Guest Editors' Introduction

Security and Privacy-Aware Emerging Computing

Deepak Puthal
Khalifa University

Thanos Stouraitis
Khalifa University

Bidyadhar Subudhi
Indian Institute of Technology Goa

IN THE EVER-EVOLVING landscape of technology, the rapid proliferation of emerging computing paradigms has opened new frontiers of innovation, transforming the way we interact with and perceive the world. This relentless march of progress has ushered in the era of "Security and Privacy-Aware Emerging Computing," a paradigm that places the fundamental values of security and privacy at its core. It seeks to develop innovative solutions that safeguard sensitive data, protect user privacy, and fortify the security of emerging computing systems.

The convergence of technologies such as edge computing, the Internet of Things (IoT), artificial intelligence (AI), blockchain, and more has unlocked unprecedented opportunities for enhancing our lives, industries, and societies. However, these advances have also introduced complex challenges in securing sensitive data, protecting individual privacy, and ensuring the resilience of these emerging computing ecosystems. This Special Section curated 10 articles that tackle security and privacy concerns in emerging computing. Below, we provide a brief introduction to all the selected articles in this Special Section.

Digital Object Identifier 10.1109/MCE.2023.3318090
Date of current version 13 October 2023.

In the article titled "Assigning trust to devices in the context of consumer IoT applications," Macedo et al. highlighted the importance of securing consumer IoT devices, particularly in applications like smart homes and wearables, to prevent potential data leaks and security threats. It introduced a mathematical trust metric based on a two-level approach for objectively assessing confidence and enhancing security in IoT device communication.

In the article titled "Securing clustered edge intelligence with blockchain," Dehury et al. discussed a blockchain-based solution to ensure the immutability and traceability of edge devices' event history, enhancing security for data from source devices to cloud servers. This secure clustered edge intelligence mechanism holds the potential for establishing transparent and efficient systems.

In the article titled "Securing industrial control systems from cyber-attacks: A stacked neural-network-based approach," Jagtap et al. presented a stacked deep-learning model validated on industrial datasets to address limitations in existing literature. Additionally, it introduced JARA, an open-source intrusion detection system capable of detecting HnS IIoT malware when deployed on a Linux virtual machine, offering enhanced cybersecurity for cyber-physical systems.

In the article titled "AI-driven EEC for healthcare IoT: Security challenges and future research directions," Adil et al. provided a comprehensive

survey of healthcare IoT applications in the context of AI-enabled emerging edge computing (EEC) technology, highlighting security challenges and suggesting future research directions to address them effectively, emphasizing the importance of secure and efficient resource utilization in healthcare IoT.

In the article titled "Enhancing cryptocurrency security using AI risk management model," Elhoseny et al. introduced an intelligent risk management model for cryptocurrency security using social media indicators, leveraging natural language processing techniques to analyze user interactions on social media platforms. The model's case study on US cryptocurrency investors reveals a significant portion of the sample exhibiting various risk indications, including technological, financial, operational, and geopolitical risks, with a mean accuracy of 77% for risk analysis, identification, and assessment.

In the article titled "Vulnerabilities and attacks on CAN-based 3D printing/additive manufacturing," Cultice and Thapliyal discussed repurposed CAN-based attacks that can manipulate sensor data, override systems, and inject dangerous commands into the network, illustrated with a spoofing attack on critical data modules in a commercial 3D printer.

In the article titled "Toward higher levels of assurance in remote identity proofing," Nanda et al. presented a path for advancing remote identity proofing (RIDP) solutions and outlined the prerequisites for achieving the highest level of assurance in identity verification. It identifies pertinent issues and security threats, examines existing countermeasures, and explores the necessary steps to enable widespread remote identity-proofing systems.

In the article titled "Real-time physical threat detection on edge data using online learning," Khakurel and Rawat discussed the practical feasibility of creating a physical threat detection system that utilizes real-time data from security cameras and sensors at the edge to enhance the accuracy, efficiency, security, and privacy of the real-time inference model.

In the article titled "AI-oriented two-phase multifactor authentication in SAGINs: Prospects and challenges", Yang et al. introduced an AI-oriented two-phase multifactor authentication scheme for space–air–ground integrated networks to enhance security. This scheme incorporates intelligence into authentication and utilizes spatial-temporal features to provide continuous and transparent protection, addressing challenges faced by conventional authentication.

In the article titled "AI-based electricity grid management for sustainability, reliability, and security," Syu et al. introduced an AI-based electricity management system for addressing greenhouse gas emissions and improving the efficiency, sustainability, reliability, and security of the smart grid. It consists of prediction, anomaly detection, detect potential attacks and failures, and ensure sustainable and reliable electricity supply.

In the article titled "Blockchain for cybersecurity in edge networks," Hazra et al. explored the potential of combining edge computing and blockchain for secure IoT applications, highlighting the scalability challenges and security issues associated with this integration.

We extend our gratitude to the authors for their outstanding contributions to this Special Section. Our heartfelt appreciation goes to all the reviewers for their dedicated efforts in reviewing the articles and for providing valuable comments and suggestions that have significantly enhanced the article quality. We also wish to express our sincere thanks to the former editor-in-chief, prof. Saraju P. Mohanty, and the current editor-in-chief, prof. Norbert Herencsar, for their invaluable support and guidance throughout this process. It is our hope that this Special Section will become a valuable reference for researchers and professionals in the fields of cybersecurity and applied computing.

Deepak Puthal is an assistant professor with the Department of Electrical Engineering and Computer Science and a member of C2PS at Khalifa University, Abu Dhabi, UAE. Contact him at deepak.puthal@ku.ac.ae.

Bidyadhar Subudhi is a professor with the School of Electrical Sciences and the dean of Research & Development with the Indian Institute of Technology Goa, Ponda, India. Contact him at bidyadhar@iitgoa.ac.in.

Thanos Stouraitis is a professor with the Department of Electrical Engineering and Computer Science and a member of System-on-Chip Lab at Khalifa University, Abu Dhabi, UAE. Contact him at thanos.stouraitis@ku.ac.ae.