Computer Modeling in
Engineering & Sciences

Tech Science Press

https://doi.org/10.32604/cmes.2026.080244

EDITORIAL

Introduction to the Special Issue on Cutting-Edge Security and Privacy Solutions for Next-Generation Intelligent Mobile Internet Technologies and Applications

Ilsun You[1,*], Gaurav Choudhary[2], Gökhan Kul[3] and Francesco Falmieri[4]

[1]Department of Information Security, Cryptology, and Mathematics, Kookmin University, Seoul, Republic of Korea
[2]DTU Compute, Denmark Technical University, Kongens Lyngby, Denmark
[3]Department of Computer and Information Science, University of Massachusetts Dartmouth, Dartmouth, NH, USA
[4]Department of Computer Science, University of Salerno, Fisciano, Italy

*Corresponding Author: Ilsun You. Email: isyou@kookmin.ac.kr

Received: 05 February 2026; Accepted: 06 February 2026; Published: 30 March 2026

1 Introduction

The growing connectivity with mobile internet has significantly enhanced our day-to-day life support through various services and applications with on-demand availability at any time or anywhere. As emerging technologies with continuous revolutions in the digital transformations, various add-on technologies such as quantum computing, AI, and next-generation networks such as 6G are becoming an integral support to mobile internet systems. The emerging technologies in the next-generation mobile internet bring a lot of new security and privacy challenges. Therefore, there is a high demand to resolve such issues and vulnerabilities associated with these systems.

In this context, the ongoing research is also focusing on a broad spectrum of security and privacy aspects relevant to Future Mobile Internet Technologies and Cyber Architecture (FMIT-CA). These include the identification of emerging and advanced cyber threats and the development of effective countermeasures, as well as recent advances in mobile malware detection and prevention. Key focus areas further extended in the directions of privacy and data protection, robust authentication and access control mechanisms, and the design of secure mobile internet protocols supported by formal verification techniques. The growing impact of AI is bringing new scope to AI- and machine learning-driven security solutions, blockchain-based security mechanisms, trust and reputation management, and mobile device management (MDM) frameworks with comprehensive security policies. Additionally, the work considers secure edge and fog computing architectures, quantum-resistant cryptography, and strategies to mitigate sophisticated cyber threats in future mobile internet environments.

The special issue of CMES on cutting-edge security and privacy solutions for next-generation intelligent mobile internet technologies and applications accepted 14 top-quality research articles with rigorous reviews. This special issue attracted papers from researchers working in the area of mobile internet security. With a current need for mobile internet security, these high-quality articles will receive substantial attention and recognition within the research community focused on related domains.

There is a growing need to intensify research on encryption and authentication as core components of cutting-edge security and privacy solutions for next-generation intelligent mobile internet technologies and applications. Cho et al. [1] focused on remote collaboration and proposed a novel mechanism that encrypts data in ‘bundle’ units, designed to meet the dual requirements of efficiency and security for frequently updated collaborative data. The proposed solution utilizes the block cipher mode of operation based on the CTR mode. Furthermore, Alawami et al. [2] proposed a driver authentication system based on the sensors installed in a vehicle. The authors emphasize rapid authentication, lightweight, privacy-preserving, and practical aspects. Sohn et al. [3] investigated the phase-level resource usage of AES variants and proposed a practical model for edge devices. The analysis is based on encryption, decryption, and key generation. The authors discussed phase-level characterization, which provides a robust basis for guiding execution strategies and forecasting critical system metrics under constrained resources. Jeon et al. [4] proposed a privacy-preserving software-defined range proof (SDRP) model with a goal of low complexity and secure authentication. The authors focused on minimizing the computational load and the number of communication exchanges. Furthermore, the proposed model has been compared with the identifiable attribute model (IAM) and the zero-knowledge proof model (ZKPM) against leakage risk, computational cost, and security efficiency.

The rapid evolution of next-generation networks, particularly the 5G core architecture, introduces complex security challenges that demand advanced and intelligent protection mechanisms. As these networks support ultra-low latency, massive connectivity, and network slicing, traditional security approaches are no longer sufficient. Kim and Kim [5] focused on the classification of 5G network slicing for DDoS attacks and proposed an efficient traffic classification model. The authors used an SVM metadata classifier for classifying attack traffic in a 5G slicing network. Furthermore, Furthermore, Feng et al. [6] present a study on security threats targeting the N2 interfaces at the 5GC boundary and proposed an anomaly detection method based on Next Generation Application Protocol (NGAP) message sequences. Furthermore, Pawana et al. [7] focused on mitigating risks associated with legacy protocol dependencies and proposed a cloud-native 5G Core Network testbed for real-world attack simulations. The authors also investigate the AI-driven defense mechanisms. Chang et al. [8] focused on anomaly detection in 5G networks and proposed a 5G network IDS- ScalaDetect-5G, which includes extraction, reconstruction and detection phases. The proposed solution used ResCLA for fine-grained classification. Furthermore, Sánchez et al. [9] focused on privacy preservation in 6G and proposed a privacy-aware transmission scheduling algorithm for 6G *ad hoc* networks. The proposed model uses a probabilistic function in which teletraffic theory and information diffusion models are combined to find the optimum balance between privacy and Quality-of-Service.

