Digital Object Identifier 10.1109/ACCESS.2020.3040469

EDITORIAL

IEEE ACCESS SPECIAL SECTION EDITORIAL: SECURITY AND PRIVACY FOR CLOUD AND IoT

The Internet of Things (IoT), which enables a wide variety of embedded devices, sensors, and actuators (known as smart things) to interconnect and exchange data, is a promising network scenario for bridging physical devices and virtual objects in the cyber world. Considering the limited capacity of smart things, cloud computing has been introduced to store and process the huge amount of data collected by the IoT. The appropriate integration of cloud computing and the IoT can be regarded as the best of two worlds, simultaneously providing omnipresent sensing services and powerful processing capabilities. Undoubtedly, the cloud-assisted IoT will boost the advancement of innovative applications and services including smart cities, industrial IoT, intelligent transportation, and electronic health systems. Despite the benefits of cloud-aided IoT, it is impossible to overlook the significance of security and privacy in this kind of highly heterogeneous and interconnected system. To deal with security threats to smart devices and sensitive data, hundreds of security solutions have recently been put forward for either the cloud or IoT environments. However, a few important characteristics such as heterogeneity and scalability have not been properly considered in these solutions.

The objective of this Special Section is to compile recent research efforts dedicated to studying the security and privacy of a rapidly increasing number of cloud and IoT applications. The Special Section solicited high-quality unpublished work representing recent advances and novel methodologies for enabling traditional security solutions for the cloud and the IoT, as well as theories and technologies proposed to defend cloud and IoT-oriented applications against adversarial or malicious attacks. Seventy-four submissions were received, and 24 articles were selected for inclusion in the Special Section after a thorough review and revision process conducted by at least two independent referees. These 24 accepted articles can be divided into three categories: Authentication and Access Control (ten articles), Attack Resilient and Cryptography (seven articles), and Privacy Protection (seven articles).

In the Authentication and Access Control category, the article "A secure authentication protocol for Internet of Vehicles," by Chen *et al.*, proposed a secure communication scheme for the purpose of authentication in an Internet of Vehicles (IoV) environment. The proposed scheme can efficiently protect the data transmitted in an insecure IoV network and preserve the privacy of vehicle users. The proposed scheme guarantees resistance to several attacks, such as offline identity guessing attack, location spoofing attack, and replay attack.

In the article "Design of a secure password-based authentication scheme for M2M networks in IoT-enabled cyber-physical systems," by Renuka *et al.*, the authors propose an efficient and secure authentication scheme for machine-to-machine (M2M) networks in IoT-enabled systems. The proposed scheme allows any pair of entities in an M2M network to mutually authenticate each other and agree on a session key for communicating data in a secure and efficient way. It thus provides good security and efficiency and is suitable for environmental sensors that are limited in terms of computation, storage, and energy resources.

In the article "Light-weight and privacy-preserving authentication protocol for mobile payments in the context of IoT," by Chen *et al.*, the authors propose a lightweight and privacy-preserving authentication protocol for mobile payment in the context of the IoT. The issues of payment trust and user privacy are the focus of the investigation. In addition, with the support of a unidirectional certificate-less proxy re-signature scheme, the proposed authentication protocol is provably secure under the extended computational Diffie–Hellman problem.

In the article "Sec-D2D: A secure and lightweight D2D communication system with multiple sensors," by Cao *et al.*, a lightweight and efficient key distribution scheme for secure device-to-device (D2D) communication is proposed. In the proposed scheme, an efficient near-field authentication process is developed to detect and validate the proximity between two devices. In addition, a robust information exchange mechanism is introduced over the audio channel and the RF channel.

In the article "Selective authentication based geographic opportunistic routing in wireless sensor networks for Internet of Things against DoS attacks," by Lyu *et al.*, a selective authentication-based geographic opportunistic routing (SelGOR) scheme is proposed to defend against Denial of Service (DoS) attacks in Wireless Sensor Networks (WSNs).

