IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Digital Object Identifier 10.1109/ACCESS.2020.3036713

EDITORIAL

IEEE ACCESS SPECIAL SECTION: SECURITY ANALYTICS AND INTELLIGENCE FOR CYBER PHYSICAL SYSTEMS

A Cyber Physical System (CPS) is a smart network system with actuators, embedded sensors, and processors to interact with the physical world by guaranteeing the performance and supporting real-time operations of safety critical applications. These systems drive innovation and are a source of competitive advantage in today's challenging world. By observing the behavior of physical processes and activating actions, CPS can alter its behavior to make the physical environment perform better and more accurately. By definition, CPS basically has two major components including cyber systems and physical processes. Examples of CPS include autonomous transportation systems, robotics systems, medical monitoring, automatic pilot avionics, and smart grids. Advances in CPS will empower scalability, capability, usability, and adaptability, which will go beyond the simple systems of today. At the same time, CPS has also increased cybersecurity risks and attack surfaces. Cyber attackers can harm such systems from multiple sources while hiding their identities. As a result of sophisticated threat matrices, insufficient knowledge about threat patterns, and industrial network automation, CPS has become extremely insecure. Since such infrastructure is networked, attacks can be prompted easily without much human participation from remote locations, thereby making CPS more vulnerable to sophisticated cyber-attacks. In turn, large-scale data centers managing a huge volume of CPS data become vulnerable to cyber-attacks. To secure CPS, the role of security analytics and intelligence is significant. It brings together huge amounts of data to create threat patterns, which can be used to prevent cyber-attacks in a timely fashion. The primary objective of this Special Section in IEEE Access is to collect a complementary and diverse set of articles, which demonstrate up-to-date information and innovative developments in the domain of security analytics and intelligence for CPS.

Our Call for Papers received a total of 58 high-quality submissions contributed by industry and academia, which were evaluated based on their quality, precision, and relevance to the theme of the Special Section. Out of them, 22 articles have been accepted for publication after a rigorous review process. The contents of these submissions are summarized below.

In the article by Li *et al.*, "A ciphertext-policy attribute-based encryption based on an ordered binary decision diagram," the authors presented a Ciphertext-Policy Attribute-Based Encryption (CP-ABE) system based on the Ordered Binary Decision Diagram (OBDD) for ensuring the security of CPS and the Internet of Things (IoTs). The proposed scheme utilizes both the high calculating efficiency and powerful description ability of OBDD in order to improve the performance.

The article titled "Context-aware verifiable cloud computing," by Yan *et al.*, proposes a context-aware verifiable computing scheme based on fully homomorphic encryption in order to verify the accurateness of the processed results of encrypted data stored in the cloud. To serve this process, four different auditing protocols were designed by the researchers, which satisfy the security requirements. Furthermore, the performance of these protocols was evaluated through system simulation, algorithm implementation, and performance analysis.

In the work by Ali *et al.*, "An automatic digital audio authentication/forensics system," the authors propose a novel automatic authentication system with the ability to distinguish between original and forged audio. The proposed system categorizes audio from different environments recorded with the same microphone based on the psychoacoustic principles of hearing. For authentication, the Gaussian mixture model has been applied in order to make automatic decisions.

Lu *et al.*, in the work titled "Depth map reconstruction for underwater Kinect camera using inpainting and local image mode filtering," investigate the problem of underwater optical imaging used for security monitoring in oceans. To overcome shortcomings of the underwater image processing techniques, this research article proposes a Kinect-based underwater depth map estimation method. The proposed approach demonstrated high-accuracy results.

In the article "A novel Internet of Things-centric framework to mine malicious frequent patterns," Usman *et al.* developed a framework for mining malicious frequent patterns for detecting misuse and distinguishing anomalies in an IoT deployment. This framework is then assessed by using three important ARM techniques including Apriori, FP-Growth, and Prefixspan from a Pakistan-based organization.

