



Submission deadline– 30<sup>th</sup> July 2024



## Call for Papers

Special Issue on

### Security and Safety of Data in Cloud Computing

Guest Editors:

- **Dengguo Feng**, Institute of Software, Chinese Academy of Sciences, China
- **Jian Ren**, Michigan State University, USA
- **Yang Zhang**, Helmholtz Center for Information Security (CISPA), Germany





# Call for Papers

Special Issue on

## *Security and Safety of Data in Cloud Computing*

### Background

As a technology integrating distributed computing, network computing and virtualization, cloud computing has attracted much attention since its emergence. By offering flexible and reliable resource services, cloud computing has been widely applied in various domains and has also enabled the advancement of transformative IT technologies such as big data and artificial intelligence. However, the extensive use of cloud computing also brings a large number of data security issues such as data theft and privacy inference. Cloud data, especially sensitive data during computation and processing, are exposed to increasing risks of security and privacy breaches, which pose great challenges to both industry and academia.

### Aims and Scope of the Special Issue

As the world's first innovative journal focusing on the intersection of cyber security and functional safety, S&S hereby calls for papers for this special issue on Security and Safety of data in Cloud Computing. The purpose is to provide a venue for global academics and industrialists for new contributions on data security and privacy protection in cloud computing, including new models, new technologies and new strategies. All submitted papers will be reviewed by the editors and then sent to at least three independent reviewers for single-blind peer review, and will be selected based on their quality and their relevance to the theme of this special issue.

This special issue covers (but not be limited to) the following topics:

- Homomorphic encryption for cloud computing
- Secure multi-party computation for cloud computing
- Differential privacy for cloud computing
- Trusted Execution Environment technique for cloud computing
- Machine learning security and privacy for cloud computing
- Privacy-preserving data retrieval for cloud computing
- System security in cloud computing
- Cloud virtualization security
- Cloud hardware security

### Submissions

Authors should submit their manuscripts online directly at: <https://sands.nestor-edp.org> and choose, during submission, the special issue: **Security and Safety of Data in Cloud Computing**. All relevant papers will be carefully considered and peer-reviewed by a distinguished team of international experts. The instructions for authors are detailed at: <https://sands.edpsciences.org/author-information/instructions-for-authors>.

**Submission deadline – 30<sup>th</sup> July 2024**

**Article Processing Charges** - S&S is an Open Access journal and no APCs in 2024.

### Guest Editors

**Dengguo Feng**, Institute of Software, Chinese Academy of Sciences, China, [fengdg@263.net](mailto:fengdg@263.net)

**Jian Ren**, Michigan State University, USA, [renjian@msu.edu](mailto:renjian@msu.edu)

**Yang Zhang**, Helmholtz Center for Information Security (CISPA), Germany, [zhang@cispa.de](mailto:zhang@cispa.de)

### Contact

**Yuanyuan Liu**, *Security and Safety* Editorial Office, [sands@edpsciences.org](mailto:sands@edpsciences.org)

## Guest Editor Biographies



**Dengguo Feng** is an Academician of Chinese Academy of Sciences, and a professor at Institute of Software, Chinese Academy of Sciences. His research interests are in the fields of Data Security, Cyber Security and Trusted Computing. He has published more than 200 highly-regarded journal and conference papers, including *Theor. Comput. Sci.*, *J. Cryptology*, IEEE IT, CRYPTO, CCS, *etc.*, and has led the development of more than 20 international or national standards. He received the First Prize of National Science and Technology Progress, the Second Prize of National Technological Invention and many other awards. He is currently an associate Editor-in-Chief of *Security and Safety* (S&S).



**Jian Ren** is currently a professor in the Department of Electrical and Computer Engineering at Michigan State University. He received his Ph.D. degree in Electrical Engineering from Xidian University, China. Prior to joining MSU, Prof. Ren was the Leading Secure Architect at Avaya Lab, Bell Lab and Racial Datacom. Prof. Ren's research interests include cybersecurity, distributed data sharing and storage, decentralized data management (e.g. medical records management), secure cloud computing, Big Data security, cost-aware privacy-preserving communications, blockchain based e-voting and AI security. Prof. Ren's research has been supported by multiple sources, including National Science Foundation, AFRL, MSU Technologies, Semiconductor Research Corporation and other industrial collaborators. He has secured 10 NSF grants, including the National Science Foundation (NSF) CAREER award in 2009. In 2020, he was invited and funded by MSU Technologies to commercialize his blockchain based large scale e-voting scheme, in collaboration with a well-known e-voting company. He has been invited as a Keynote Speaker and Distinguish Speaker for multiple conferences. Prof. Ren has been the Executive Chair of the IEEE ICNC conference since 2019. Prof. Ren served as an Associate Editor for multiple journals. Currently, he is serving as Editor-in-Chief of *IET Communications*, Associate Editor of, *IEEE Internet of Things Journal*, and *ACM Transactions on Sensor Networks*.



**Yang Zhang** is currently a tenured faculty at CISPA. His research concentrates on trustworthy machine learning (privacy, safety, and security). Moreover, he works on measuring and understanding misinformation and unsafe content like hateful memes on the Internet. Over the years, he has published multiple papers at top venues in information security, including CCS, NDSS, Oakland, and USENIX Security. His work has received the NDSS 2019 distinguished paper award and the CCS 2022 best paper award runner-up.