Guest Editorial Special Section on Trustworthy AI-Enabled Edge Computing in Next-Generation Wireless Networks

Received 7 August 2025; accepted 7 August 2025. Date of current version 15 September 2025.

Digital Object Identifier 10.1109/OJCOMS.2025.3597376

Guest Editorial Special Section on Trustworthy AI-Enabled Edge Computing in Next-Generation Wireless Networks

THE CONVERGENCE of Artificial Intelligence (AI), edge computing, and next-generation wireless networks such as 5G and beyond (6G) is setting the stage for a paradigm shift across countless industries. This synergy promises to unlock unprecedented capabilities, from intelligent automation in Industry 5.0 and real-time analytics in smart grids to immersive experiences and autonomous systems. By processing data closer to its source, AI-enabled edge computing significantly reduces latency, conserves network bandwidth, and enhances the privacy of sensitive information. However, the widespread deployment of these technologies hinges on a critical factor, i.e., trust. Ensuring that AI models operating at the network edge are secure, private, robust, fair, and explainable is paramount for their adoption in high-stakes, mission-critical applications.

This Special Section on "Trustworthy AI-Enabled Edge Computing in Next-Generation Wireless Networks" was conceived to explore this crucial intersection. It aims to bring together the latest research and innovations that address the multifaceted challenges of building and maintaining trust in decentralized intelligent systems. The response from the research community was outstanding, and after a rigorous peer-review process, we are proud to present a collection of high-quality articles that push the boundaries of knowledge in this domain. These contributions span from foundational frameworks and comprehensive surveys to novel algorithms, practical applications, and robust defense mechanisms.

The papers in this section can be broadly categorized into several key themes that collectively form a holistic view of the state of the art.

Foundational Frameworks and Overviews: To set the context, several papers provide a broad perspective on the role of Trustworthy AI in emerging network paradigms. In the first article [A1], the survey offers a comprehensive analysis of Federated Learning (FL) as a cornerstone of trustworthy AI for 5G/6G security, examining its applications, vulnerabilities, and future directions. Shifting the focus to industrial applications, the second article [A2] explores the critical role of Explainable AI (XAI) in Industry 5.0, highlighting its potential to foster transparency and enable effective human-AI collaboration. Furthermore, a third article [A3] introduces the IoT-LF framework, which harnesses FL for privacy-preserving digital forensics in IoT environments, demonstrating the power of decentralized learning in automated cyberattack analysis.

Privacy Preservation in Decentralized Learning: A significant portion of this section is dedicated to what is arguably the most pressing concern in distributed AI: data privacy. The fourth article [A4] exposes fundamental privacy risks by demonstrating how membership information can be leaked in Federated Contrastive Learning (FCL) networks through carefully crafted inference attacks. In response to such threats, several articles propose innovative solutions. The fifth article [A5] introduces a privacy-preserving hierarchical federated reinforcement learning framework that improves task offloading in vehicular fog computing. The sixth article by Chen et al. [A6] presents a novel machine unlearning technique based on weight perturbation that can efficiently erase private data traces from trained models, offering an alternative to costly retraining. Furthering the goal of safeguarding user data, the seventh article [A7] proposes the PEDA framework to enforce data usage control policies in private 5G networks. Finally,DEEPFL is introduced in the eighth article [A8], a framework based on differential evolution that simultaneously enhances privacy protection and defends against poisoning attacks in maritime edge computing environments without adding computational overhead.

Security, Robustness, and Trust Management: Beyond privacy, the security and robustness of AI models against adversarial attacks are critical for establishing trust. Several papers tackle these challenges head-on. The ninth article [A9] proposes a coordinated defense mechanism that combines robust aggregation against data poisoning with game-theoretic power control to thwart jamming attacks in wireless FL networks. Similarly, the tenth article [A10] develops an adaptive trust management system that validates contributions from edge nodes before aggregation, preserving global model accuracy even when a high percentage of nodes are malicious. At the infrastructure level, the eleventh article [A11] presents a method for trustworthy analytics within the ETSI Zero-Touch Network and Service Management (ZSM) framework, using a security game model to assess the resilience of 5G components against intrusions. Focusing on hardware security, the twelfth article [A12] develops a real-time RFID tag cloning detection system using Graph Neural

Networks (GNNs) that operates without requiring changes to existing protocols or hardware.

