IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Digital Object Identifier 10.1109/ACCESS.2020.3021604

EDITORIAL

IEEE ACCESS SPECIAL SECTION EDITORIAL: ARTIFICIAL INTELLIGENCE IN CYBERSECURITY

I. INTRODUCTION

The Internet has a significant impact on people's daily lives and work. Recent studies claim that Artificial Intelligence (AI) has resulted in advances of many scientific and technological fields, that is, AI-based medicine, AI-based transportation, and AI-based finance. The era of AI is upon us. As one of the biggest concerns, security is of significance to the development of a sustainable, resilient, and prosperous Internet ecosystem. However, cybersecurity still faces many challenging issues such as intrusion detection, privacy protection, proactive defense, anomalous behaviors, advanced threat detection, and so on. In addition, many threat variations emerge and spread continuously. AI-assisted self-adaptable approaches are expected to deal with these security issues. A joint consideration of the interweaving nature between AI and cybersecurity is a key factor for driving future secure Internet.

This Special Section of IEEE Access on AI technologies in cybersecurity and related issues aims at bringing the researchers together to disseminate their findings in the field of AI-related theory analysis for security and privacy while pushing forward potential cooperation with related engineering fields in the context of AI in cybersecurity.

The Call for Papers aroused great enthusiasm in the scientific community and received a lot of submissions. Among these, 30 articles were accepted for inclusion in this Special Section after a thorough review process by at least two independent referees. Theese accepted articles can be broadly categorized into three groups: the first, with ten articles, mainly tackles network security detection. The second group, consisting of another ten articles, addresses data privacy protection and authentication issues. Finally, the third group, which includes the last ten articles, focuses on AI-based cybersecurity in different industrial applications.

In the first group, the article, "Harnessing artificial intelligence capabilities to improve cybersecurity," by Zeadally *et al.*, explores AI's potential in improving cybersecurity solutions.

The article "Classification hardness for supervised learners on 20 years of intrusion detection data," by D'hooge *et al.*, surveys the classification of supervised machine learning methods on network intrusion detection data under increasingly difficult conditions, through an evaluation of public data sets that cover 20 years of data generation.

The article "An optimization method for intrusion detection classification model based on deep belief network," by Wei *et al.*, proposes a new joint optimization algorithm to optimize the intrusion detection classification model based on deep belief network.

The article "An adaptive ensemble machine learning model for intrusion detection," by Gao *et al.*, proposes an adaptive ensemble learning model to integrate the advantages of algorithms for different types of data detection and achieves optimal results through ensemble learning.

The article "Performance evaluation of a combined anomaly detection platform," by Monshizadeh *et al.*, introduces an efficient platform named Hybrid Anomaly Detection Model (HADM), which can filter network traffic and identify malicious activities on the network.

The article "SMASH: A malware detection method based on multi-feature ensemble learning," by Dai *et al.*, proposes a malware dynamic detection method based on mufti-feature ensemble learning. The method adopts the combination of software features with high-detection precision and low-level hardware features.

The article "Machine learning based file entropy analysis for ransomware detection in backup systems," by Lee *et al.*, proposes to use machine learning for classifying infected files based on file entropy analysis. The proposed method can recover the original file from the backup system by detecting ransomware-infected files that have been synchronized to the backup system.

The article "An empirical evaluation of deep learning for network anomaly detection," by Malaiya *et al.*, designs and examines deep learning models constructed based on fully connected networks, variational auto encoder, and sequence-to-sequence structures.

The article "Cyber threat detection based on artificial neural networks using event profiles," by Lee *et al.*, develops an AI-SIEM system based on a combination of event profiling for data preprocessing and different artificial neural network methods.

The article "Abnormal behavior detection scheme of UAV using recurrent neural networks," by Xiao *et al.*, proposes a UAV abnormal behavior detection scheme using Recurrent Neural Networks.

In the second group, the article "Securing data with blockchain and AI," by Wang *et al.*, proposes a secure networking architecture (named SecNet) to significantly improve the security of data sharing and the security of the whole network.

The article ‘‘Smart contract-based secure model for miner registration and block validation,’’ by Zhang and Lee, designs a new smart contract-based model that is secure against rewriting-history attacks.

The article ‘‘APDP: Attack-proof personalized differential privacy model for a smart home,’’ by Zhang *et al.*, introduces a smart home model based on fog computing and secured by differential privacy, and applies a personalized differential privacy scheme to provide privacy protection.

