Call for Papers

------- Special Section on Next-Generation Security for Mobile Internet and Digital Ecosystems -------

The IEICE Transactions on Information and Systems announces that it will publish a special section entitled “Special Section on Next-Generation Security for Mobile Internet and Digital Ecosystem” in June 2027.

With the commercialization of 5G and Beyond (5GB) communication, the era of hyperconnectivity is arriving, accelerating the evolution of next-generation ICT platforms. As data collected from autonomous vehicles, robots, and mobile devices, such as smartphones and tablets, are transmitted in real-time to large-scale computing systems, the practical use of artificial intelligence is advancing rapidly. Compared to the era of traditional personal computing, the speed and volume of mobile data have increased significantly. This shift has led to an explosion in the use of intelligent, always-connected devices, such as smart cars, wearables, and digital assistants, which now permeate every aspect of our daily lives. In this hyper-connected environment, mobile devices serve as essential gateways not only for individuals but also for digital ecosystems, enabling rich interactions and business intelligence through the exchange of diverse data. However, such connectivity also introduces a wide range of potential security and privacy threats that must be proactively addressed.

Hence, the main motivation for this special section is to bring together researchers, practitioners, policymakers, and experts across both hardware and software domains to explore the latest advances in security and privacy for mobile internet platforms, applications, and interconnected systems. This special section places particular emphasis on innovative approaches to information security that can address the challenges posed by 5GB/6G, Industry 4.0, Society 5.0, ICT platform transformation, and global supply chains.

This special section is associated with the 9th International Conference on Mobile Internet Security (MobiSec 2025), one of the leading international conferences on mobile and cybersecurity. The call is open not only to authors who participated in MobiSec 2025 but also to all researchers and professionals working in relevant fields.

1. Scope

This special section aims at the timely dissemination of research in these areas. Possible topics include, but are not limited to:

- Security for 5G/6G and Next-Generation Mobile Networks
- Mobile, Wireless, and Cellular System Security
- Network/Edge/Cloud Security and Infrastructure Protection
- Data Security and Privacy in Edge and Distributed Environments
- (Post-Quantum) Cryptography, Lightweight/Advanced Encryption, and Side-Channel Countermeasures
- Security for IoT and Cyber-Physical Systems
- Embedded Systems and Hardware Security
- Trusted Execution Environments and Trustworthy Computing
- Security for AI Systems and Applications of AI in Security (e.g., AI-Driven Threat Detection)
- Digital Forensics and Malware Analysis in Mobile Ecosystems
- Secure Access Control, Authentication, and Authorization
- Secure Protocol Design and Real-World Protocol Analysis
- Blockchain and Distributed Ledger Security
- Supply Chain Security and Digital Platform Ecosystem Resilience
- Automated Tools for Software/Binary Vulnerability Analysis
- Operating System, Storage, and File System Security
- Web and Application Security
- HCI Security and Privacy (e.g., for Wearables and Smart Devices)
- Security for Unmanned Systems (Vehicles, Drones, Ships)
- Denial-of-Service Attacks and Botnet Defense
- Exploit Techniques, Vulnerability Research, and Practical Cryptanalysis

- Privacy-Preserving Technologies (e.g., Anonymity, Anti-Censorship Tools)
- Security Policy, Management, and Governance Models
- Safety and Security Issues in Digital Transformation and Industry 4.0/5.0 Platforms
- Emerging Trends and Challenges in Mobile Internet and Application Security
- Case Studies and Practical Security Applications in Real-World Environments
- Emerging New Topics in Mobile Internet Security

2. Submission Instructions

- A manuscript should be prepared according to the guidelines given in "The Information for Authors" (https://www.ieice.org/eng/shiori/mokuji_iss.html). We encourage the authors to use the IEICE Style File (https://www.ieice.org/ftp/index-e.html). The preferred length of the manuscript is 8 pages for a PAPER and 2 pages for a LETTER, with the format determined by the IEICE Style File.
- Submit the manuscript through the IEICE website (https://review.ieice.org/regist/regist_baseinfo_e.aspx). Choose "[Special-NX] Next-Generation Security for Mobile Internet and Digital Ecosystems" in the menu of "Journal/Section" in the submission page. Do not choose "[Regular-ED] Information and Systems" or other special sections.
- Authors must agree to the "Copyright Transfer, Article Processing Charge Agreement, Notices from the IEICE, and Privacy Policy" via electronic submission.
- Submission deadline of the manuscript is June 26, 2026.

Contact:

SeongHan Shin
Cyber Physical Security Research Institute,
National Institute of Advanced Industrial Science and Technology (AIST), Tokyo, Japan
Tel: +81-3-3599-8001, Email: seonghan.shin@aist.go.jp

3. Special Section Editorial Committee

Guest Editor-in-Chief: Ilsun YOU (Kookmin University, Korea)
Guest Associate Editor-in-Chief: Hyungrok JO (Yokohama National University, Japan), SeongHan SHIN (AIST, Japan), Dongseong KIM (The University of Queensland, Australia)
Guest Associate Editors: Pelin ANGIN (Middle East Technical University, Türkiye), Philip V. ASTILLO (University of San Carlos, Philippines), Haehyun CHO (Soongsil University, Korea), Gaurav CHOUDHARY (Technical University of Denmark, Denmark), Swee-Huay HENG (Multimedia University, Malaysia), Hyunho KANG (National Institute of Technology, Tokyo College, Japan), Jiyoon KIM (Gyeongsang National University, Korea), Jongkil KIM (Ewha Womans University, Korea), Il-Gu LEE (Sungshin Women's University, Korea), Takao MURAKAMI (The Institute of Statistical Mathematics, Japan), Hoonyong PARK (AUTOCRYPT, Korea), Jungsoo PARK (Kangnam University, Korea), Ki-Woong PARK (Sejong University, Korea), Shingo SATO (Yokohama National University, Japan), Daemin SHIN (Financial Security Institite, Korea), Sang Uk SHIN (Pukyong National University, Korea), Kunwar SINGH (National Institute Technology, Trichy, India), Kuniyasu SUZAKI (Institute of Information Security, Japan), Toshihiro YAMAUCHI (Okayama University, Japan)

*** Upon acceptance for publication, all authors, including authors of invited papers, should pay the page charges covering the partial cost of publication around November 2026. If payment is not completed by December 15, 2026, your manuscript will be handled as a rejection.**

* The standard period of 60 days between the notification (of conditional acceptance) and the second submission can be shortened according to the review schedule.

* If there are non-members among the authors, we recommend that the authors take this opportunity to join the IEICE. For detailed information on the IEICE Membership Application, please visit the webpage, https://www.ieice.org/eng_r/join/individual_member.html. If all authors are non-members, the article processing charge for non-members will be applied, except for invited papers.

* Open Access Publishing: All papers published in the IEICE Transactions on Information and Systems since January 2008 have been opened to all readers in the world through J-STAGE. https://www.jstage.jst.go.jp/browse/transinf

* IEICE has begun a multilingual (16 languages) translation trial of IEICE Transactions Online in April 2024.

* Please visit https://globals.ieice.org/.