Research area in Strategic Objective *"System Software Technology to support Safety, Security, and Trust in the era of Society 5.0"*

Creation of System Software for Society 5.0 by Integrating Fundamental Theories and System Platform Technologies

Research supervisor: Yasuo Okabe (Professor, Academic Center for Computing and Media Studies, Kyoto University)

Overview

Society 5.0 proposed by Japan is a data-driven society in which people and things are connected, a variety of knowledge and information is shared, and new, never-before-seen value is produced. The spread of the novel coronavirus disease (COVID-19) will led to further progress in the digital transformation of society. As a result, a variety of data that could potentially lead to violation of confidentiality and privacy will likely be stored in public cloud-based systems, which raises concerns of increased security and privacy risks.

The realization of a safe, secure, and reliable data-driven society requires the implementation of a framework that balances free information sharing and personal information protection. In the construction of increasingly ingenious and complex social systems, it is necessary to run system software based on "Security-by-Design" and "Privacy-by-Design" on various execution environments composed by hybrid hardware and operating systems. The new vulnerabilities in state-of-the-art hardware and OS reported in recent years are becoming more serious issues for Japan, which relies on overseas technologies. It has become difficult to solve fundamental issues with conventional individual responses. It is essential to view the entire social system from the perspective of "by-design", to research and develop innovative technologies with a view to integrating them with theories such as distributed cooperative parallel processing and AI, and to create open system software that is safe, secure, and reliable in principle, and that has no black box in it and does not rely on other countries.

This research area aims to produce innovative, foundational system software that is safe, secure, and trusted in the era of Society 5.0. This will be realized by promoting research and development that integrates and fuses fundamental theories and system platform technologies in a cross-cutting manner. Specifically, it aims to achieve the following three goals:

(1) The creation of security technologies that make it possible to build secure services even in platform environments that include non-trusted hardware and operating systems.
(2) The creation of advanced information sensing, sharing, and analysis technologies that ensure privacy even in open and malicious environments.
(3) The creation of sophisticated architecture, design, and implementation technologies of system software that enables to deploy adaptive information sensing, sharing, and analysis in secure and privacy preserving manner.

This research area will be operated as part of the Ministry of Education, Culture, Sports, Science and Technology (MEXT)'s Artificial Intelligence/Big Data/IoT (Internet of Things)/Cybersecurity Integration Project (AIP Project : Advanced Integrated Intelligence Platform Project).

Research Supervisor's Policy for Application, Selection, and Management of the Research Area

1. Background

In the era of Society 5.0, it is likely that a wide variety of data obtained from various systems throughout society, such as traffic, energy, manufacturing, health, and education will be mutually connected, creating new social value. The spread of COVID-19 has also raised awareness of the need for social transformation with a view to the digitization of society and the post-COVID-19 era. However, realizing such a society requires addressing the various challenges likely to arise in these new ICT platforms and system software related to security and privacy.

These challenges require a variety of research to be promoted. For example, research to deal with cyber threats targeting vulnerabilities found out in ICT platform hardware and software, confidential information leakage and privacy violation of personal information, safe and secure information sharing and processing using "by-Design" concepts throughout the system.

Solving increasingly ingenious and complex security and privacy issues requires collaboration between researchers in the fields of architecture, operating systems, networking, software, databases, security, and privacy to promote fundamental research (theory) and applied research (system platform and system software). These actions are expected to deploy advanced system software technologies that support safety, security, and trust in the era of Society 5.0.

2. Examples of research projects that match the targets to be achieved

Based on the background above, this research area promotes research and development that integrates and fuses fundamental theories and system platform technologies in a cross-cutting manner. It aims to essentially solve the critical issues of security and privacy across various social infrastructures. Specifically, the area will involve the following types of research. However, research is not necessarily limited to these topics, and we are hoping for more free and challenging proposals.

(1) The creation of disruptive security technologies that make it possible to build secure services even in platform environments that include non-trusted hardware and operating systems.

