IEEE Transactions on Consumer Electronics

Call for Papers

Special Section on "Zero Trust Edge and Federated Learning for Consumer Internet of Things"

Theme:

Zero trust edge integrates network and security to create an integrated protection framework that ensures consistent policy deployment and implementation at each edge. Federated learning is a distributed machine learning method that can solve data privacy issues. Consumer Internet of Things (CIoT) refers to the use of IoT products in consumer electronics to interconnect physical and digital objects. These devices integrate wireless technology and microcontrollers, making it easier to share consumer data and information between devices or computers. The CIoT has transformed the field of consumer electronics and elevated consumer electronics to another level through the interaction between consumers and products. With the rapid increase in the number of consumer electronic devices connected to the network, the data transmitted in the network is also growing geometrically. Traditional cloud computing centers are no longer able to meet the low latency and intensive network access and service requirements, and are prone to a series of attack methods such as single point attacks, collusion attacks, and man in the middle attacks, which pose a hidden danger to data security. Zero trust edge makes distributed federated learning possible. Zero trust edge overcomes the obstacles of secure digital acceleration, including user experience, security technology, and implicit trust. At the same time, federated learning not only fits perfectly with the zero trust edge computing model, but also retains data on terminal devices, reduces the risk of data leakage, and solves the problem of data islands.

However, zero trust edge and federated learning not only enhance the advantages of CIoT, but also face significant challenges. Firstly, it is necessary to face numerous security threats, such as gradient leakage attacks. Secondly, latency and communication costs are also the pain points. In addition, it is necessary to develop new algorithms and architectures that can effectively utilize zero trust edges and federated learning to meet the needs of CIoT while ensuring robustness and security. Finally, it is necessary to address the high-dimensional and heterogeneous nature of the data generated in CIoT, which requires new data management and analysis techniques. And new methods and mechanisms are needed to effectively manage and deploy applications, infrastructure, and networks in the distributed CIoT. Zero trust edge that supports artificial intelligence can also solve issues related to data security and privacy. Therefore, further research and innovation are needed in algorithm design, architecture, and security protection.

To provide more suitable solutions for zero trust edge and federated learning for CIoT, this special issue focuses on the latest research progress and new technologies. We encourage researchers to share the latest and most advanced solutions in this field. The topics of interest in this issue include (but are not limited to):

Topics of interest in this Special Section include (but are not limited to):

- Zero trust edge for CIoT
- Federated learning for CIoT
- Blockchain enables zero trust edge for CIoT
- Privacy protection authentication for CIoT
- Resource management of zero trust edge and federated learning for CIoT
- The security architecture of zero trust edge and federated learning for CIoT
- Collaboration and data sharing of zero trust edge and federated learning for CIoT
- Access control of zero trust edge and federated learning for CIoT
- AI-enabled zero trust edge for CIoT
- AI-enabled privacy-preserving for CIoT
- Secure communication for CIoT

Important dates:

- End of submission of Manuscripts: May 31, 2024
- Expected publication date (tentative): 1st quarter, 2025

Guest Editors:

Editor-in-Chief: Dr. Kim Fung Tsang kf.tce.eic@gmail.com

- Xin Ning, Institute of Semiconductors, Chinese Academy of Sciences, China, ningxin@semi.ac.cn
- Prayag Tiwari, Halmstad University, Sweden, prayag.tiwari@ieee.org
- Lusi Li, Old Dominion University, USA, lusili@cs.odu.edu
- Neeraj Kumar, Thapar Institute of Engineering and Technology, India, neeraj.kumar@thapar.edu

Instructions for authors:

Manuscripts should be prepared following guidelines at: https://ctsoc.ieee.org/publications/ieee-transactions-on-consumer-electronics.html and must be submitted online following the IEEE Transactions on Consumer Electronics instructions: https://ctsoc.ieee.org/publications/ieee-transactions-on-consumer-electronics.html. During submission, the Special Section on "**Zero Trust Edge and Federated Learning for Consumer Internet of Things**" should be selected.