Novel Edge AI Systems and Applications: This Special Section also showcases the application of trustworthy AI principles to solve real-world problems. For the renewable energy sector, the thirteenth article [A13] proposes an edge IoT architecture that uses data fingerprinting and neural networks to enable on-site data analysis, enhancing responsiveness while reducing cloud dependency. In the realm of IoT security, the fourteenth article [A14] puts forward a GNN-based method for LoRa device fingerprint identification by converting radio signals into graph representations, achieving high classification accuracy. Addressing the need for efficient and fair data exchange, the fifteenth article [A15] designs a blockchain-based system for data trading and placement at the edge, which improves producer profit and data access speed while lowering energy consumption. For public safety, the sixteenth article [A16] details a multimodal deep learning system for violence detection that integrates audio and video analysis, achieving high accuracy and real-time performance on resource-constrained Jetson Nano edge devices.

Federated Model Personalization and Optimization: Finally, recognizing that a one-size-fits-all model is often suboptimal in heterogeneous edge environments, a comparative study on federated model personalization is presented in the last article [A17]. By evaluating techniques such as Active Learning, Knowledge Distillation, and Local Memorization, the paper offers valuable insights into optimizing AI performance for next-generation IoT applications by fine-tuning models with local data.

In conclusion, the articles presented in this Special Section offer a rich and diverse tapestry of research in trustworthy AI for next-generation networks. They collectively underscore the rapid progress being made in developing AI systems that are not only intelligent but also secure, private, and reliable. We hope that this collection will serve as a valuable resource for researchers, practitioners, and policymakers, and that it will inspire further innovations in this vital field.

Our guest editorial team members sincerely thank the authors for their excellent contributions and to the dedicated reviewers whose insightful feedback was instrumental in shaping the quality of this section. We also would like to express our appreciation to the Editor-in-Chief and the editorial staff for their support in making this special section possible.

APPENDIX: RELATED ARTICLES

[A1] A. Blika et al., "Federated learning for enhanced cybersecurity and trustworthiness in 5G and 6G networks: A comprehensive survey," *IEEE Open J. Commun. Soc.*, vol. 6, pp. 3094–3130, 2025, doi: 10.1109/OJCOMS.2024.3449563.

[A2] T. R. Gadekallu et al., "XAI for industry 5.0—Concepts, opportunities, challenges, and future directions," *IEEE Open J. Commun. Soc.*, vol. 6, pp. 2706–2729, 2025, doi: 10.1109/OJCOMS.2024.3473891.

[A3] H. Mohamed, N. Koroniotis, N. Moustafa, F. Schiliro, and A. Y. Zomaya, "Harnessing federated learning for digital forensics in IoT: A survey and introduction to the IoT-LF framework," *IEEE Open J. Commun. Soc.*, vol. 6, pp. 3161–3191, 2025, doi: 10.1109/OJCOMS.2024.3492919.

[A4] K. Chen et al., "Private data leakage in federated contrastive learning networks," *IEEE Open J. Commun. Soc.*, vol. 6, pp. 3222–3235, 2025, doi: 10.1109/OJCOMS.2024.3454247.

[A5] Z. Wei, J. Mao, B. Li, and R. Zhang, "Privacy-preserving hierarchical reinforcement learning framework for task offloading in low-altitude vehicular fog computing," *IEEE Open J. Commun. Soc.*, vol. 6, pp. 3389–3403, 2025, doi: 10.1109/OJCOMS.2024.3457023.

[A6] K. Chen et al., "Private data protection with machine unlearning for next-generation networks," *IEEE Open J. Commun. Soc.*, vol. 6, pp. 3280–3291, 2025, doi: 10.1109/OJCOMS.2024.3518503.

[A7] H. Zafar, U. Fattore, F. Cirillo, and C. J. Bernardos, "Data usage control for privacy-enhanced network analytics in private 5G networks," *IEEE Open J. Commun. Soc.*, vol. 6, pp. 2976–2992, 2025, doi: 10.1109/OJCOMS.2024.3522379.

[A8] C. Han, T. Yang, Z. Cui, and X. Sun, "DEEPFL: A differential evolution-based framework for privacy protection and poisoning attack defense in maritime edge computing," *IEEE Open J. Commun. Soc.*, vol. 6, pp. 3305–3319, 2025, doi: 10.1109/OJCOMS.2024.3521329.

[A9] S. Barkatsa, M. Diamanti, P. Charatsaris, S. Voikos, E. E. Tsiropoulou, and S. Papavassiliou, "Coordinated jamming and poisoning attack detection and mitigation in wireless federated learning networks," *IEEE Open J. Commun. Soc.*, vol. 6, pp. 3745–3759, 2025, doi: 10.1109/OJCOMS.2025.3558672.

[A10] B. Hathout, P. Shepherd, T. Dagiuklas, K. Nagaty, A. Hamdy, and J. Rodriguez, "Adaptive trust management for data poisoning attacks in MEC-based FL infrastructures," *IEEE Open J. Commun. Soc.*, vol. 6, pp. 3140–3160, 2025, doi: 10.1109/OJCOMS.2024.3523368.

