

Guest Editorial

Special Issue on Security and Privacy of Intelligent Vehicles

INTELLIGENT vehicles are systems tightly integrating computation, communication, and physical behavior. The recent proliferation of artificial intelligence, machine learning, the Internet of Things (IoT), and edge-fog-cloud computing envisions that intelligent vehicles are capable of innovative solutions to change our lifestyles. However, the potential benefits come along with new challenges and concerns on security and privacy. This special issue consists of 12 papers and covers broad research contributions, including 1) intrusion detection from in-vehicular networks to connected vehicles, drones, and global positioning systems; 2) authentication with matchmaking encryption, certificateless cryptography, and blockchains for Internet of Vehicles; 3) privacy protection with data sharing and cross-vehicle federated learning; and 4) secure data analysis supported by the cloud. The special issue seeks to assist theoretical analysis, system architecture design, emerging applications, and social impacts of intelligent vehicles.

APPENDIX: RELATED ARTICLES

- [A1] H. Zhao, Y. Wang, A. Cheng, S. Wang, J. Yuan, and H. Wang, "Safeguarding GRU-based intrusion detection systems from adversarial attacks with dynamic label watermark in CAN bus communication," *IEEE Internet Things J.*, vol. 12, no. 7, pp. 7668–7676, Apr. 2025, doi: [10.1109/JIOT.2024.3524504](https://doi.org/10.1109/JIOT.2024.3524504).
- [A2] T. Zhang et al., "Hybrid transfer and self-supervised learning approaches in neural networks for intelligent vehicle intrusion detection and analysis," *IEEE Internet Things J.*, vol. 12, no. 7, pp. 7677–7692, Apr. 2025, doi: [10.1109/JIOT.2024.3518636](https://doi.org/10.1109/JIOT.2024.3518636).
- [A3] G. O. Anyanwu and H. Karimipour, "CLDP-FATD: Secure federated averaging threat detection framework for IVSN based on client-level differential privacy," *IEEE Internet Things J.*, vol. 12, no. 7, pp. 7693–7707, Apr. 2025, doi: [10.1109/JIOT.2024.3521609](https://doi.org/10.1109/JIOT.2024.3521609).
- [A4] V. U. Ihekoronye, S. O. Ajakwe, J. M. Lee, and D.-S. Kim, "DroneGuard: An explainable and efficient machine learning framework for intrusion detection in drone networks," *IEEE Internet Things J.*, vol. 12, no. 7, pp. 7708–7722, Apr. 2025, doi: [10.1109/JIOT.2024.3519633](https://doi.org/10.1109/JIOT.2024.3519633).
- [A5] Z. Wang, G. Li, and Z. Wang, "GPS attack detection and defense for secure localization of automated vehicles based on vehicle-to-vehicle technology," *IEEE Internet Things J.*, vol. 12, no. 7, pp. 7723–7735, Apr. 2025, doi: [10.1109/JIOT.2024.3424518](https://doi.org/10.1109/JIOT.2024.3424518).
- [A6] Z. Peng, C. Peng, Y. Tian, and H. Ding, "Securing intelligent vehicles: Authentication and bilateral control via inner product matchmaking encryption," *IEEE Internet Things J.*, vol. 12, no. 7, pp. 7736–7748, Apr. 2025, doi: [10.1109/JIOT.2024.3476669](https://doi.org/10.1109/JIOT.2024.3476669).
- [A7] L. Zhang, X. Yang, Y. Zheng, T. Yu, A. Yang, and N. Han, "EACAS: An efficient anonymous cross-domain authentication scheme in Internet of Vehicles," *IEEE Internet Things J.*, vol. 12, no. 7, pp. 7749–7762, Apr. 2025, doi: [10.1109/JIOT.2024.3505209](https://doi.org/10.1109/JIOT.2024.3505209).
- [A8] W. Jiang and Z. Guo, "An anonymous authentication scheme for Internet of Vehicles based on TRUG-PBFT main-secondary chains and zero-knowledge proof," *IEEE Internet Things J.*, vol. 12, no. 7, pp. 7763–7777, Apr. 2025, doi: [10.1109/JIOT.2024.3429342](https://doi.org/10.1109/JIOT.2024.3429342).
- [A9] M. Islam, M. H. Rehmani, L. Gao, and J. Chen, "An optimized privacy-utility tradeoff framework for differentially private data sharing in blockchain-based Internet of Things," *IEEE Internet Things J.*, vol. 12, no. 7, pp. 7778–7792, Apr. 2025, doi: [10.1109/JIOT.2025.3530247](https://doi.org/10.1109/JIOT.2025.3530247).
- [A10] R. Zhou, D. Li, W. Li, X. Zhang, X. Du, and M. Guizani, "Group-grained data search and sharing with privacy protection for vehicular social networks," *IEEE Internet Things J.*, vol. 12, no. 7, pp. 7793–7808, Apr. 2025, doi: [10.1109/JIOT.2024.3523910](https://doi.org/10.1109/JIOT.2024.3523910).
- [A11] L. Lu, X. Chu, A. Guo, Y. Fang, B. Martinez-Pastor, and R. Teixeira, "Cross-vehicle federated learning for unsupervised scoring of driver behavior under privacy constraint," *IEEE Internet Things J.*, vol. 12, no. 7, pp. 7809–7827, Apr. 2025, doi: [10.1109/JIOT.2024.3494716](https://doi.org/10.1109/JIOT.2024.3494716).
- [A12] S. Agrawal, P. Tekchandani, S. Banerjee, A. K. Das, S. Pal, and S. Shetty, "Secure cloud-storage-based big data analytics scheme for intelligent vehicles environment," *IEEE Internet Things J.*, vol. 12, no. 7, pp. 7828–7845, Apr. 2025, doi: [10.1109/JIOT.2024.3524089](https://doi.org/10.1109/JIOT.2024.3524089).

CHUNG-WEI LIN, *Guest Editor*

Department of Computer Science and Information
Engineering
National Taiwan University
Taipei 106319, Taiwan
E-mail: cwlin@csie.ntu.edu.tw

BO CHEN, *Guest Editor*

Department of Computer Science
Michigan Technological University
Houghton, MI 49931 USA
E-mail: bchen@mtu.edu

WEIZHI MENG, *Guest Editor*

School of Computing and Communications
Lancaster University
Lancaster LA1 4YR, U.K.
E-mail: weizhi.meng@ieee.org

YU CHEN, *Guest Editor*

Department of Electrical and Computer Engineering
Binghamton University—State University of New York
Binghamton, NY 13902 USA
E-mail: ychen@binghamton.edu

QI ZHU, *Guest Editor*

Department of Electrical and Computer Engineering
Northwestern University
Evanston, IL 60208 USA
E-mail: qzhu@northwestern.edu