The article by Wang *et al.*, "Verification of implementations of cryptographic hash functions," is concerned with the verification of cryptographic hash functions through the precision of protocol consistency. This article proposes an automated verification framework, VeriHash, which presents an innovative cryptographic model design in order to model semantics of hash function implementations, compositional verification for scalability, and protracted array theories for operations analysis. The proposed verification framework has been evaluated on two SHA-3 implementations.

In the article by Wang *et al.*, ‘‘A fast feature fusion algorithm in image classification for cyber physical systems,’’ the authors studied challenges associated with the establishment of Cyber Physical Systems (CPS) with image classification systems. The main contribution of this research is the fast feature fusion algorithm based on genetic algorithm, dynamic weight assignment, and partial selection method for CPS image classification. The experimental results demonstrate that the proposed approach can attain high classification accuracy with lower hardware consumption and training time.

In the article by Chen *et al.*, ‘‘Fast trajectory planning and robust trajectory tracking for pedestrian avoidance,’’ the authors address the problem of pedestrian avoidance, due to which a high percentage of pedestrian accidents occur all over the world. The research proposed a method to quickly identify a feasible path for pedestrian avoidance while guaranteeing its feasibility.

In the article by Liu *et al.*, ‘‘SEDEA: State estimation-based dynamic encryption and authentication in smart grid,’’ the authors address security issues present in the communication between Remote Terminal Units (RTUs) and Control Center (CC) in the smart grid through SEDEA. This scheme uses commands from CC and measurements reported from RTUs to generate encryption keys. Moreover, such an approach updates its key regularly in order to ensure secure communication.

In the article by Khan *et al.*, ‘‘A continuous change detection mechanism to identify anomalies in ECG signals for WBAN-based healthcare environments,’’ the researchers have paid attention to an important concern regarding forgery of ECG data being transmitted from sensors to Personal Server (PS). This research makes use of a simplified Markov model-based detection mechanism to determine that intrusion has been occurred.

The article ‘‘Evidential network modeling for cyber-physical system state inference,’’ by Friedberg *et al.*, discusses monitoring of CPS to detect deviances from normal operations in order to support timely and accurate control decisions. This research presented evidential networks for state inference in CPS, which assists in identifying causality between higher and lower level system states.

The work by Xu *et al.*, ‘‘Achieving efficient detection against false data injection attacks in smart grid,’’ discusses an efficient real-time decision scheme to prevent False Data Injection Attack (FDIA) in state estimation. It is widely used in system monitoring of smart grids. The simulation results demonstrated that the scheme is efficient.

The work titled ‘‘Privacy preservation in e-Healthcare environments: State of the art and future directions,’’ by Sahi *et al.*, presents the challenges in preserving the privacy of patient records in e-Healthcare. Furthermore, this research also reviews several privacy preservation mechanisms being deployed in e-Healthcare.

In the article ‘‘A novel data analytical approach for false data injection cyber-physical attack mitigation in smart grids,’’ Wang *et al.* developed a data analytical approach based on a data-centric paradigm in order to detect False Data Injection Attacks (FDIAs). This research makes use of the Margin Setting Algorithm (MSA) to detect time attack and playback attack. The proposed scheme is then compared with two other popular schemes including Artificial Neural Network (ANN) and Support Vector Machine (SVM). The results demonstrate that the proposed approach works efficiently.

In the article by Mehmood *et al.*, ‘‘Secure knowledge and cluster-based intrusion detection mechanism for smart wireless sensor networks,’’ the authors present a knowledge-based context-aware scheme to deal with security issues present in wireless sensor networks (WSNs). This scheme manages intrusions produced by malicious nodes with the help of the knowledge base placed at the base station. Cluster Heads (CHs), in turn, gather categorized events from the knowledge base and block maliciously repeated activities.

Loukas *et al.*, in the work titled, ‘‘Cloud-based cyber-physical intrusion detection for vehicles using deep learning,’’ investigate the recognition of cyber-attacks against vehicles. Since vehicles can manage limited processing resources, lightweight techniques can be employed. This research covers such a limitation through computational offloading based on deep learning. This research has further developed a mathematical model to determine possessing and latency of the approach, which turns out to be efficient in case of a reliable network.