The article ‘‘Latent-space-level image anonymization with adversarial protector networks,’’ by Kim and Yang, proposes a privacy-preserving adversarial protector network as an image anonymization tool to convert an image into another synthetic image that is immune to model inversion attacks.

The article ‘‘A machine learning framework for biometric authentication using electrocardiogram,’’ by Kim *et al.*, introduces a framework for electrocardiogram-based biometric authentication in order to mitigate identified challenges on ECG authentication.

The article ‘‘Certificateless deniable authenticated encryption for location-based privacy protection,’’ by Chen *et al.*, proposes a certificateless deniable authenticated encryption scheme based on certificateless cryptosystems, which avoids managing public key certificates in public key infrastructure-based cryptosystems and key escrow problems in identity-based cryptosystems.

The article ‘‘In-air gesture interaction: Real time hand posture recognition using passive RFID tags,’’ by Cheng *et al.*, proposes a real-time static and dynamic gesture recognition system for in-air interaction using the backscatter communication between the battery-free passive tags and the RFID reader.

The article ‘‘An enhanced electrocardiogram biometric authentication system using machine learning,’’ by Al Alkeem *et al.*, proposes a versatile RRIF biometric authentication system which uses a regression-based interpretable ML approach with the new Overall Performance (OP) measure based on the data quality.

The article ‘‘Learning based adaptive network immune mechanism to defense eavesdropping attacks,’’ by Liu *et al.*, proposes a learning-based adaptive network immune mechanism to prevent eavesdropping attacks.

The article ‘‘Technical mapping of the grooming anatomy using machine learning paradigms: An information security approach,’’ by Zambrano *et al.*, uses a database of real cyber-pedophile chats and proposes latent dirichlet allocation topic modeling to determine the stages of the attack.

In the third group, the article ‘‘BiN: A two-level learning-based bug search for cross-architecture binary,’’ by Wu *et al.*, proposes a cross-platform large-scale binary vulnerability search method based on two-level feature semantic learning to alleviate the vast differences in the assembly codes caused by different compilation scenarios.

The article ‘‘DeepTAL: Deep learning for TDOA-based asynchronous localization security with measurement error and missing data,’’ by Xue *et al.*, proposes an improved localization algorithm for source localization using deep learning to address TDOA measurement errors or missing data in an asynchronous localization.

The article ‘‘Blog reliability analysis with conflicting interests of contexts in the extended branch for cyber-security,’’ by Ko *et al.*, proposes a method to define a fake blogger’s features by analyzing the blogger’s tendency on comments and blog posts, including photos.

The article ‘‘Sina weibo bursty event detection method,’’ by Yang *et al.*, proposes a bursty event detection method for quantifying the influence of microblog text.

The article ‘‘Visualize your IP-over-optical network in realtime: A P4-based flexible multilayer in-band network telemetry (ML-INT) system,’’ by Niu *et al.*, designs a P4-based flexible multilayer in-band network telemetry system to visualize an IP-over-optical network in real time.

The article ‘‘Steganalysis of AMR speech based on multiple classifiers combination,’’ by Tian *et al.*, presents a novel steganalysis scheme based on multiple classifiers combination, which focuses on steganalysis in adaptive multi-rate speech streams to detect covert communication behaviors effectively to prevent illegal uses of AMR steganography.

The article ‘‘A Q-learning based scheme to securely cache content in edge-enabled heterogeneous networks,’’ by Dai *et al.*, proposes a cooperative scheme between edge server and content provider in HetNets to improve the performance of content delivery, and proposes a Q-learning based scheme for content caching to improve the hit ratio.

The article ‘‘A rerouting framework against routing interruption for secure network management,’’ by He *et al.*, proposes a fast rerouting framework for routing interruption, which consists of two parts: diagnosing routing interruption and implementing fast rerouting.

The article ‘‘Ontology-based security context reasoning for power IoT-cloud security service,’’ by Choi and Choi, proposes a security context ontology model by analyzing the security vulnerabilities of a power system in a power IoT–Cloud environment and defines the security context inference rules.

The article ‘‘AID shuffling mechanism based on group-buying auction for identifier network security,’’ by Guan *et al.*, proposes an artificial intelligence based method called three-stage auction mechanism for identifier allocation, to promote the security of access network in identifier network.

Finally, the Lead Editor and all the Guest Editors would like to express their gratitude to all the authors who submitted their research articles to our Special Section. They highly appreciate the contributions of the volunteering reviewers for their constructive comments and suggestions. They would also like to acknowledge the guidance from the Editor-in-Chief and the entire IEEE ACCESS staff.