- Safe and secure computing architecture with hierarchical and decentralized authority
  - Distributed collaboration across multiple trusted spaces
  - Architecture level security verification, etc.
- Technologies to build trusted isolation execution environments
  - AI automated security policy operations with zero-trust architecture
  - Next-generation TEE (Trusted Execution Environment)
  - Formal secure software verification and data authenticity for safe execution, etc.
- Next-generation information sharing platform in heterogeneous environments
  - Automatic vulnerability assessment and real-time threat detection
  - Data protection and dynamic information flow tracking (DIFT)
  - Next-generation PKI, distributed identity, distributed/integrated access control, etc.

(2) The creation of advanced information sensing, sharing, and analysis technologies that ensure privacy even in open and malicious environments.
  - Privacy protection technologies using cryptography with advanced functionality
    - High-performance privacy-preserving data mining with homomorphic encryption
  - Privacy policy management taking GDPR and others into account
  - Sophisticated differential privacy and local differential privacy

(3) The creation of sophisticated architecture, design, and implementation technologies of system software that enables to deploy adaptive information sensing, sharing, and analysis in secure and privacy preserving manner.
  - Integrated technologies that challenges to tackle both (1) and (2) above
  - High-performance computing algorithms for security and privacy treatment
  - Data authenticity and provenance guarantee technologies
  - Advanced operations in heterogeneous distributed data processing environments (i.e. various CPU, OS, VM combination)

3. Conducting the envisioned research

This research area expects research members to advance future-thinking fundamental technologies while maintaining an attitude that is aware of the real world and specifically envisions how theoretical research can be implemented in society, along with establishing technologies that essentially solve real-world issues related to security and privacy. We are hoping for proposals that are not limited to fundamental theories or system platform technologies but that are integrated in a way that, through theory, can guarantee that systems as a whole completely satisfy security and privacy requirements.

We are also aiming to improve international competitiveness by envisioning use-cases for research results and self-assessing benchmarks against competing global technologies. Steering will be strengthened at the time of interim evaluation (e.g., appropriate budget control, verification of research signpost and final goals). Research results are expected to be made available as open-source software (OSS) and open APIs so that they can be widely disseminated in a variety of environments. Collaboration and cooperation with other teams in this research area and PRESTO (Precursory Research for Embryonic Science and Technology) researchers working under the same strategic objectives is expected, alongside mutual use of research products.

During research and development, research teams are recommended to consider using mdx (a platform designed to create a data-driven society) and SINET5. The mdx is scheduled to be officially operational in FY2022 as a high-performance virtual environment.

4. Research period and funding

The research period will be five years and six months (from October 2022 to the end of March 2028), and the total budget will be in the range of 150 million to 350 million yen (excluding indirect costs). We will promote research and development that integrates and fuses fundamental theories and system platform technologies in a cross-cutting manner, so the aim is to increase the size of the budget per project. We are also considering budgetary measures to support research acceleration, etc., as needed

and promote collaboration through having multiple teams utilize each other's results.

5. Points to keep in mind when applying

This research area will be operated as CREST (Core Research for Evolutionary Science and Technology), a form of team-based research. We are particularly hoping for research and development proposals that go beyond elemental technologies and that integrate and fuse fundamental theories and system platform technologies in a cross-sectional manner. Team members and budget sizes may be increased as a result of transdisciplinary collaboration. It notes that it is recommended to consider incorporating not only security and privacy researchers but also statistical mathematics and computer science researchers, system software/hardware researchers/engineers, and social science experts into your team. Although the research topics in this area are illustrated in Section 2, a principal investigator may have a team structure that aims to attain a single target or a team structure with goals that span multiple achievement targets. In addition, we believe that incorporating a human resource development perspective is vital in this area. Therefore, we expect junior researchers to develop further and also expect challenging research proposals from junior and young researchers.

When applying for this research area, please describe your envisaged goal outcomes in five years and six months and your milestone in three years as precisely as possible. In particular, be sure to include a promising use-case roadmap that indicates how you intend to apply your research results in the real world. For larger-budget proposals, it must include a detail explanation concerning on a proof of concept system development and its experiments execution plan

This research area will be operated as one research area of MEXT's Artificial Intelligence/Big Data/IoT (Internet of Things)/Cybersecurity Integration Project (AIP Network Laboratory: Advanced Integrated Intelligence Platform Network Laboratory). It also contributes to the AIP project's integrated management by working on research projects in collaboration with the RIKEN Center for Integrative Research on Innovative Intelligence and other related research institutions.