Computer Modeling in Engineering & Sciences

Tech Science Press

https://doi.org/10.32604/cmes.2026.082568

EDITORIAL

Introduction to the Special Issue on Next-Generation Intelligent Networks and Systems: Advances in IoT, Edge Computing, and Secure Cyber-Physical Applications

Nishu Gupta[1,*] **and Manuel J. C. S. Reis**[2]

[1]IEETA, University of Aveiro, Campus Universitário de Santiago, Aveiro, Portugal
[2]Engineering Department & IEETA, University of Trás-os-Montes e Alto Douro, Quinta de Prados, Vila Real, Portugal

*Corresponding Author: Nishu Gupta. Email: nishugupta@ieee.org

Received: 18 March 2026; Accepted: 19 March 2026; Published: 27 April 2026

The accelerating convergence of intelligent networking paradigms, data-driven modeling, and cyber-physical integration is reshaping the foundations of modern engineering systems. Within this context, this Special Issue of Computer Modeling in Engineering & Sciences (CMES) is devoted to recent advances in next-generation intelligent networks and systems, with a particular emphasis on the synergistic roles of the Internet of Things (IoT), edge computing, and secure cyber-physical applications.

CMES has long served as a platform for disseminating high-quality research on computational methods, mathematical modeling, and simulation-driven engineering. In alignment with this scope, the present Special Issue highlights how advanced modeling techniques, algorithmic innovations, and simulation frameworks are enabling the design, analysis, and optimization of complex, distributed, and intelligent networked systems.

The rapid proliferation of IoT devices has introduced unprecedented scale and heterogeneity into networked environments. These systems generate massive volumes of multi-modal data, necessitating efficient computational models for data fusion, inference, and control. Traditional cloud-centric architectures, while powerful, often fail to meet the stringent requirements of latency-sensitive and mission-critical applications. Consequently, edge computing has emerged as a pivotal paradigm, enabling decentralized processing and localized intelligence. From a modeling perspective, this shift introduces new challenges in distributed optimization, resource allocation, and system-level performance evaluation.

A central theme of this Special Issue is the role of computational intelligence in enhancing network functionality. Machine learning and deep learning models are increasingly embedded within network architectures to support predictive analytics, anomaly detection, and adaptive control. These models must be carefully designed to operate under constraints typical of edge environments, including limited computational resources, energy efficiency requirements, and dynamic network conditions. Contributions in this issue address these challenges through novel lightweight models, federated learning strategies, and hybrid computational frameworks that integrate physics-based and data-driven approaches.

Cyber-physical systems (CPS) represent another critical focus area, where the interplay between physical processes and computational intelligence necessitates rigorous modeling and validation. The integration of sensing, communication, and actuation components introduces complex interdependencies that must be captured through multi-scale and multi-physics modeling techniques. Several papers in this issue employ advanced numerical methods, stochastic modeling, and system identification techniques to enhance the

reliability and robustness of CPS applications across domains such as smart manufacturing, energy systems, and intelligent transportation.

Security and privacy considerations are deeply intertwined with the design of next-generation networks. From a modeling and simulation standpoint, the characterization of threats, vulnerabilities, and defense mechanisms requires sophisticated analytical tools. This Special Issue includes contributions that develop mathematical models for intrusion detection, trust evaluation, and secure communication protocols. Techniques such as blockchain-based frameworks, game-theoretic security modeling, and AI-driven threat intelligence are explored to address the evolving landscape of cyber threats in IoT-enabled CPS environments.

Another important dimension reflected in this issue is the integration of next-generation communication technologies, including beyond-5G and emerging 6G networks. These technologies introduce new opportunities for ultra-reliable low-latency communication (URLLC), massive machine-type communications (mMTC), and enhanced mobile broadband (eMBB). Modeling and simulation play a crucial role in evaluating these systems, particularly in terms of network scalability, spectrum efficiency, and quality of service. Contributions in this area leverage tools such as stochastic geometry, queuing theory, and network simulation platforms to analyze performance trade-offs and guide system design.

