Issue would not have been possible. We hope this Special Issue will serve as a good reference for researchers, scientists, engineers, and academicians in the field of security and privacy protection for Big Data and IoT.

FENGHUA LI, *Guest Editor*
Institute of Information Engineering
Chinese Academy of Sciences
Beijing 100093, China

HUI LI, *Guest Editor*
School of Cyber Engineering
Xidian University
Xi'an, Shaanxi 710071, China

CONG WANG, *Guest Editor*
Department of Computer Science
City University of Hong Kong
Hong Kong

KUI REN, *Guest Editor*
School of Computer Science and Technology
Zhejiang University
Hangzhou, Zhejiang 310058, China

ELISA BERTINO, *Guest Editor*
Department of Computer Science
Purdue University
West Lafayette, IN 47907 USA

Fenghua Li received the B.S. degree in computer software and the M.S. and Ph.D. degrees in computer systems architecture from Xidian University, Xi'an, China, in 1987, 1990, and 2009, respectively.

He is currently a Professor and the Doctoral Supervisor with the Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China. He has authored or co-authored over 80 papers in academic journals and conferences. His current research interests include network security, system security, privacy computing, and trusted computing.

Dr. Li was a recipient of the Best Paper Award of IEEE TRUSTCOM 2015. He served as the General Chair for International Symposium on Privacy Computing in 2017 and 2018.

Hui Li received the B.Sc. degree from Fudan University, Shanghai, China, in 1990, and the M.Sc. and Ph.D. degrees from Xidian University, Xi'an, China, in 1993 and 1998, respectively.

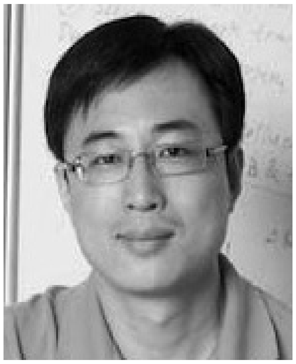
He is currently a Professor with the School of Cyber Engineering, Xidian University, where he has been a Professor since 2005. He has authored or co-authored over 160 papers in academic journals and conferences. His current research interests include cryptography, wireless network security, cloud computing security, privacy preservation, and information theory.

Dr. Li was a recipient of the Distinguished Paper Award in ASIACCS 2013. He served as the Chair of the ACM SIGSAC China Chapter, the TPC Co-Chair of ISPEC 2009 and IAS 2009, the General Co-Chair of E-Forensic 2010, ProvSec 2011, and ISC 2011, and the Honorary Chair of NSS 2014 and ASIACCS 2016.

Cong Wang (SM'17) received the B.E. degree in electronic information engineering and the M.E. degree in communication and information system from Wuhan University, Wuhan, China, and the Ph.D. degree in electrical and computer engineering from the Illinois Institute of Technology, Chicago, IL, USA.

He is an Associate Professor with the Department of Computer Science, City University of Hong Kong, Hong Kong. His research has been supported by multiple government research fund agencies, including the National Natural Science Foundation of China, Hong Kong Research Grants Council, and Hong Kong Innovation and Technology Commission. He has been published frequently in peer-reviewed journals and conferences. He has over 16 000 Google Scholar Citations with an H-index of 30 in 2019. His current research interests include data and computation outsourcing security in the context of cloud computing, blockchain, and decentralized application, network security in emerging Internet architecture, multimedia security, and privacy-enhancing technologies in the context of big data and Internet of Things.

Dr. Wang was a recipient of the Outstanding Supervisor Award in 2017 and the President's Award from the City University of Hong Kong in 2016. He was a co-recipient of the Best Student Paper Award of IEEE ICDCS in 2017 and the Best Paper Award of IEEE MSN in 2015 and CHINACOM in 2009. He is one of the founding members of the Young Academy of Sciences of Hong Kong. He serves/has served as an Associate Editor for the IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, the IEEE INTERNET OF THINGS JOURNAL, IEEE NETWORKING LETTERS, and as the TPC Co-Chair for a number of IEEE conferences/workshops. He is a member of the ACM.



Kui Ren (F'15) received the B.Eng degree in chemical engineering and the M.Eng degree in materials engineering from Zhejiang University, Hangzhou, China, in 1998 and 2001, respectively, and the Ph.D degree in electrical and computer engineering from the Worcester Polytechnic Institute, Worcester, MA, USA, in 2007.

He is currently a Distinguished Professor with the School of Computer Science and Technology, Zhejiang University, Hangzhou, China, where he also directs the Institute of Cyber Space Research. His current research interests include cloud and data security, AI and Internet of Things security, and privacy-enhancing technologies.

Dr. Ren is a Distinguished Member of the ACM.

Elisa Bertino received the Ph.D. degree in computer science from the University of Pisa, Pisa, Italy, in 1980.

She is currently a Professor of computer science with Purdue University, West Lafayette, IN, USA, and serves as a Research Director of the Center for Education and Research in Information Assurance and Security and the Director of the Cyber Center. She was a Professor and the Department Head of the Department of Computer Science and Communication, University of Milan, Milan, Italy. She has been a Visiting Researcher with IBM Research-Almaden, San Jose, CA, USA; Microelectronics and Computer Technology Corporation, Austin, TX, USA; Rutgers University, New Brunswick, NJ, USA; and Telcordia Technologies, Piscataway, NJ, USA. She is currently a Professor of computer science with Purdue University and a Professor of electrical and computer engineering. She is currently the Director of the Purdue Cyberspace Security Laboratory, where she leads multidisciplinary research in data security and privacy. Her current research interests include digital identity management, biometrics, data trustworthiness, privacy techniques, security for sensors and drones, security for content distribution networks, systems for the management of security and privacy policies, and assured information sharing.

Dr. Bertino was a recipient of the 2002 IEEE Computer Society Technical Achievement Award for outstanding contributions to database systems and database security and advanced data management systems and the 2005 IEEE Computer Society Tsutomu Kanai Award for pioneering and innovative research contributions to secure distributed systems. She is a Fellow of the ACM and AAAS.