IEEE CONSUMER ELECTRONICS MAGAZINE
- SPECIAL SECTION CALL FOR ARTICLES -
Security and Privacy-Aware Emerging Computing

IEEE

IEEE CTSoc™
CONSUMER TECHNOLOGY SOCIETY

Consumer technology is not new, but it is becoming more intelligent by integrating computing and communication features into the end devices. These devices are connected to the Internet to receive and transmit data for decision-making and alert systems. In a more and more complex and specialized upcoming world in terms of computing, the efforts for new models and algorithms are more important and necessary than ever. This feature opens the door for attackers, where attackers can perform various types of attacks from all the aspects, such as software, hardware, and networks. Simultaneously, we cannot avoid devices' communication properties because it is the basics of developing smart applications, such as smart cities, villages, healthcare, etc. Where, the security and privacy-aware solutions in designing become unavoidable for any emerging computing infrastructure building.

Many contributions are made to secure the systems by adopting the core approaches and modifying them. However, this special section aims to foster the dissemination of fundamental security and privacy solution designing or solutions to secure emerging computing, such as the Internet of Things and Edge Computing. In particular, we encourage submissions related to one or more of the following topics:

- **Fundamental cryptography and applied cryptography for the emerging computing**
- **AI-enabled security and privacy-preserving solutions**
- **User-centric security and privacy-preserving solutions**
- **Context-aware security and privacy-preserving solutions**
- **Experimental platform development for security and privacy-preserving solutions**
- **Testbed development for the security and privacy-preserving solutions**
- **Novel blockchain consensus development**

Submission Procedure:

Submissions should follow IEEE standard template available at https://template-selector.ieee.org/ and should consist of the following: (i) A manuscript of maximum 6-page length: A PDF of the complete manuscript layout with figures, tables placed within the text, and (ii) Source files: Text should be provided separately from photos and graphics and may be in Word or LaTeX format. High resolution original photos and graphics (300 dpi) are required for the final submission. Images embedded in Word or Excel documents are not suitable; however, figures and graphics may be provided in a PowerPoint slide deck, with one figure/graphic per slide. The submissions which have been previously published at a conference need to have at least 50% new material and should be mentioned in the cover letter. ScholarOne Manuscripts URL for submitting the manuscripts is the following: http://mc.manuscriptcentral.com/cemag. The authors need to select "Security and Privacy-Aware Emerging Computing" in Step-1 of submission to ensure that the article is considered for this Special Section. NOTE: Articles exceeding 6 pages (including text, tables, and figures) during author proof will be charged at US$ 250 per page for extra pages beyond the first allowed 6 pages. For any questions, please contact the lead guest editor Dr. Deepak Puthal.

IMPORTANT DATES:

- **ARTICLE SUBMISSION DUE: NOVEMBER 1, 2022**
- **AUTHOR NOTIFICATION: MARCH 1, 2023**
- **APPROX. PUBLICATION DATE: Q4/2023**

GUEST EDITORS:

- **DEEPAK PUTHAL (SMIEEE), KHALIFA UNIVERSITY, ABU DHABI, UAE (DEEPAK.PUTHAL@IEEE.ORG)**
- **THANOS STOURAITIS (FIEEE), KHALIFA UNIVERSITY, ABU DHABI, UAE (THANOS.STOURAITIS@KU.AC.AE)**
- **BIDYADHAR SUBUDHI (SMIEEE), INDIAN INSTITUTE OF TECHNOLOGY GOA, INDIA (BIDYADHAR@IITGOA.AC.IN)**