Various approaches contribute to enhancing security, trust, and efficiency in future intelligent communication systems. Lee and Kim [10] focused on anomaly detection in O-RAN and proposed an ensemble Transformer–CNN model. The proposed solution integrated the advantages of the Transformer and the CNN. Shin and Shin [11] proposed a blockchain-driven vehicle data trading marketplace model for better decentralization, transparency, and traceability. The authors included the Multi-party computation (MPC) technique, the MOZAIK architecture, and the random leader selection technique for privacy.

Various approaches focused on behavioural aspect in the IoT and cyber physical environments. Yoon et al. [12] focused on behaviour aspects and proposed a structure-aware threat detection framework. This solution transforms hierarchical audit logs into a unified 2D data structure for granular detection. Yun and Min [13] focused on risk modelling and proposed a robust quantitative risk scoring model. This model is based on MITRE ATT&CK, CVE, CVSS, and the Cyber Kill Chain into a unified assessment methodology. Furthermore, Shin et al. [14] proposed a data-driven forensic framework for the EV charging infrastructures.

Finally, we are very pleased with the technical depth of this special section and believe it will make a meaningful contribution to the field of future Cutting-Edge Security and Privacy Solutions for Next-Generation Intelligent Mobile Internet Technologies and Applications. We strongly believe that accepted articles in this special issue will encourage further study and innovation in these areas. We sincerely thank all the authors for their high-quality contributions and the reviewers for their valuable efforts in maintaining the quality of this special section. We also extend our gratitude to the Editor-in-Chief and the editorial staff for their continuous support and guidance.

Funding Statement: The authors received no specific funding for this study.

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

References

1. Cho C, Kim B, Cho H, Youn T. A new encryption mechanism supporting the update of encrypted data for secure and efficient collaboration in the cloud environment. Comput Model Eng Sci. 2025;142(1):813–34. doi:10.32604/cmes.2024.056952.
2. Alawami MA, Jung D, Park Y, Ku Y, Choi G, Park KW. DriveMe: towards lightweight and practical driver authentication system using single-sensor pressure data. Comput Model Eng Sci. 2025;143(2):2361–89. doi:10.32604/cmes.2025.063819.
3. Sohn E, Lee S, Kim S, Sohn K, Kumar M, Park KW. Phase-level analysis and forecasting of system resources in edge device cryptographic algorithms. Comput Model Eng Sci. 2025;145(2):2761–85. doi:10.32604/cmes.2025.070888.
4. Jeon S, Lee Y, Lee I. Software defined range-proof authentication mechanism for untraceable digital ID. Comput Model Eng Sci. 2025;142(3):3213–28. doi:10.32604/cmes.2025.062082.
5. Kim M, Kim H. Ensemble encoder-based attack traffic classification for secure 5G slicing networks. Comput Model Eng Sci. 2025;143(2):2391–415. doi:10.32604/cmes.2025.063558.
6. Feng S, Cui B, Chang S, Jiang M. Temporal attention LSTM network for NGAP anomaly detection in 5GC boundary. Comput Model Eng Sci. 2025;144(2):2567–90. doi:10.32604/cmes.2025.067326.
7. Pawana IWAJ, Abella V, Lastre JK, Ko Y, You I. Enhancing roaming security in cloud-native 5G core network through deep learning-based intrusion detection system. Comput Model Eng Sci. 2025;145(2):2733–60. doi:10.32604/cmes.2025.072611.
8. Chang S, Cui B, Feng S. ScalaDetect-5G: ultra high-precision highly elastic deep intrusion detection system for 5G network. Comput Model Eng Sci. 2025;144(3):3805–27. doi:10.32604/cmes.2025.067756.
9. Sánchez BB, Alcarria R, Robles T. Information diffusion models and fuzzing algorithms for a privacy-aware data transmission scheduling in 6G heterogeneous ad hoc networks. Comput Model Eng Sci. 2026;146(2):43. doi:10.32604/cmes.2025.072603.
10. Lee S, Kim H. An AI/ML framework-driven approach for malicious traffic detection in open RAN. Comput Model Eng Sci. 2025;145(2):2657–82. doi:10.32604/cmes.2025.070627.
11. Shin SJ, Shin SU. ORTHRUS: a model for a decentralized and fair data marketplace supporting two types of output. Comput Model Eng Sci. 2025;145(2):2787–819. doi:10.32604/cmes.2025.072602.
12. Yoon S, Shin D, Euom I. Structure-aware malicious behavior detection through 2D spatio-temporal modeling of process hierarchies. Comput Model Eng Sci. 2025;145(2):2683–706. doi:10.32604/cmes.2025.071577.
13. Yun T, Min M. MITRE ATT&CK-driven threat analysis for edge-IoT environment and a quantitative risk scoring model. Comput Model Eng Sci. 2025;145(2):2707–31. doi:10.32604/cmes.2025.072357.
14. Shin D, Ha J, Euom I. Data-driven digital evidence analysis for the forensic investigation of the electric vehicle charging infrastructure. Comput Model Eng Sci. 2025;143(3):3795–838. doi:10.32604/cmes.2025.066727.