The proposed scheme can meet the requirements of authenticity and reliability in WSNs. In addition, by analyzing statistic state information (SSI) of wireless links, SelGOR leverages an SSI-based trust model to improve the efficiency of data delivery.

In the article "A novel attribute-based access control scheme using blockchain for IoT," by Ding *et al.*, the authors propose a novel attribute-based access control scheme for data security in IoT systems. The proposed scheme adopts blockchain technology to record the distribution of attributes and can thus avoid single point failure and data tampering. In addition, the access control process is optimized to meet the need for high efficiency and lightweight calculation for IoT devices.

In the article "Efficient attribute-based access control with authorized search in cloud storage," by Hao *et al.*, the authors propose an efficient attribute-based access control with authorized search scheme (EACAS) in cloud storage. The proposed scheme extends the anonymous key-policy attribute-based encryption (AKP-ABE) to support fine-grained data retrieval with attribute privacy preservation. In addition, by integrating the key delegation technique into AKP-ABE, EACAS enables data users to customize search policies based on their access policies and generate the corresponding trapdoor using the secret key granted by the data owner to retrieve their data of interest.

In the article "Fingerprint recognition strategies based on a fuzzy commitment for cloud-assisted IoT: A minutiae-based sector coding approach," by Shi *et al.*, a fingerprint recognition scheme using a minutiae-based sector coding strategy is proposed for cloud-assisted IoT. The proposed approach classifies the minutiae of a fingerprint into many designed sectors and encodes them according to the extracted features. In addition to adopting the fuzzy commitment, a key encryption process is accomplished using BCH codes and Hash mappings.

In the article "Privacy-oriented blockchain-based distributed key management architecture for hierarchical access control in the IoT scenario," by Ma *et al.*, a new blockchain-based distributed key management architecture (BDKMA) with fog computing is proposed to reduce latency, and multi-blockchains are operated in the cloud to achieve cross-domain access. The proposed scheme utilizes blockchain technology to satisfy the decentralization, fine-grained auditability, high scalability, and extensibility requirements, as well as the privacy-preserving principles for hierarchical access control in the IoT.

In the article "Proxy re-encryption in access control framework of information-centric networks," by Wang *et al.*, an efficient proxy re-encryption (PRE) scheme in an information-centric networking (ICN) framework is proposed to help reduce overhead on the user-side, while guaranteeing flexible data sharing between subscribers and even their co-operators. The proposed scheme has the additional benefits of noninteractivity and collusion resistance. The authors prove the scheme is secure against adaptive replayable adaptive chosen ciphertext attack (RCCA) in re-encryption and secure against chosen ciphertext attack (CCA) in complete ICN encryption.

In the Attack Resilient and Cryptography category, the article "A novel low-rate denial of service attack detection approach in ZigBee wireless sensor network by combining Hilbert–Huang transformation and trust evaluation," by Chen *et al.*, proposes a novel Low-rate Denial of Service (LDoS) attack detection approach combining Hilbert–Huang Transformation (HHT) and Trust evaluation in Zigbee wireless sensor networks (WSNs). The proposed approach consists of three algorithms: a) a scalable LDoS attack detection architecture for cloud-based IoT network environments; b) a novel HHT-based LDoS attack detection algorithm in Zigbee WSNs; and c) an intrinsic mode function (IMF) components trust evaluation approach combining a correlation coefficient and a KS test.

In the article "ARCA-IoT: An attack-resilient cloud-assisted IoT system," by Javaid *et al.*, the authors propose an Attack-Resilient Cloud-Assisted (ARCA) system to deal with three challenges, i.e., interoperability, scalability, and trustworthiness, germane to cloud-assisted IoT environments. ARCA-IoT leverages the concept of the cloud and Web technologies to facilitate interoperability and scalability. For trustworthiness, it is identified that trust is dynamic in context. In addition, the Naive Bayes classifier is integrated into the ARCA-IoT system to prevent trustworthiness-maneuvering attacks.