[A11] P. Radoglou-Grammatikis et al., "Trustworthy analytics in ETSI ZSM: A 5G security case study," *IEEE Open J. Commun. Soc.*, vol. 6, pp. 3292–3304, 2025, doi: 10.1109/OJCOMS.2024.3505555.

[A12] B. Zhang, "Securing RFID with GNN: A real-time tag cloning attack detection system," *IEEE Open J. Commun. Soc.*, vol. 6, pp. 3251–3264, 2025, doi: 10.1109/OJCOMS.2024.3502630.

[A13] Z. Zeng, L. Gao, H. Ma, and W. Li, "Fingerprint-based deduplication for renewable energy data on-site analyzing," *IEEE Open J. Commun. Soc.*, vol. 6, pp. 2730–2740, 2025, doi: 10.1109/OJCOMS.2024.3476277.

[A14] B. Zhang, "GNN for LoRa device fingerprint identification," *IEEE Open J. Commun. Soc.*, vol. 6, pp. 3131–3139, 2025, doi: 10.1109/OJCOMS.2024.3492922.

[A15] S. Yang et al., "Efficient data trading and placement in blockchain-based edge computing systems," *IEEE Open J. Commun. Soc.*, vol. 6, pp. 2679–2692, 2025, doi: 10.1109/OJCOMS.2024.3492914.

[A16] Mohammed, A. L. Swapnil, M. D. Peris, I. H. Nihal, R. Kha, and M. A. Matin, "Multimodal deep learning for violence detection: VGGish and MobileViT integration with knowledge distillation on Jetson Nano," *IEEE Open J. Commun. Soc.*, vol. 6, pp. 2907–2925, 2025, doi: 10.1109/OJCOMS.2024.3520703.

[A17] I. Siniosoglou et al., "Applied federated model personalization in the industrial domain: A comparative study," *IEEE Open J. Commun. Soc.*, vol. 6, pp. 3192–3210, 2025, doi: 10.1109/OJCOMS.2024.3457803.

SHAOHUA WAN, *Lead Guest Editor*
Shenzhen Institute for Advanced Study
University of Electronic Science and Technology of China
Shenzhen 518110, China

ZHIPENG CAI, *Guest Editor*
Department of Computer Science
Georgia State University
Atlanta, GA 30302, USA

QUANYAN ZHU, *Guest Editor*
Department of Electrical and Computer Engineering
New York University
New York, NY 10012, USA

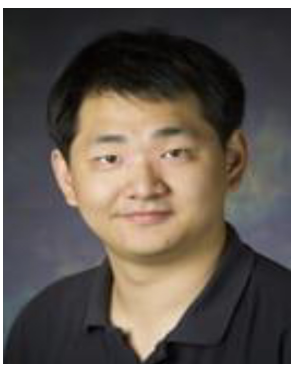
SOTIRIOS K. GOUDOS, *Guest Editor*
ELEDIA@AUTH, School of Physics
Aristotle University of Thessaloniki
541 24 Thessaloniki, Greece

ATHANASIOS V. VASILAKOS, *Guest Editor*
Center for AI Research
University of Agder
4879 Grimstad, Norway

CARLA FABIANA CHIASSERINI, *Guest Editor*
Department of Electronic and Communications
Politecnico di Torino
10129 Turin, Italy

SHAOHUA WAN (Senior Member, IEEE) received the Ph.D. degree from the School of Computer, Wuhan University in 2010. He is currently a Full Professor with the Shenzhen Institute for Advanced Study, University of Electronic Science and Technology of China. From 2016 to 2017, he was a Visiting Professor with the Department of Electrical and Computer Engineering, Technical University of Munich, Germany. He is an author of over 150 peer-reviewed research papers and books, including over 50 IEEE/ACM Transactions papers, such as IEEE TRANSACTIONS ON MOBILE COMPUTING, IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, *ACM Transactions on Embedded Computing Systems*, IEEE TRANSACTIONS ON COMMUNICATIONS, IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, *ACM Transaction on Design Automation of Electronic Systems*, IEEE TRANSACTIONS ON MULTIMEDIA, IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, and IEEE TRANSACTIONS ON AUTOMATION SCIENCE AND ENGINEERING, and many top conference papers in the fields of edge intelligence. Over 16000 citations have been recorded to his publications and his H-index is 72 according to Google scholar. His main research interests include deep learning for Internet of Vehicles. He is an Associate Editor of IEEE SYSTEMS JOURNAL and IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS. He had served as the Lead Guest Editor for IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, and *ACM Transactions on Multimedia Computing Communication*. He is also an ACM Senior Member.

