

Strategic International Collaborative Research Program (SICORP)  
 Collaboration Hubs for International Research Program (Japan-India)  
 Executive Summary of Phase 1 Final Report

1. Project title : 「SECURITY IN THE INTERNET OF THINGS SPACE」
2. Research period : Oct. 2016 ~ Mar. 2022
3. Main participants :

Japan-side

	Name	Title	Affiliation	Role in the research project
PI	Koji Okamura	Professor	Cybersecurity Center, KU	WP6
Co-PI	Yoshihiro Okada	Professor	ICER, KU	WP5
Co-PI	Kouichi Sakurai	Professor	ISEE, KU	WP3
Co-PI	Kenji Hisazumi	Associate Professor	System Engineering and Science, Shibaura Institute of Technology	WP1
Co-PI	Takatsugu Ono	Associate Professor	System LSI Research Center, KU	WP2
Co-PI	Kosuke Kaneko	Associate Professor	QREC, KU	WP4
Total number of participants throughout the research period:				48

Partner-side

	Name	Title	Affiliation	Role in the research project
PI	Sanjiva Prasad	Professor	IITD	WP1,3
Co-PI	Kolin Paul	Professor	IITD	WP3,6
Co-PI	Smruti Ranjan Sarangi	Professor	IITD	WP2
Co-PI	Subodh Sharma	Assistant Professor	IITD	WP4
Collaborator	Ranjan Bose	Professor	IITD	WP5,6
Total number of participants throughout the research period:				15

4. Summary of the international joint research

The IoT space is also called the fourth industrial revolution because of its ability to dramatically change people's lives by collecting various information and feeding back the results of advanced analysis of that information. Moreover, its practical application is expected to continue to increase world wide. As the IoT becomes more widely used, its security becomes even more important. The objective of this research is to "realize a secure IoT cyberspace" by comprehensively conducting research and development to secure the IoT space. In this research, we aim to secure the IoT space, which consists of complex IoT devices, networks, servers, and various information, by integrating the research areas in which the Indian Institute of Technology Delhi and Kyushu University. In order to realize a secure IoT space, we have conducted research on technologies to secure the IoT space, and research on improving human literacy to use the IoT space safely. In this research, we kept "security by design" in mind as the basic policy for making the IoT space technologically secure, and aimed to commercialize the space with security measures in place, rather than retrofitting security measures. Another feature of this research is that it includes training and education for people who provide the IoT space services and the

people who use those services. In this research, six research topics for making the IoT space safe were determined, and a WP (Working Package) for each topic was composed of members from the Japanese side and the Indian side. This research conducted by these six WPs is general-purpose for IoT and improves security for systems, data, and humans, and the results of this research are applicable to IoT in general.

Since FY2020, after human-behavioral restrictions due to measures to prevent the spread of COVID19 have been started, regular online meetings attended by the person in charge of each WP have been held to confirm the progress of research and exchange information. Furthermore, in 2020 and 2021, we will host open online workshops on "safe IoT space" and "future safe society" co-sponsored by IEEE, and young researchers from each WP including keynote speeches from the United States and the United Kingdom. We provided opportunities for researchers to make presentations and continued online joint research.

## 5. Outcomes of the international joint research

### 5-1 Scientific outputs and implemented activities of the joint research

In order to realize a secure IoT space, we conducted research on the technology to secure the IoT space, and research on improving human literacy to use the IoT space safely. In (WP1), "security by design" was considered as the basic policy to make the IoT space technologically secure, we aimed to commercialize IoT systems with security measures in place, rather than retrofit security measures, and to consider security from the time of IoT system design. In (WP2) we aimed to study security measures at the architecture level. Next, since input data in IoT systems always goes through the cloud, we conducted a study on cloud security considering IoT data (WP3), and a study on applications on IoT systems with security measures taken at the platform level (WP4). In the research on improving human security literacy, we conducted a study on the development of educational materials for IoT security measures (WP5) and a study on the training of experts who can use IoT systems safely (WP6).

### 5-2 Synergistic effects of the joint research

The synergistic effects of this research including those related to joint research, international human exchanges, and the return of the results of joint research. Regarding joint research, both Japanese and Indian sides have different strengths in terms of the basic technology for the same research purpose, and by combining these strengths, the purpose was reached and the degree of achievement became great. Thus, the results became better. In international human exchange, the joint research was further activated by inviting researchers from companies and other related organizations when holding symposiums in both Japan and India. In addition, we were able to invite researchers from countries other than Japan and India to the symposium and expand international exchanges.

### 5-3 Scientific, industrial or societal impacts/effects of the outputs (Spillover effects)

For the spillover effect of this research, the software developed in this research has been released on GitHub. In addition, in order to help more people other than students and researchers to understand and easily learn from our research, we have created teaching materials based on the research content and published them on Moodle, LMS (learning management system) that is opened to the public. In addition, training materials for professional development are also available on Moodle.

## 6. Potential as international collaborative research hub

With the basic policy of this research, "Security by Design", the results of this research enable security measures to be built into the design, hardware and platform from the beginning. The blockchain technologies that we have worked on to realize a secure platform should become one of the fundamental technologies that will support the international community in the future.