In the article "BRIoT: Behavior rule specification-based misbehavior detection for IoT-embedded cyber-physical systems," by Sharma *et al.*, the authors propose a lightweight behavior rule specification-based misbehavior detection mechanism for IoT-embedded cyber-physical systems (BRIoT). The main idea of the proposed approach is to model a system through which the misbehavior of an IoT device, manifested as a result of attacks exploiting an exposed vulnerability, may be detected through automatic model-checking and formal verification, regardless of whether the attack is known or unknown.

In the article "Constructing features for detecting android malicious applications: Issues, taxonomy, and directions," Wang *et al*. present a clear and comprehensive survey of the state-of-the-art work that detects malicious applications (malapps) by characterizing the behaviors of said apps with various types of features. The authors collected a total of 1947 papers, among which 236 papers were used in a survey comprising four dimensions: features extracted, feature selection methods employed (if any), detection methods used, and scale of the evaluation performed. This article not only presents a taxonomy of the features that the related literature employs but also highlights the issues of constructing features for malapp detection.

In the article "Flow context and host behavior based Shadowsocks's traffic identification," by Zeng *et al.*, a novel ShadowSocks (SS) detection method based on flow context

and host behavior is proposed. The method can not only identify SS flows accurately, but can also be applied to a large-scale network environment. Twelve-dimensional features corresponding to three aspects are extracted to build the detection model, i.e., the relationship between flows, the hosts' flow behavior, and the hosts' DNS behavior.

In the article "A complexity-reduced block encryption algorithm suitable for the Internet of Things," by Guo *et al.*, the proposed complexity-reduced secure and fast encryption routine (SAFER)-Fermat block encryption method accounts for both the confusion and diffusion principles. In the proposed algorithm, a novel diffusion layer exploiting the Fermat number theory transform is proposed, while the confusion layer remains unchanged as the SAFER algorithm.

In the article "A lightweight cellular automata based encryption technique for IoT applications," Roy *et al.* propose a lightweight cellular automata (CA)-based cipher, known as the Lightweight CA Cipher (LCC), for IoT applications. In the proposed method, encryption is done at the perception layer, where the sensor nodes are deployed, while decryption is done at the network layer, where gateway devices are installed. The experimental results show the proposed method is more efficient than some existing ciphers like DES and 3DES when randomness, execution time, and implementation simplicity are considered as prime requirements.

In the Privacy Protection category, the article "A generalized constraint of privacy: α-mutual information security," by Yao, studied the security of a variety of cryptographic tasks, including traditional privacy (e.g., seeded extractors, encryptions, commitments, and secret sharing schemes) and differential privacy from the perspective of α-mutual information. The authors first propose a modular and unified framework to study the relations hips between statistical security and mutual information security for a series of privacy schemes outside the sphere of prior work that focused on a special scheme. In addition, the authors introduce α-mutual information security via the Rényi entropy for a series of privacy schemes and aim to bridge the gap between statistical security and α-mutual information security.

In the article "A sanitization approach to secure shared data in an IoT environment," Lin *et al.* propose a sanitization approach by adopting the hierarchical-cluster method to hide confidential information while still discovering useful and meaningful information in the sanitized dataset. In addition, the multi-objective particle swarm optimization framework and an algorithm known as HCMPSO are utilized to balance four side effects, namely hiding failure, missing cost, artificial cost, and database dissimilarity (Dis), and to thereby provide optimized solutions for data sanitization.

In the article "A secure and privacy preserving partial deterministic RWP model to reduce overlapping in IoT sensing environment," by Hosen *et al.*, the authors propose a secure and privacy-preserving node mobility model in which the nodes take part in periodic rounds securely. An identity (ID)-based authentication mechanism for joining nodes in the network and a method for detection of malicious nodes based on their survival strategies are proposed in the model.

In the article "MSCryptoNet: Multi-scheme privacy-preserving deep learning in cloud computing," by Kwabena *et al.*, the authors propose a novel framework, called MSCryptoNet, which enables the scalable execution and conversion of a state-of-the-art learned neural network to MSCryptoNet models in the privacy-preservation context. The authors also design a method for approximation of the activation function used as the basis of the convolutional neural network (i.e., Sigmoid and Rectified linear unit) with low-degree polynomials, which is vital for computations in homomorphic encryption schemes.

