Guest Editorial: Special Section on Autonomous Intelligence for Security and Privacy Analytics

WE INTERACT with a wide variety of computing systems in our daily life. These computing systems are often connected through a network to provide a wide array of services. Depending on our specific circumstances, our interactions can be with embedded and cyber-physical systems (CPSs) or Internet-of-Things (IoT) devices. While these devices vary in terms of form factors, hardware–software integration, and energy constraints, they have one commonality—security and privacy are the primary design considerations. These systems collect and analyze sensitive data, which may include our personal, financial, as well as health information on a regular basis. As a result, the existing academic and industrial efforts have focused on designing systems with security and privacy in mind. Given the complexity of these systems and the diversity of the potential attacks, machine learning (ML) has become an attractive solution for security and privacy analytics.

ML has made its mark for detecting known software, firmware, as well as hardware vulnerabilities. There are also recent efforts to utilize learning to detect known unknowns (e.g., minor variation of known vulnerabilities) as well as unknown unknowns (e.g., major variation of known vulnerabilities). On the other hand, the security of the ML tool itself can be a critical concern. For example, recent fault injection attacks on neural networks show that modification of just a few parameters can lead to misclassification of a specified input pattern into an adversarial class. Likewise, side channels could also potentially be useful to leak the parameters of a trained ML tool, leading to IP issues. Clearly, there is a need for efficient solutions to ensure that the implementation of ML algorithms is robust against faults and side channels to enhance overall system security and privacy.

The articles in this special issue cover a wide variety of topics that investigate the impact of ML on IoT security and privacy analytics. We received many high-quality submissions for this special issue from two avenues: 1) we invited some of the top-rated articles from the International Conference on VLSI Design 2019 and 2) we also received several submissions based on the general call for articles for this journal. We selected the following ten articles after a rigorous two-stage review process.

The first article "Hardware Trojan detection using changepoint-based anomaly detection techniques" by Elnaggar *et al.* introduces an ML-based runtime hardware Trojan detection method for microprocessor cores. This approach uses a changepoint-based anomaly detection algorithm to detect the activation of Trojans that introduce abnormal patterns in the data streams obtained from performance counters. It does not modify the original microprocessor design to integrate on-chip monitoring sensors. They are able to detect the activation of Trojans that cause a denial-of-service (DoS), the degradation of system performance, and change in functionality of a microprocessor core.

The second article "Practical approaches toward deep-learning-based cross-device power side-channel attack" by Golder *et al.* presents profiling-based cross-device power SCA attacks using deep-learning techniques on 8-bit microcontroller devices running AES-128. The authors show that utilizing principal component analysis (PCA)-based preprocessing and multidevice training, a multilayer perceptron (MLP)-based 256-class classifier can achieve an average accuracy of 99.43% in recovering the first key byte from all the 30 devices in the data set, even in the presence of significant interdevice variations.

The third article "Efficient on-chip randomness testing utilizing machine learning techniques" by Mrazek *et al.* proposes a new hardware platform for randomness testing. The platform exploits the principles of genetic programming, which is an ML technique developed for the automated program and circuit design. The platform is capable of evolving efficient randomness distinguishers directly on a chip. Each distinguisher is represented as a Boolean polynomial in the algebraic normal form. Randomness testing is conducted for bitstreams that are either stored in an on-chip memory or generated by a circuit placed on the chip. The platform is evaluated in terms of the quality of randomness testing, performance, and resource utilization.

The fourth article "Memristor-based neuromorphic hardware improvement for privacy-preserving ANN" by Fu *et al.* proposes a linear optimization method to address the accuracy degradation by optimizing the performance of memristor in the weight updating processes. Instead of complying with the traditional hardware and algorithm, it calculates the update parameters along a piecewise line by using different input pulses. The proposed method can mitigate the nonlinear problem of memristor without prereading the precise current conductance each time, thereby avoiding complex peripheral circuits.

The fifth article "Toward secure microfluidic fully programmable valve array biochips" by Shayan *et al.* shows that fully programmable valve arrays (FPVAs) are vulnerable to malicious operations similar to digital and flow-based microfluidic biochips. FPVAs are further prone to new classes of attacks—tunneling and deliberate aging. The study establishes the

Digital Object Identifier 10.1109/TVLSI.2019.2951850

security metrics and describes possible attacks on real-life bioassays. Furthermore, it studies the use of ML techniques to detect and classify attacks based on the golden and real-time biochip state. In order to boost the classifier's performance, the authors propose a smart checkpointing mechanism.

