# Special Issue on Data Security for Internet of Things

## Aims and Scopes

This Special Issue aims to provide a view of recent progress on data security techniques in Internet of Things (IoT). With the explosive growth of IoT devices, edge intelligence, 6G-enabled communications, and ubiquitous sensor networks, ensuring data security in IoT environments has become a critical challenge. Traditional security mechanisms often fall short in IoT due to resource constraints, heterogeneous protocols, and dynamic device topologies. This Special Issue aims to bring together cutting-edge research that addresses data security in IoT systems. Active researchers on data security for IoT are highly encouraged to submit their recent original works to this Special Issue. The covered topics include, but are not limited to, the following:

- Data security architectures for IoT ecosystems
- Zero-trust architectures for IoT ecosystems
- Secure AI methods for IoT
- Secure and lightweight authentication schemes for IoT
- Post-quantum cryptographic schemes for IoT
- Security mechanism for smart homes, factories, and cities
- Privacy-preserving data aggregation and federated learning in IoT
- Blockchain-based identity and trust management for IoT
- Data integrity verification in heterogeneous IoT networks
- New technologies for data security

## Special Issue Editors

Guest Editor: Prof. Hong Zhong
Email: zhongh@ahu.edu.cn
Website: https://cs.ahu.edu.cn/2021/1214/c20806a276921/page.htm
School of Computer Science and Technology, Anhui University, Hefei, 230601, China

Interests: IoT security, information security, data security

Guest Editor: Prof. Pengfei Hu
Email: phu@sdu.edu.cn
Website: https://perfecthu.github.io/
School of Computer Science and Technology at Shandong University, Qingdao, 266237, China
Interests: IoT Security, AI Security

Guest Editor: Assoc. Prof. Ke Cheng
Email: chengke@xidian.edu.cn
Website: https://faculty.xidian.edu.cn/CHENGKE
School of Computer Science and Technology, Xidian University, Xi'an, 710126, China
Interests: Data security, secure multi-party computation, LLM security

Guest Editor: Assoc. Prof. Qingyang Zhang
Email: qyzhang@ahu.edu.cn
Website: https://qyzhang.com/
School of Computer Science and Technology, Anhui University, Hefei, 230601, China
Interests: Data security, edge computing

## Author's Guidelines

The submissions should follow the formatting guidelines of the Journal of Networking and Network Applications (**https://iecscience.org/public/ueditor/php/upload/file/20200202/1580614065642302.zip**). Any questions regarding this special issue should be sent to the guest editors. All submitted papers will be reviewed by at least three reviewers and selected based on their originality, significance, relevance, and clarity of presentation. The manuscript should be prepared in J-NaNA Latex standard and converted into a PDF for auto-submission system. Electronic paper should be submitted to the J-NaNA Submission System at **https://www.manuscriptmanager.net/jnna**.

## Keywords

- IoT
- Data security
- Secure authentication
- Edge computing
- Secure AI
-

## Publication Schedule

Manuscript Submission Deadline: September 15, 2025
Notification of Acceptance/Rejection/Revision: October 15, 2025
Final Manuscript Due: November 15, 2025
Tentative Publication Date: December 1, 2025

## Benefits of Publishing in a Special Issue

- Ease of navigation: Grouping papers by topic helps scholars navigate broad scope journals more efficiently.
- Greater discoverability: Special Issues support the reach and impact of scientific research. Articles in Special Issues are more discoverable and cited more frequently.
- Expansion of research network: Special Issues facilitate connections among authors, fostering scientific collaborations.
- External promotion: Articles in Special Issues are often promoted through the journal's social media, increasing their visibility.
- Special Issues with more than 5 articles can be published, ensuring wide and rapid dissemination.
- The Article Processing Charge (APC) for publication in this open access journal is **No fee**.

## J-NaNA's homepage

- https://iecscience.org/public/journals/J-NaNA