In the article "Privacy leakage in smart homes and its mitigation: IFTTT as a case study," by Xu *et al.*, the authors investigate how IFTTT ("If This, Then That"), one of the most popular smart home platforms, has the capability to monitor the daily life of a user in a variety of ways that are hardly noticeable. In addition, the authors propose multiple ideas for mitigating privacy leakages, which when taken together form a "Filter-and-Fuzz" (F&F) process. This involves first filtering out events that are unneeded by the IFTTT platform and then fuzzifying the values and frequencies of the remaining events.

In the article "Privacy-preserving wildcards pattern matching protocol for IoT applications," by Qin *et al.*, the authors propose a new protocol using secret sharing and oblivious transfer (OT), and later improve its efficiency with OT extension, making the protocol very efficient for lightweight IoT devices. In addition, the protocol supports queries with wildcards that can be used for the batch search. This protocol is provably secure against honest-but-curious adversaries.

Finally, the invited article "A new weight-and sensitivity-based variable maximum distance to average vector algorithm for wearable sensor data privacy protection," by Zhang *et al.*, tackles the problem of privacy protection with wearable devices when published data can be solved based on the variable-maximum distance average vector. This article proposes a new weight- and sensitivity-based variable maximum distance average vector (WSV-MDAV) method aiming at solving the problems germane to the existing privacy protection algorithm. The proposed approach considers the differential importance among all the identifiers by assigning them corresponding weight coefficients.

The Guest Editors hope that this Special Section will benefit the scientific community and contribute to the extant knowledge base and would like to thank the authors for their contributions. In addition, they highly appreciate the contributions of the reviewers for their constructive comments and suggestions. Finally, the Guest Editors would like to

acknowledge the guidance from IEEE Access Editor-in-Chief and other staff members.

KUO-HUI YEH, *Guest Editor*
Department of Information Management
National Dong Hwa University
Hualien 97401, Taiwan

WEIZHI MENG, *Guest Editor*
Department of Applied Mathematics and Computer Science
Technical University of Denmark
2800 Lyngby, Denmark

SK HAFIZUL ISLAM, *Guest Editor*
Department of Computer Science and Engineering
Indian Institute of Information Technology Kalyani
Kalyani 741235, India

KUAN ZHANG, *Guest Editor*
Department of Electrical and Computer Engineering
University of Nebraska-Lincoln
Lincoln, NE 68588, USA

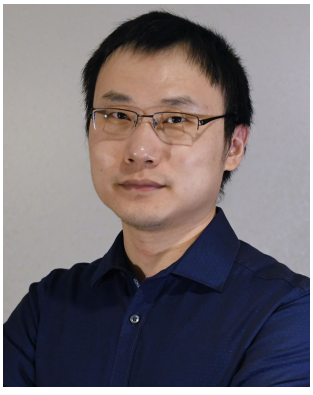
ENNAN ZHAI, *Guest Editor*
Alibaba Group
Bellevue, WA 98004, USA

KUO-HUI YEH (Senior Member, IEEE) received the M.S. and Ph.D. degrees in information management from the National Taiwan University of Science and Technology, Taipei, Taiwan, in 2005 and 2010, respectively. He is currently a Full Professor with the Department of Information Management, National Dong Hwa University, Hualien, Taiwan. He has authored over 100 articles in refereed journals and conferences. His research interests include the IoT security, blockchain, mobile security, NFC/RFID security, authentication, digital signature, data privacy, and network security. He is a member of the ACM. In addition, he has served as a TPC member for 40 international conferences/workshops on information security. He is also an Associate/Academic Editor of the *Journal of Information Security and Applications* (JISA), IEEE Access, *Security and Communication Networks* (SCN), the *Journal of Internet Technology* (JIT), and *Frontiers in Communications and Networks-Security, Privacy and Authentication*, and has served as a Guest Editor for *Future Generation Computer Systems* (FGCS), IEEE Access, *Annals of Telecommunications*, *Computers, Materials and Continua* (CMC), *Mathematical Biosciences and Engineering* (MBE), and the *International Journal of Information Security* (IJIS), JIT, *Sensors*, and *Cryptography*.