The sixth article "Analysis of security of split manufacturing using machine learning" by Zeng *et al.* analyzes the security of split manufacturing using ML, based on the data collected from layouts provided by industry, with eight routing metal layers and significant variation in wire size and routing congestion across the layers. Many types of layout features are considered in their ML model, including those obtained from placement, routing, and cell sizes. The authors propose efficient techniques to make their ML model scalable with a minor impact on the effectiveness of the attack. They further improve the performance in the top routing layer by making use of higher quality training samples and by exploiting the routing convention.

The seventh article "Securing a wireless network-on-chip against jamming-based DoS and eavesdropping attacks" by Vashist *et al.* proposes a mechanism to make the wireless communication in a wireless network-on-chip (WiNoC) secure against persistent jamming-based DoS attacks and eavesdropping from both external and internal attackers. The authors use a burst error correction code to monitor the rate of burst errors received over the wireless medium and deploy an ML classifier to detect the persistent jamming attack and distinguish it from random burst errors. In the event of persistent jamming attack, alternate routing strategies are proposed to avoid the DoS attack over the wireless medium so that a secure data transfer can be sustained even in the presence of persistent jamming.

The eighth article "A blockchain-based privacy-preserving authentication scheme for VANETs" by Lu *et al.* proposes a privacy-preserving scheme for vehicular *ad hoc* networks (VANETs). It records all the certificates and transactions permanently and immutably in the blockchain to make the activities of the semitrusted authorities transparent and verifiable. With a novel data structure named the Merkle Patricia Tree, the authors extend the conventional blockchain structure to provide a distributed authentication scheme without the revocation list. To achieve conditional privacy, they allow a vehicle to use multiple certificates. The linkability between the certificates and the real identity is encrypted and stored in the blockchain and can only be revealed in case of any disputes.

The ninth article "A systematic evaluation of profiling through focused feature selection" by Picek *et al.* investigates how advanced feature selection techniques stemming from the ML domain can be used to improve the attack efficiency. The authors perform a systematic evaluation of the methods using data sets containing software and hardware implementations of AES, including the random delay countermeasure. Their results show that wrapper and hybrid feature selection methods perform extremely well over a wide range of test scenarios and a number of features selected. They show that the use of appropriate feature selection techniques is more important for an attack on the high-noise data sets, including those with countermeasures than on the low-noise ones.

The last article "High-performance CNN accelerator on FPGA using unified Winograd-GEMM architecture" by Kala *et al.* presents a unified architecture, where both Winograd-based convolution and general elementwise matrix multiplication (GEMM) can be accelerated using the same set of processing elements. This approach leads to efficient utilization of field-programmable gate array (FPGA) hardware resources while computing all layers in convolutional neural network (CNN). The proposed architecture shows the performance improvement in the range of $1.4\times$ to $4.02\times$ with only 13% additional FPGA resources with respect to the baseline GEMM-based architecture. The authors mapped popular CNN models, such as AlexNet and VGG-16, onto the proposed accelerator, and the measured performance compares favorably with other state-of-the-art implementations.

Finally, we would like to acknowledge the support of the IEEE Editorial Office throughout the selection and publication process of the special issue. We would also like to express our sincere gratitude to the dedicated reviewers who contributed their valuable time and effort during the review process. We hope that this collection of articles contributes to the active discussion among the researchers in both academia and industry on the role of ML in detecting a wide variety of security- and privacy-related attacks and developing effective countermeasures.

PRABHAT MISHRA, *Guest Editor*
Department of Computer and Information Science and Engineering
University of Florida
Gainesville, FL, USA

DEBDEEP MUKHOPADHYAY, *Guest Editor*
Department of Computer Science and Engineering
Indian Institute of Technology Kharagpur
Kharagpur, India

SWARUP BHUNIA, *Guest Editor*
Department of Electrical and Computer Engineering
University of Florida
Gainesville, FL, USA

Prabhat Mishra (SM'08) received the Ph.D. degree in computer science and engineering from the University of California at Irvine, Irvine, CA, USA, in 2004.

