From the Editor's Desk

Ubiquitous Connectivity of Consumer IoT Devices

Norbert Herencsar
Brno University of Technology

I WELCOME THE readers to the fourth issue of the year 2022, the July/August issue of the *IEEE Consumer Electronics Magazine* (MCE). Future communication networks are anticipated to significantly expand to connect many tens of billions of devices and support a wide range of consumer technology applications in healthcare, navigation, manufacturing industry, remote monitoring, and disaster management under the umbrella of the Internet-of-Things (IoT) paradigm. The expansion is supported by fifth-generation (5G) and technologies beyond that offer network slicing, reconfigurable connectivity, traffic steering, and flexible deployment options to improve the overall efficiency of applications and minimize interference. Security plays an essential role in communication networks for seamlessly connecting billions of IoT devices and ensuring operational efficiency while effectively utilizing resources. The Third-Generation Partnership Project has proposed dedicated 5G security functions that operate between IoT devices and the core. The discovery and placement of these functions, such as the authentication server function, the security anchor function, or the session management function, is challenging and depends on the types of applications and devices. Behavior modeling is pivotal for understanding new types of attacks in 5G and beyond IoT since adversaries are becoming intelligent. Therefore, it is my pleasure to introduce a collection of high-quality articles dedicated to consumer IoT devices in this issue.

Digital Object Identifier 10.1109/MCE.2022.3177030
Date of current version 7 June 2022.

FEATURE ARTICLES

Abusive Adversaries in 5G and Beyond IoT: The 5G and subsequent cellular network generations aim to extend the ubiquitous connectivity of billions of IoT for their consumers. This article investigates behavior modeling against abusive adversaries in the context of 5G and beyond security functions for IoT. A complexity security tradeoff enables a better understanding of the limitations of state-based behavior modeling. It paves the way for a future direction for developing more robust solutions against abusive modeling.

A Design of Smart Unmanned Vending Machine for New Retail Based on Binocular Camera and Machine Vision: In this article, a binocular camera system is designed to effectively solve the problems of distortion and coverage caused by a monocular camera. Besides, an image-stitching algorithm is developed. The results suggest that the designed method achieves the goal in terms of inference speed and average precision and it is able to satisfy the requirements for real-world consumer applications.

Fetus Heart Rate Monitoring—A Preliminary Implementation With Remote Sensing: In this article, an implementation of a system monitoring the fetus's heart rate has been designed and implemented as a mobile wearable measuring system with remote sensing. The proposed implementation is capable of patient monitoring using a smart or satellite phone, thus complying with the health safety distance measures required due to

Published by the IEEE Consumer Technology Society

various situations, including that of the COVID-19 pandemic.

HLDNet—Abandoned Object Detection Using Hand Luggage Detection Network: This article presents a deep learning-based detection method that is suitable for use in outdoor environments because it is robust to ghost effects and illumination changes. The proposed method can detect restricted hand luggage accessories and it can be applied for consumer applications.

KF-Loc—A Kalman Filter and Machine Learning Integrated Localization System Using Consumer-Grade Millimeter-Wave Hardware: This work uses consumer-grade millimeter-wave (mmWave) equipment to enable fast and low-cost implementation of a localization system. Compared with machine learning only localization systems, a significant reduction in root-mean-square error by 28.5% and 54.3% within the two investigated aisles was achieved.

Reliability and Security of Extreme Parallelism: This article provides a systematic overview of current reliability and security concerns in the context of extreme parallelism. Hardware failures that can lead to programming errors are presented. In addition, the security implications of parallel computing are discussed.

SPECIAL SECTION: 6TH IEEE INTERNATIONAL SYMPOSIUM ON SMART ELECTRONIC SYSTEMS (IEEE-ISES'20)

This Special Section is dedicated to the 6th Edition of the Symposium on Smart Electronic Systems (IEEE-iSES'20). The conference was hosted virtually due to the unprecedented situation caused by the COVID-19 pandemic. This Special Section presents a selected set of articles related to the MCE scope.

Humans in the Loop: Cybersecurity Aspects in the Consumer IoT Context: In this article, the need toward a human-centric approach to cybersecurity by shifting focus from *humans as a problem* to *humans as a solution* is investigated. A security and privacy-preserving framework for illustrating how a human-centric approach can be initiated, what are its essential components, and how security and privacy can be preserved with a human focus is proposed.

Application of Artificial Immune Recognition System for Monitoring the Brake System Using Vibration Based Statistical Learning: This study attempts to display the faults that occur in a brake system using vibration analysis through an artificial intelligence technique called an artificial immune recognition system. Based on the outcome, an electronics-based diagnostic module is proposed for categorizing and displaying the nature of brake faults in the infotainment system.

Hardware Software Co-design Framework for Data Encryption in Image Processing Systems for the IoT Environment: This article presents a hardware–software co-simulation of AES-128 bit encryption and decryption for IoT edge devices using the Xilinx system generator. Very high-speed integrated circuit hardware description language implementation of AES-128 bit algorithm is done. To give a practical example of the usage of the proposed framework, it was applied to biomedical images as a case study.

Design and Analysis of Secure Quasi-Adiabatic Tristate Physical Unclonable Function: This article discusses the hardware security modules, which have become quintessential as digital systems continue evolving. The physical unclonable function (PUF) is a hardware security module that exploits the intrinsic variations in the manufacturability of integrated circuits. The proposed quasi-adiabatic tristate PUF can be very effectively used for IoT and RFID applications requiring lower energy values to operate.

I would like to thank the Guest Editors, Professors Himanshu Thapliyal, Tosiron Adegbija, and Saraju P. Mohanty, for all the hard work for this Special Section which will be interesting reading for Consumer Technology Society (CTSoc) members.

LOOKING FORWARD

MCE will continue the trend of covering more themes for enthusiastic and dedicated readers in future issues on the current topics and emerging topics with the active support from the editorial board members, reviewers, and authors around the world.

Norbert Herencsar is an associate professor with the Department of Telecommunications, Brno University of Technology, Brno, Czech Republic. Herencsar received his Ph.D. degree in teleinformatics from the Brno University of Technology. He is a senior member of IEEE. Contact him at herencsn@ieee.org.