From the Editor's Desk

Security and Trust in Forthcoming Consumer IoT Systems

Norbert Herencsar
Brno University of Technology

I WELCOME THE readers to the third issue of the year 2023, the May/June Issue of the *IEEE Consumer Electronics Magazine* (*MCE*).

Consumer Internet of Things (CIoT) devices are becoming increasingly popular and pervasive, but they are often vulnerable to security breaches and attacks due to their lack of security features. The lack of security and trust in IoT devices poses a significant threat to consumer privacy and safety. As a result, research in the field of security and trust in forthcoming CIoT systems has gained a lot of attention in recent years. Various security and trust mechanisms have been proposed and implemented to address these concerns, including device authentication, access control, encryption, and data integrity checks. Some of the proposed solutions use blockchain technology to provide a tamper-proof and decentralized infrastructure, while others use machine learning algorithms to identify and prevent potential attacks. However, despite these solutions, consumer IoT devices remain vulnerable due to a lack of standardization and regulation and the use of legacy systems and outdated software. The complexity and diversity of IoT systems make it difficult to implement security and trust mechanisms uniformly across all devices. Therefore, there is a pressing need for standardization and regulation of security and trust mechanisms in consumer IoT devices to ensure the safety and privacy of users. This would involve collaboration between various stakeholders, including device manufacturers, regulators, and consumers, to develop common standards and best practices for security and trust in forthcoming consumer IoT systems.

In this issue of *MCE*, it is my pleasure to provide practitioners and researchers with high-quality, state-of-the-art articles dedicated to security and trust in forthcoming consumer IoT systems.

COLUMNS

Looking Beyond the Horizon: This article discusses how the business landscape has been disrupted in the past by emerging technologies, such as digital imaging and cloud downloads, and how current emerging technologies have the potential to do the same. The impacts of such disruptions on existing stakeholders will also be explored.

Metaverse Meets Consumer Electronics: Nowadays, different technical giants are separately promoting their metaverses resulting in "islands" of decentralized, multicentered metaverse systems. This column discussed the requirements of standards and corresponding communication protocols of the metaverse to build a unified, fully connected metaverse ecosystem.

Digital Object Identifier 10.1109/MCE.2023.3254319
Date of current version 8 April 2023.

Published by the IEEE Consumer Technology Society

FEATURE ARTICLES

Deep Neural Network (DNN) Migration in IoTs—Emerging Technologies, Current Challenges, and Open Research Directions: This article presents a framework for DNN model migration, comprising DNN model preprocessing, partition-offloading plan, and improved partition-uploading plan. The authors address challenges of achieving more efficient DNN migration and highlight unresolved issues for future research direction.

Decentralized ME-Centric Framework—A Futuristic Architecture for Consumer IoT: This article presents a decentralized ME-centric architecture for the CIoT, improving agility, scalability, resiliency, and security. It integrates edge computing, decentralized storage, digital twins, and blockchain with semantic ontologies to create a comprehensive outlook for consumers.

Managing the Far-Edge—Are Today's Centralized Solutions a Good Fit?: This work compares cloud and edge infrastructures, evaluating leading open-source edge solutions in terms of scalability and service instantiation time in a medium-sized far-edge system. Results suggest that mainstream edge solutions require powerful centralized controllers and stable, high-bandwidth connectivity, limiting their suitability for highly decentralized scenarios in the far edge.

Private Blockchain-Based AI-Envisioned Home Monitoring Framework in Internet of Medical Things (IoMT)-Enabled COVID-19 Environment: This article proposes a fog-based private blockchain-enabled home monitoring framework for the IoMT in a COVID-19 context. The article outlines the development phases and provides a practical demonstration of the proposed blockchain system for secure patient home monitoring.

Security Management on Arduino-Based Electronic Devices: This work analyzes vulnerabilities in Arduino boards, which are popular for their low cost, open hardware, and prototyping potential. The study shows that most Arduino boards have limitations and security vulnerabilities in their software, hardware, and communication due to low-cost design requirements.

Internet of Cross-Chains—Model-Driven Cross-Chain as a Service Platform for the Internet of Everything (IoE) in Smart City: This article presents a communication platform for smart cities within the IoE network, specifically addressing the security, privacy, scalability, and cross-communication challenges of the Internet of Robotics Things. The proposed extended cross-chain-based blockchain technology provides a multifaceted solution for modern urban environments.

Distributed Cloud Computing—Architecture, Enabling Technologies, and Open Challenges: This article outlines a distributed cloud, interpreting the concept of distributed cloud computing and describing its architecture and enabling technologies. A case study is conducted on service deployment and discovery, providing a preliminary assessment of service discovery time, and open research challenges are discussed.

NAHAP—PUF-Based Three Factor Authentication System for IoMT: This article proposes a physical unclonable function-based three-factor authentication system, Neighbor Assisted Healthcare Authentication Protocol, to enhance security in the IoMT. The framework requires low computational time (6 ms), with minimal communication overhead, and demonstrated 100% reliability, as demonstrated through formal and informal analysis.

LOOKING FORWARD

I hope that the current issue dedicated to *Security and Trust in Forthcoming Consumer IoT Systems* becomes a good read for a broader set of the Consumer Technology community to advance their knowledge. *MCE* will continue the trend of covering more themes for enthusiastic and dedicated readers in future issues on the current and emerging topics with the active support from the editorial board members, reviewers, and authors worldwide.

Norbert Herencsar is an Associate Professor with the Department of Telecommunications, Brno University of Technology, Brno, 60190, Czech Republic. He received the Ph.D. degree in teleinformatics from the Brno University of Technology. He is the Editor-in-Chief of the *IEEE Consumer Electronics Magazine*. He is a senior member of the IEEE. Contact him at herencsn@ieee.org.