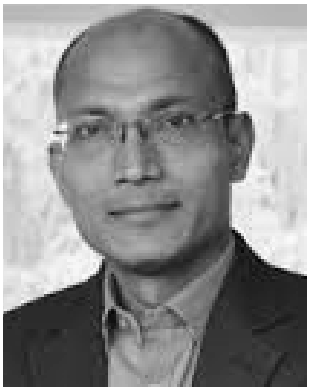
He is currently a Professor with the Department of Computer and Information Science and Engineering, University of Florida, Gainesville, FL, USA. He is also a UF Preeminence Term Professor, the Research Director of the Nelms Institute for the Connected World, and a member of the Florida Institute of Cybersecurity. His current research interests include embedded and cyber-physical systems, hardware security and trust, computer architecture, energy-aware computing, formal verification, system-on-chip validation, and quantum computing.

Dr. Mishra is a recipient of several awards, including the NSF CAREER Award, the IBM Faculty Award, ten best paper awards and nominations, and the EDAA Outstanding Dissertation Award. He serves as an Associate Editor for the *ACM Transactions on Design Automation of Electronic Systems*, the IEEE TRANSACTIONS ON VERY LARGE SCALE INTEGRATION (VLSI) SYSTEMS, and the *Journal of Electronic Testing*. He is also a Distinguished Scientist of ACM.

Debdeep Mukhopadhyay (SM'17) received the B.Tech., M.S., and Ph.D. degrees from IIT Kharagpur, Kharagpur, India, in 2001, 2004, and 2007, respectively.

He was a Visiting Scientist with Nanyang Technological University, Singapore; a Visiting Associate Professor with New York University Shanghai (NYU), Shanghai, China; an Assistant Professor with IIT Madras, Chennai, India; and a Visiting Researcher with the Tandon School of Engineering, NYU, New York, NY, USA. He is currently a Professor with the Department of Computer Science and Engineering, IIT Kharagpur, Kharagpur, India. He initiated the Secured Embedded Architecture Laboratory with a focus on embedded security and side-channel attacks. He has recently incubated a startup on hardware security, ESP Pvt. Ltd., Kharagpur. His current research interests include cryptography, hardware security, and VLSI.

Dr. Mukhopadhyay was a recipient of the prestigious Swarnajayanti DST Fellowship from 2015 to 2016, the Young Scientist Award from the Indian National Science Academy, the Young Engineer Award from the Indian National Academy of Engineers, the Outstanding Young Faculty Fellowship from IIT Kharagpur in 2011, and the Techno-Inventor Best Ph.D. Award by the Indian Semiconductor Association. He is in the program committee of several top international conferences. He serves as an Associate Editor for the *IACR Transactions on Cryptographic Hardware and Embedded Systems*, *ACM Transactions on Embedded Computing Systems*, the IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, and the *Journal of Cryptographic Engineering* (Springer). He is also a Young Associate of the Indian Academy of Science.



Swarup Bhunia (SM'87) received the B.E. degree (Hons.) from Jadavpur University, Kolkata, India, in 1995, the M.Tech. degree from IIT Kharagpur, Kharagpur, India, in 1997, and the Ph.D. degree from Purdue University, West Lafayette, IN, USA, in 2005.

He was appointed as the T. and A. Schroeder Associate Professor of Electrical Engineering and Computer Science at Case Western Reserve University, Cleveland, OH, USA. He is currently the Director of the Warren B. Nelms Institute for the Connected World and a Semmoto Endowed Chair Professor of IoT with the University of Florida, Gainesville, FL, USA. He has over 250 publications in peer-reviewed journals and premier conferences. His current research interests include hardware security and trust, adaptive nanocomputing, and novel test methodologies.

Dr. Bhunia received the IBM Faculty Award, the NSF CAREER Award, the SRC Inventor Recognition Award, the SRC Technical Excellence Award, and several best paper awards/nominations. He has been serving as an Associate Editor for the IEEE TRANSACTIONS ON COMPUTER-AIDED DESIGN OF INTEGRATED CIRCUITS AND SYSTEMS, the IEEE TRANSACTIONS ON MULTI-SCALE COMPUTING SYSTEMS, the *ACM Journal of Emerging Technologies*, and the *Journal of Low Power Electronics*.