The research article by Li *et al.*, titled ‘‘Gender identification via reposting behaviors in social media,’’ studies gender identification over social networks through reposting behaviors. This research proposed an approach supported by homophily and four intuitive procedures by integrating knowledge of statistics and sociology. The experimental results demonstrate the accuracy of the proposed scheme.

In the work by Napiah *et al.*, ‘‘Compression header analyzer intrusion detection system (CHA-IDS) for 6LoWPAN communication protocol,’’ the authors present CHA-IDS, which addresses the detection of combined routing attacks by capturing and handling raw data for data collection, system actions, and data analysis. It makes use of correlation-based feature selection to determine required features, which are then tested by means of six machine learning algorithms. Experimental results demonstrate that the proposed scheme is efficient.

The article ‘‘A critical analysis of mobility management related issues of wireless sensor networks in cyber physical systems,’’ authored by Al-Muhtadi *et al.*, studied mobility management problems in CPS and WSN. The major contribution of this research is to evaluate existing mobility management approaches against quadruple set of metrics.

In the article by Cheon *et al.*, "Toward a secure drone system: Flying with real-time homomorphic authenticated encryption," the authors investigate security issues of networked vehicle systems. This research proposed a linearly homomorphic authenticated encryption (LinHAE) approach to secure vehicle systems against forgery and eavesdropping attacks.

The work titled "Security analysis of smartphone and cloud computing authentication frameworks and protocols," by Siddiqui *et al.*, addresses an important concern of today's world regarding the security and authenticity of information. The authors performed a review and security analysis of cloud computing and smartphone authentication protocols and frameworks to analyze authentication challenges.

The invited article "A survey on mobile edge networks: Convergence of computing, caching and communications," by Wang *et al.*, reviews mobile edge networks and issues associated with caching, communication technologies, and computing at the network edge. Furthermore, it presents use cases and applications of mobile edge networks and concludes with a review of several future directions.

Finally, the leading editor and the guest editors of the Special Section express their gratitude to the authors for their contributions to the volunteering referees for their dedication and to the whole IEEE ACCESS editorial staff for their invaluable support.

HAIDER ABBAS, *Lead Guest Editor*
National University of Sciences and Technology (NUST)
Islamabad 44000, Pakistan

HIROKI SUGURI, *Guest Editor*
Miyagi University
Miyagi 981-3298, Japan

ZHENG YAN, *Guest Editor*
Aalto University
02150 Espoo, Finland
Xidian University
Xi'an 710071, China

WILLIAM ALLEN, *Guest Editor*
Florida Institute of Technology
Melbourne, FL 32901, USA

XIALI (SHARON) HEI, *Guest Editor*
Delaware State University
Dover, DE 19901, USA

HAIDER ABBAS (Senior Member, IEEE) received the M.S. degree in engineering and management of information systems and the Ph.D. degree in information security from KTH, Sweden, in 2006 and 2010, respectively. He is a Cyber Security Professional, who received professional training and certifications from the Massachusetts Institute of Technology (MIT), Cambridge, MA, USA; Stockholm University, Sweden; IBM; and EC-Council. He is the principal advisor for several graduate and doctoral students at King Saud University, Saudi Arabia; National University of Sciences and Technology, Pakistan; and Florida Institute of Technology, Melbourne, FL, USA. He has also won many awards and received several research grants for ICT related projects from various research funding authorities and working on scientific projects in the USA, EU, Saudi Arabia, and Pakistan. He is an Associate Editor or on the editorial board for a number of international journals, including the IEEE JOURNAL OF BIOMEDICAL AND HEALTH INFORMATICS, *Journal of Network and Computer Applications*, *Electronic Commerce Research*, IEEE ACCESS, and *Cluster Computing*.

HIROKI SUGURI received the Ph.D. degree in software and information science from Iwate Prefectural University in 2004. He is currently a Professor of Informatics with the School of Project Design, Miyagi University, Japan. His research interests include distributed computing, system modeling, and project management. He served the Foundation for Intelligent Physical Agent as a Technical Committee Chair and the Director (1998–2001). He was the Chair of the technical group on software enterprise modeling in the Institute of Electronics, Information and Communication Engineers from 2015 to 2016. He was bestowed with a Distinguished Service Award by the Information and Systems Society of IEICE in 2017.