Energy efficiency and sustainability are also key considerations in the development of intelligent networks. The increasing density of connected devices and edge nodes raises significant concerns regarding energy consumption and environmental impact. Several articles in this Special Issue propose energy-aware computational models, optimization algorithms, and green networking strategies that aim to reduce the carbon footprint while maintaining system performance.

The diversity of contributions in this Special Issue reflects the field's interdisciplinary nature. Authors present a wide spectrum of methodologies, including analytical modeling, numerical simulation, optimization techniques, and experimental validation. Application domains span healthcare systems, smart cities, industrial automation, and environmental monitoring, demonstrating the broad applicability of intelligent networked systems in addressing real-world challenges.

From an engineering sciences perspective, a unifying thread across these works is the emphasis on model-driven design and validation. Accurate and computationally efficient models are essential for understanding system behavior, predicting performance under varying conditions, and ensuring reliability in deployment. The integration of data-driven methods with traditional modeling approaches represents a promising direction for future research, enabling more adaptive and context-aware systems.

Looking forward, several open challenges remain. These include the need for scalable, interpretable Artificial Intelligence (AI) models, robust frameworks for cross-domain interoperability, and comprehensive simulation environments that capture the full complexity of cyber-physical interactions. Furthermore, the ethical and societal implications of intelligent systems—particularly regarding data privacy, security, and trust—require continued attention from both researchers and practitioners.

In conclusion, this Special Issue provides a timely and comprehensive overview of emerging trends and methodologies in next-generation intelligent networks and systems. By emphasizing the role of computational modeling and engineering analysis, it contributes to bridging the gap between theoretical advancements and practical implementations.

The Guest Editors would like to express their sincere appreciation to all authors for their valuable contributions, to the reviewers for their insightful and rigorous evaluations, and to the editorial team of Computer Modeling in Engineering & Sciences for their continuous support and guidance throughout the publication process. It is our hope that this Special Issue will stimulate further research and innovation at

the intersection of intelligent networking, computational modeling, and cyber-physical systems. Below, we briefly outline the key insights from these articles and showcase their contribution.

Article [1] presents a literature review that addresses three research questions: identifying major threats and challenges in AIoT ecosystems, reviewing state-of-the-art security and privacy techniques, and evaluating their effectiveness. The review identifies key challenges, including data privacy leakage, authentication, cloud dependency, and attack surface expansion, and finds that emerging techniques, while promising, often involve trade-offs related to latency, scalability, and compliance.

Article [2] proposes a Fog-Edge adaptive cybersecurity system framework that intelligently distributes AI-powered anomaly detection algorithms across edge, fog, and cloud layers to optimize security efficacy, latency, and privacy.

Article [3] presents a robust framework that integrates AI and edge-level traffic prediction for Cyber Physical Systems-Internet of Things (CPS-IoT) systems. In addition, it implements distributed computing for selecting forwarders and analyzing threats across the IoT system, thereby enhancing stability while improving energy efficiency.

Article [4] introduces a robust distributed Denial-of-Service attack detection framework tailored for software-defined networking-based IoT environments, built upon a novel, synthetic multi-vector dataset generated in a Mininet-Ryu testbed using real-time flow-based labeling.

Article [5] proposes an impact-aware, taxonomy-driven machine learning framework with edge deployment and Shapley additive explanations (SAE)- based Explainable AI (XAI) for attack detection and classification in IIoT-CPS settings. It includes unsupervised clustering (K-Means and DBSCAN) to extract latent traffic patterns, and supervised classification based on taxonomy to categorize attacks into seven high-level categories.

Article [6] proposes a deep learning model that integrates AlexNet for feature extraction, principal component analysis for dimensionality reduction, and RNNs to detect malicious activity in QR code images.

Article [7] proposes a new wavelet transform-assisted Bayesian deep learning-based probabilistic (WT-BDLP) approach to mitigate malicious data-injection attacks in 6G edge networks.

Article [8] proposes an efficient content caching algorithm that adapts to dynamic vehicular demands on highways to maximize request satisfaction.

