IEEE CTSoc
CONSUMER TECHNOLOGY SOCIETY

IEEE Transactions on Consumer Electronics

Call for Papers

Special Section on "Secure and Privacy-Preserving Federated Learning for Autonomous Vehicles: Advances, Challenges, and Applications"

Theme:

Autonomous vehicles (AVs) provide driver-assistive technologies to drive the vehicle without the human operator's intervention to evade human-generated driving errors, saving many lives and facilitating hassle-free traveling. Since AVs regularly interact with central servers and other AVs for human-free driving during training AI models, the vehicle's and its owner's sensitive information must be protected. Therefore, federated learning has the great potential to revolutionize the AV industry. Federated learning, an emerging branch of machine learning, has the capabilities of AI modules at individual nodes for collaborative training of the machine learning model without sharing the sensitive information generated by AVs with the cloud and by exchanging the trained gradients periodically. During this process, the central server aggregates the gradients, and gradients are updated locally at individual nodes for collaborative training of the model.

Although the sensitive information is kept at local AVs, the adversaries can still extract sensitive information via inference attacks from shared gradients and empirical loss, promoting the biggest challenge for privacy preservation. Another big concern is that participating AVs may be compromised and work as malicious nodes. Moreover, this situation worsens when multiple malicious nodes work collaboratively to fail the machine learning models. Therefore, developing efficient and lightweight cryptographic primitives for federated learning is another big challenge.

Practitioners, researchers, and academicians are invited to contribute original research articles and review papers that transform Federated Learning's role in future autonomous driving.

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

- Privacy-preserving algorithms of federated learning for AVs
- Secure federated aggregation models for AVs
- Federated learning models for poor environmental and road conditions for autonomous driving
- Blockchain-based robust and scalable models of federated learning for AVs
- Differential privacy powered anonymous data scheme for AVs
- Lightweight cryptographic primitives for sharing AV training parameters to the central server.
- Effective algorithms for providing robustness against Byzantine faults for AVs
- Managing collusion attack for federated learning in AVs
- Secure computer vision-powered algorithms to identify various objects for AVs
- Secure data analytics algorithms for real-time estimation of traffic for AVs
- Analysis of adversarial attacks on federated learning for AVs
- Enhancing trust management in federated learning for AVs
- Multi-modal federated learning algorithms for escalating the protection and safety of AVs
- Elevating the security of the communication model for federated learning empowered AVs
- Federated learning for investigating security breaches in AVs
- Privacy-preserving federated learning models for the location of AVs

Important dates:

- End of submission of Manuscripts: **July 31, 2024**
- Expected publication date (tentative): 2nd Quarter, 2025

Guest Editors:

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

- Dr. Saru Kumari, Chaudhary Charan Singh University, India. (saru@ieee.org) (Female academician, Recipient of **India Research Excellence - Citation Awards 2023 by Clarivate Analytics**)
- Prof. Mohammad Shojafar, University of Surrey, Guildford, United Kingdom (m.shojafar@surrey.ac.uk)
- Prof. Hu Xiong, University of Electronic Science and Technology of China, China (xionghu@uestc.edu.cn)
- Prof. Chien-Ming Chen, Nanjing University of Information Science and Technology, China (chienmingchen@ieee.org)

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 **"(Secure and Privacy-Preserving Federated Learning for Autonomous Vehicles: Advances, Challenges, and Applications)"** should be selected.