ZHIPENG CAI (Fellow, IEEE) received the B.S. degree from the Department of Computer Science and Engineering, Beijing Institute of Technology, and the M.S. and Ph.D. degrees from the Department of Computing Science, University of Alberta. He is currently an Assistant Professor with the Department of Computer Science, Georgia State University (GSU). Prior to joining GSU, he was a Research Faculty with the School of Electrical and Computer Engineering, Georgia Institute of Technology. His research areas focus on networking and big data. He is a recipient of the NSF CAREER Award. He is the Steering Committee Chair of the International Conference on Wireless Algorithms, Systems, and Applications. He also chaired several international conferences, such as IEEE ICDCS 2019 and IEEE IPCCC18. He served/is serving on the editorial boards for several technical journals, such as IEEE INTERNET OF THINGS JOURNAL, IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, and IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY.



QUANYAN ZHU (Senior Member, IEEE) received the B.Eng. degree (with Distinction and Hons.) in electrical engineering from McGill University, Montreal, ON, Canada, in 2006, the M.A.Sc. degree from the University of Toronto, Toronto, ON, Canada, in 2008, and the Ph.D. degree from the University of Illinois at Urbana–Champaign, Champaign, IL, USA, in 2013. He is an Associate Professor with the Department of Electrical and Computer Engineering, New York University (NYU), New York, NY, USA, where he is also an affiliated Faculty Member with the Center of Cyber Security and the Center for Urban Science and Progress. From 2013 to 2014, he was a Postdoctoral Research Associate with the Department of Electrical Engineering, Princeton University, Princeton, NJ, USA. His current research interests include cyber–physical systems, cyber security and deception, game theory, machine learning, and network optimization and control. He is a recipient of many awards, including the NSF CAREER Award and the INFORMS Koopman Prize. He is a recipient of Best Paper Awards at 5th International Conference on Resilient Control Systems and 18th International Conference on Information Fusion. He spearheaded and chaired INFOCOM Workshop on Communications and Control on Smart Energy Systems and Midwest Workshop on Control and Game Theory. He has served as the General Chair of the 7th Conference on Decision and Game Theory for Security in 2016, the 9th International Conference on Network Games, Control and Optimization in 2018, and the 5th International Conference on Artificial Intelligence and Security in 2019.

SOTIRIOS K. GOUDOS (Senior Member, IEEE) received the B.Sc. degree in physics, the first M.Sc. degree in electronics, and the Ph.D. degree in physics from the Aristotle University of Thessaloniki, Thessaloniki, Greece, in 1991, 1994, and 2001, respectively, the second M.Sc. degree in information systems from the University of Macedonia, Greece, in 2005, the Diploma degree in electrical and computer engineering from the Aristotle University of Thessaloniki in 2011, where he is an Associate Professor with the Department of Physics. He is the Director of the ELEDIA@AUTH Lab Member of the ELEDIA Research Center Network. His research interests include antenna and microwave structures design, evolutionary algorithms, wireless communications, machine learning, and semantic Web technologies. He has participated as a Guest Editor or a Lead Guest editor in more than 20 special issues in international journals. He has co-organized four special sessions in international conferences. He is the founding Editor-in-Chief of the *Telecom* (MDPI). He was honored as an IEEE Access Outstanding Associate Editor in 2019 and 2020.

ATHANASIOS V. VASILAKOS (Senior Member, IEEE) is with the Center for AI Research, University of Agder, Grimstad, Norway. He is WoS Highly Cited Researcher from 2016 to 2021. He served or is serving as an Editor for many technical journals, such as the IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT, IEEE TRANSACTIONS ON CLOUD COMPUTING, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, IEEE TRANSACTIONS ON CYBERNETICS, IEEE TRANSACTIONS ON NANO BIOSCIENCE, IEEE TRANSACTIONS ON INFORMATION TECHNOLOGY IN BIOMEDICINE, *ACM Transactions on Autonomous and Adaptive Systems*, and the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS.

CARLA FABIANA CHIASSERINI (Fellow, IEEE) is currently a Full Professor with the Politecnico di Torino, Italy, and a Research Associate with the Italian National Research Council. Her research interests include 5G-and-beyond networks, NFV, mobile edge computing, connected vehicles, and distributed machine learning at the network edge. She currently serves as the Editor-in-Chief for the *Computer Communications* and the Associate Editor-in-Chief for the IEEE TRANSACTIONS ON NETWORK SCIENCE AND ENGINEERING. She is a Fellow of AAIA.