Article [9] introduces a synthetic dataset modeled on the widely used KDDCUP benchmark, augmented with healthcare-relevant attributes to better simulate the unique conditions of clinical environments.

Article [10] presents an innovative energy-efficient protocol based on deep Q-learning (DQN), specifically developed to prolong the operational lifespan of WSNs used in border surveillance. By harnessing DQN's adaptive power, the proposed protocol dynamically adjusts node activity and communication patterns. This approach ensures optimal energy usage while maintaining high coverage, connectivity, and data accuracy.

Article [11] proposes a clustered, distributed, federated learning architecture tailored for a 6G-enabled Tactile-IoT environment, in which clients are grouped into clusters based on data similarity and/or geographical proximity, enabling local intra-cluster aggregation before inter-cluster model sharing.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Ali Khan S, Mazhar T, Shah SFA, Ahmad W, Khan S, BiBi A, et al. Security and privacy challenges, solutions, and performance evaluation in AIoT-enabled smart societies. Comput Model Eng Sci. 2026:1–39. doi:10.32604/cmes.2026.075882.
2. Al-Quayed F. AI-powered anomaly detection and cybersecurity in healthcare IoT with fog-edge. Comput Model Eng Sci. 2026;146(1):45. doi:10.32604/cmes.2025.074799.
3. Haseeb K, Qureshi I, Abbas N, Ali M, Shah MA, Abbas Q. Trust-aware AI-enabled edge framework for intelligent traffic control in cyber-physical systems. Comput Model Eng Sci. 2025;145(3):4349–62. doi:10.32604/cmes.2025.072326.
4. Karmous N, Jlassi W, Aoueileyine MO, Filali I, Bouallegue R. A new dataset for network flooding attacks in SDN-based IoT environments. Comput Model Eng Sci. 2025;145(3):4363–93. doi:10.32604/cmes.2025.074178.
5. Zhukabayeva T, Ahmad Z, Tasbolatuly N, Zhartybayeva M, Mardenov Y, Karabayev N, et al. An impact-aware and taxonomy-driven explainable machine learning framework with edge computing for security in industrial IoT–cyber physical systems. Comput Model Eng Sci. 2025;145(2):2573–99. doi:10.32604/cmes.2025.070426.
6. Alsulami AA, Abu Al-Haija Q, Alturki B, Yafoz A, Alqahtani A, Alsini R, et al. Efficient malicious QR code detection system using an advanced deep learning approach. Comput Model Eng Sci. 2025;145(1):1117–40. doi:10.32604/cmes.2025.070745.
7. Pillai BS, Kulkarni R, kumar Kondeti VSS, Rajendran S. Wavelet transform-based Bayesian inference learning with conditional variational autoencoder for mitigating injection attack in 6G edge network. Comput Model Eng Sci. 2025;145(1):1141–66. doi:10.32604/cmes.2025.070348.
8. Ahmed F, Mansoor B, Javed MA, Saudagar AKJ. An efficient content caching strategy for fog-enabled road side units in vehicular networks. Comput Model Eng Sci. 2025;144(3):3783–804. doi:10.32604/cmes.2025.069430.
9. Usama M, Aziz A, Hassan I, Akhmetzhanova S, Qasem SN, Albarrak AM, et al. Enhancing healthcare cyber-security through the development and evaluation of intrusion detection systems. Comput Model Eng Sci. 2025;144(1):1225–48. doi:10.32604/cmes.2025.067098.
10. Rajput N, Kumar A, Pal R, Gupta N, Uitto M, Mäkelä J. Deep Q-learning driven protocol for enhanced border surveillance with extended wireless sensor network lifespan. Comput Model Eng Sci. 2025;143(3):3839–59. doi:10.32604/cmes.2025.065903.
11. Alnajar O, Barnawi A. A novel clustered distributed federated learning architecture for tactile Internet of Things applications in 6G environment. Comput Model Eng Sci. 2025;143(3):3861–97. doi:10.32604/cmes.2025.065833.