CHI-YUAN CHEN, *Associate Editor*
Department of Computer Science
and Information Engineering
National Ilan University
Yilan 260, Taiwan

WEI QUAN, *Guest Editor*
Beijing Jiaotong University
Beijing 100044, China

NAN CHENG, *Guest Editor*
Department of Electrical
and Computer Engineering
University of Waterloo
Waterloo, ON N2L 3G1, Canada

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

JONG-HYOUK LEE, *Guest Editor*
Department of Computer
and Information Security
Sejong University
Seoul 05006, South Korea

GREGORIO MARTINEZ PEREZ, *Guest Editor*
Departamento de Ingenieria de la
Informacion y las Comunicaciones (DIIC)
University of Murcia (UMU)
30100 Murcia, Spain

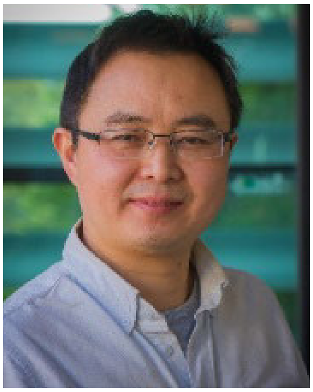
HONGKE ZHANG, *Guest Editor*
School of Electronic and
Information Engineering
Beijing Jiaotong University
Beijing 100044, China

SHIUHPYNG SHIEH, *Guest Editor*
Department of Computer Science
and Information Engineering
National Chiao Tung University
Hsinchu 30010, Taiwan

CHI-YUAN CHEN (Senior Member, IEEE) received the Ph.D. degree in electrical engineering from National Dong Hwa University in 2014. Since 2014, he has been with National Ilan University, where he is currently an Associate Professor with the Department of Computer Science and Information Engineering. He has authored or coauthored more than 70 international journal and conference papers, published in journals and magazines, including *IEEE Network*, *IEEE Communications Magazine*, the IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, and IEEE ACCESS. His research interests include mobile communication, network security, and quantum communication. He has served as the Editor-in-Chief for *Communications of the CCISA (CCCISA)*, the Executive Editor-in-Chief for the *Journal of Internet Technology (JIT)*, and an Associate Editor for IEEE ACCESS, *IET Networks*, *Human-Centric Computing and Information Sciences (HCIS)*, and the *Journal of Computers (JoC)*. He is an Editorial Board Member of the *International Journal of Smart Grid and Green Communications (IJSGGC)*.

WEI QUAN received the Ph.D. degree from the Beijing University of Posts and Telecommunications (BUPT) in 2014. He worked as a Postdoctoral Fellow from 2014 to 2016. He is currently an Assistant Professor with the School of Electronic and Information Engineering, Beijing Jiaotong University (BJTU), China. His research interests include key technologies for the future Internet, 5G network architecture, vehicular networks, and Internet of Energy. He has published more than 20 papers in prestigious international journals and conferences, including *IEEE Communications Magazine*, the IEEE WIRELESS COMMUNICATIONS, *IEEE Network*, the IEEE COMMUNICATIONS LETTERS, IFIP Networking, and the IEEE Wireless Communications and Networking Conference (WCNC). He has also served as a technical reviewer for some important international journals and conferences.

NAN CHENG received the B.E. and M.S. degrees from the Department of Electronics and Information Engineering, Tongji University, Shanghai, China, in 2009 and 2012, respectively, and the Ph.D. degree from the Department of Electrical and Computer Engineering, University of Waterloo, in 2015. He is currently a Postdoctoral Fellow with the Department of Electrical and Computer Engineering, University of Toronto, Toronto, ON, Canada, under the supervision of Prof. B. Liang. His current research focuses on big data in vehicular networks and self-driving systems. His research interests also include performance analysis, MAC, opportunistic communication for vehicular networks, cognitive radio, WiFi, smart grids, and cellular traffic offloading.



SHUI YU (Senior Member, IEEE) is currently a Professor with the School of Computer Science, University of Technology Sydney, Ultimo, NSW, Australia. His research interests include network science, security and privacy, big data, and mathematical modeling. He has published two monographs, edited two books, and published more than 350 technical papers in top journals and conferences, such as the 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/ACM TRANSACTIONS ON NETWORKING, and INFOCOM. He initiated the research field of networking for big data in 2013. His H-index is 46. He is also serving on a number of prestigious editorial boards, including the IEEE COMMUNICATIONS SURVEYS AND TUTORIALS (Area Editor) and *IEEE Communications Magazine*. He is a member of AAAS and ACM, and a Distinguished Lecturer of the IEEE Communication Society.