ZHENG YAN (Senior Member, IEEE) received the B.Eng. degree in electrical engineering and the M.Eng. degree in computer science and engineering from Xi'an Jiaotong University, in 1994 and 1997, respectively, the second M.Eng. degree in information security from the National University of Singapore, in 2000, and the Licentiate of Science and the Doctor of Science in Technology in electrical engineering from the Helsinki University of Technology, in 2005 and 2007, respectively. She is currently a Professor with Xidian University, Xi'an, China, and a Docent/Visiting Professor with Aalto University, Finland. She joined the Nokia Research Center, Helsinki, in 2000, working as a Senior Researcher until 2011. Prior to joining Nokia, she worked as a Research Scholar at the Institute for Information Research from 1997 to 1999, and a Software Engineer at the IBM partner SingaLab, Singapore, from 1999 to 2000. She has authored more than 120 peer-reviewed publications (95% first or the corresponding author) and solely authored two books. She is the inventor of ten patents and 35 PCT patent applications, 26 of which were solely invented. Her research interests are in trust, security and privacy, mobile applications and services, social networking, cloud computing, pervasive computing, and data mining. She serves as an Organizational Committee Member for more than 30 conferences and as a technical committee member for more than 50 international conferences and workshops. She is an Associate Editor of IEEE Access, IEEE IoT Journal, *Security and Communication Networks* (Wiley), *KSII Transactions on Internet and Information Systems*, and a special issue leading guest editor for more than ten journals, such as *Information Sciences, ACM TOMM*, *Information Fusion*, IEEE Systems Journal, *Future Generation Computer Systems*, *Computers & Security, SCN, IJCS*, ACM/Springer *MONET*, and *IET Information Security*, and acts as a Reviewer for many top journals. She was the Organizer of the IEEE TrustCom/BigDataSE/ISPA-2015, EAI MobiMedia2016, IEEE CIT2014/2017, CSS2014, ICA3PP2017, NSS2017, IEEE RACIT2014, IEEE GTWSM2014/2016, IEEE TrustID2011/2012/2013, IEEE DASC 2012, IEEE/IFIP DMIoT2013 with IEEE/IFIP EUC 2013, a special track about Pervasive Social Computing with UIC/ATC2010, and IEEE iThings 2012 security track. She serves as a Steering Committee or Organization Committee Member for more than 30 conferences and a TPC member for more than 50 conferences, i.e., GLOBECOM, ICSOC, ACM MobileHCI, ACM SAC, and so on.

WILLIAM ALLEN is currently an Associate Professor of Computer Sciences with the Florida Institute of Technology. He has served as an Assistant Professor with the Computer Sciences Department from 2003 to 2010, teaching a range of undergraduate and graduate courses, conducting both funded and unfunded research, and advising master's and Ph.D. students. From 1995 to 2003, he was a Lecturer of Computer Science with the University of Central Florida, teaching a wide range of undergraduate courses for computer science and information technology majors. His research interests include balancing usability with security and privacy, forensic analysis of digital data, and improving software design methodologies to develop more secure software.

XIALI (SHARON) HEI received the B.S. degree in electrical engineering from Xi'an Jiaotong University, the M.S. degree in software engineering from Tsinghua University, and the Ph.D. degree in computer science from Temple University, in 2014, focusing on computer security. Her advisors were Xiaojiang Du and Shan Lin. She is currently an Assistant Professor with the Department of Computer and Information Sciences, Delaware State University. Prior to joining Delaware State University, she was an Assistant Professor with Frostburg State University. She has received several awards, i.e., ACM 2014 MobiHoc Best Poster Runner-up Award, Dissertation Completion Fellowship, The Bronze Award Best Graduate Project in Future of Computing Competition, IEEE INFOCOM and IEEE GLOBECOM Student Travel Grant, and so on.

• • •