WEIZHI MENG received the B.Eng. degree in computer science from the Nanjing University of Posts and Telecommunications, China, and the Ph.D. degree in computer science from the City University of Hong Kong (CityU), Hong Kong. He is currently an Assistant Professor with the Department of Applied Mathematics and Computer Science, Technical University of Denmark (DTU), Kongens Lyngby, Denmark. He was previously known as Yuxin Meng, and prior to joining DTU, he worked as a Research Scientist with the Infocomm Security (ICS) Department, Institute for Infocomm Research, A∗STAR, Singapore, and as a Senior Research Associate with CityU after graduation. His primary research interests are cybersecurity and intelligent technology in security, including intrusion detection, smartphone security, biometric authentication, HCI security, cloud security, trust computing, malware detection, cyber-physical system security, and the IoT security. He also has a strong interest in applied cryptography. He is a member of the ACM and the IEEE Computer Society/IEEE Communications Society. He won the Outstanding Academic Performance Award during his doctoral study and is a recipient of the Hong Kong Institution of Engineers (HKIE) Outstanding Paper Award for Young Engineers/Researchers in both 2014 and 2017, as well as a co-recipient of the Best Student Paper Award from the 10th International Conference on Network and System Security (NSS) in 2016.

SK HAFIZUL ISLAM received the M.Sc. degree in applied mathematics from Vidyasagar University, Midnapore, India, in 2006, and the M.Tech. degree in computer applications and the Ph.D. degree in computer science and engineering from the Indian Institute of Technology [IIT (ISM)] Dhanbad, Jharkhand, India, in 2009 and 2013, respectively, under the INSPIRE Fellowship Ph.D. Program funded by the Department of Science and Technology, Government of India. He is currently an Assistant Professor with the Department of Computer Science and Engineering, Indian Institute of Information Technology Kalyani (IIIT Kalyani), West Bengal, India. Before joining IIIT Kalyani, he was an Assistant Professor with the Department of Computer Science and Information Systems, Birla Institute of Technology and Science, Pilani (BITS Pilani), Rajasthan, India. He has more than five years of teaching and eight years of research experience. He has authored or coauthored 70 research papers in journals and published in the proceedings of conferences of international repute. His research interests include cryptography, information security, WSNs, the IoT, and cloud computing.

KUAN ZHANG joined the Electrical and Computer Engineering Department, University of Nebraska–Lincoln (UNL), as an Assistant Professor, in September 2017. He was a Postdoctoral Fellow with the University of Waterloo, Canada, from 2016 to 2017. His research interests include broad areas of cybersecurity and cyber-physical systems, including network and system security, privacy, big data analysis, social networks, e-healthcare systems, vehicular communications, cloud/edge computing, and the Internet of Things. He was a recipient of the Best Paper Award at the IEEE WCNC 2013 and Securecomm 2016.



ENNAN ZHAI received the Ph.D. degree from Yale University in 2015, under the guidance of Dr. Bryan Ford. He joined the Alibaba Group Seattle as a Staff Engineer/Researcher in June 2018. In addition, he is an Associate Research Scientist with the Computer Science Department, Yale University. His dissertation work (published in OSDI'14) focused on building the first cloud-reliability auditing system (known as Independence-as-a-Service or INDaaS) that can proactively detect deep, unexpected dependencies that have the potential to cause cloud-scale correlated failures. His research focuses on building secure and reliable systems by utilizing techniques in areas including distributed systems, programming languages, and cryptography. He is currently working on enhancing the reliability and safety of large-scale distributed systems by proposing efficient, accurate, and deep auditing techniques. He is also working on building PriFi—the first low-latency and tracking-resistant anonymous communication system.