JONG-HYOUK LEE received the Ph.D. degree in computer engineering from Sungkyunkwan University, Suwon, South Korea. In 2009, he joined INRIA, France, where he undertook the protocol design and implementation for IPv6 vehicular communication and security. He started his academic profession with TELECOM Bretagne, France, in 2012, as an Assistant Professor. In 2013, he moved to Sangmyung University, Cheonan, South Korea. In March 2020, he joined the Department of Computer and Information Security, Sejong University, as an Associate Professor. He is an author of the Internet Standards: IETF RFC 8127 and IETF RFC 8191. His research interests include blockchain, malware analysis, and protocol analysis. He received the Best Paper Award at the IEEE WiMob 2012 and the Best Land Transportation Paper Award from the IEEE Vehicular Technology Society in 2015. He received the Haedong Young Scholar Award in 2017. He was a Tutorial Speaker at the IEEE WCNC 2013, the IEEE VTC 2014 Spring, and the IEEE ICC 2016. He was introduced as the Young Researcher of the Month by the National Research Foundation of Korea Webzine in 2014. He is an Associate Editor of the IEEE TRANSACTIONS ON CONSUMER ELECTRONICS and *IEEE Consumer Electronics Magazine*.

GREGORIO MARTINEZ PEREZ received the Ph.D. degree in computer science from the University of Murcia, Spain. He has been working as a Visiting Researcher with a few universities around Europe. He is currently a Full Professor with the Department of Information and Communications Engineering, University of Murcia. He has published more than 200 journal articles and conference papers in his areas of expertise. His research interests include cybersecurity and data science. He has been involved and leading more than 20 European and international research and development projects and contracts in the last ten years. He is a member of the program committee of a number of international conferences. He is also on the Editorial Board of 16 international journals.

HONGKE ZHANG received the M.S. and Ph.D. degrees in electrical and communication systems from the University of Electronic Science and Technology of China, Chengdu, China, in 1988 and 1992, respectively. From 1992 to 1994, he was a Postdoctoral Researcher with Beijing Jiaotong University, Beijing, China, where he is currently a Professor with the School of Electronic and Information Engineering and the Director of the National Engineering Laboratory for Next Generation Internet Technologies. His research interests include future Internet architecture and next-generation network technologies. His research has resulted in many articles, books, patents, systems, and equipment in the areas of communications and computer networks. He is the author of more than ten books and the holder of more than 80 patents. He is the Chief Scientist of the National Basic Research Program of China (973 Program) and has also served on the Editorial Boards of several international journals.

SHIUHPYNG SHIEH (Fellow, IEEE) received the M.S. and Ph.D. degrees in electrical and computer engineering from the University of Maryland, College Park, MD, USA. He is currently a University Chair Professor with the Computer Science Department and the Director of the Taiwan Information Security Center, National Chiao Tung University (NCTU). His research interests include system penetration and protection, malware behavior analysis, and network and system security. He has served as an Advisor for the National Security Council of Taiwan, the Chair of the Department of Computer Science, NCTU, and the President of the Chinese Cryptology and Information Security Association (CCISA). Being actively involved in the IEEE, he has served as the Editor-in-Chief for the IEEE Reliability, RS Newsletter, and Reliability Society VP Tech, and an Editor for the IEEE TRANSACTIONS ON RELIABILITY and the IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING. He has also served as an ACM SIGSAC awards committee member, an Associate Editor for the *ACM Transactions on Information and System Security*, the *Journal of Computer Security*, the *Journal of Information Science and Engineering*, and the *Journal of Computers*, and the Guest Editor for the IEEE INTERNET COMPUTING. Furthermore, he was on the organizing committees of many conferences, such as the Founding Steering Committee Chair and the Program Chair of the ACM Symposium on Information, Computer, and Communications Security (AsiaCCS), the Steering Committee Chair of the IEEE Conference on Dependable and Secure Computing, and the Program Chair of the IEEE Conference on Security and Reliability. Along with Virgil Gligor of Carnegie Mellon University, he invented the first U.S. patent in the intrusion detection field, and has published 200 technical articles, patents, and books. He is an ACM Distinguished Scientist, the IEEE Reliability Society Distinguished Engineer of the Year, and a Distinguished Professor of the Chinese Institute of Electrical Engineers.