Security Infrastructure Technology for Integrated Utilization of Big Data

Atsuko Miyaji · Tomoaki Mimoto
Editors

Security Infrastructure Technology for Integrated Utilization of Big Data

Applied to the Living Safety and Medical Fields

Springer Open

Editors
Atsuko Miyaji
Osaka University
Suita, Osaka, Japan

Tomoaki Mimoto
KDDI Research, Inc.
Fujimino, Japan

ISBN 978-981-15-3653-3 ISBN 978-981-15-3654-0 (eBook)
https://doi.org/10.1007/978-981-15-3654-0

This Springer imprint is published by the registered company Springer Nature Singapore Pte Ltd.
The registered company address is: 152 Beach Road, #21-01/04 Gateway East, Singapore 189721, Singapore

Foreword

The Japan Science and Technology Agency (JST) is an independent public body of the Ministry of Education, Culture, Sports, Science and Technology (MEXT). JST plays a key role in implementing science and technology policies formulated in line with the nation's Science and Technology Basic Plan. The Basic Research Programs at JST focus on fundamental research areas that help developing technological breakthroughs, which in turn lead to the advance of S&T and creation of new industries. The programs also encourage researches that trigger, through innovations, reformation of social and economic structures. Core Research for Evolutionary Science and Technology (CREST) program is one of the Basic Research Programs at JST. With an aim to promote and encourage the development of breakthrough technologies that contribute to the attainment of the country's strategic objectives, JST provides a variety of research funding programs for promising research projects. CREST is one of JST's major undertakings for stimulating achievement in fundamental science fields. In addition, returning the fruits of such research to society through innovations is another important responsibility of JST.

"Advanced Core Technologies for Big Data Integration" study area will aim for the creation, advancement, and systematization of next-generation core technology solving of essential issues common among a number of data domains, and integrated analysis of big data in a variety of fields. Specific development targets include technology for stable operation of large-scale data management systems that compress, transfer, and store big data, technology for efficiently retrieving truly necessary knowledge by means of search, comparison, and visualization across diverse information, and the mathematical methods and algorithms enabling such services. In pursuing these studies, with a view to overall system design up to the creation of value for society from big data, the creation, advancement, and systematization of next-generation common core technology highly acceptable to the public will be undertaken, through active efforts at fusion with fields outside of information and communication technology. There are total 11 projects. Especially, "The Security Infrastructure Technology for Integrated Utilization of Big Data," by Atsuko Miyaji (Research director), focuses on secure well-balanced utilization of big data. Many existing security researches focus on technologies of "fast encrypted

calculation" since they focus on statistical computation such as sum and average. However, the big data are varied, and thus, there are many usages. It cannot be said that use only for statistical data such as sum and average is enough. It would not be limited to statistical data in the case of medical image data, picture data, etc. What should be the security infrastructure for the utilization of such a wide variety of big data? In addition, extremely secure technologies often may give any benefit to neither the data owner nor the data user. Her project builds a technology to realize balanced security and utilization of big data from the viewpoint of three organizations of the data owner, analyst, and user. Their technology can be combined with fast encrypted calculation, which is a typical target of existing cryptographic researches. We really hope that their concept of security infrastructure technology for the utilization of big data would open up the world of big data utilization in various fields such as the medical and living safety field.

January 2020

Prof. Masaru Kitsuregawa
The University of Tokyo
Tokyo, Japan

Preface

A project of "The Security Infrastructure Technology for Integrated Utilization of Big Data" started in October 2014. Our team consists of four groups: security primitive group under the guidance of Atsuko Miyaji at Osaka university, security management primitive group under Kiyomoto at KDDI Laboratory, the living safety field under Kitamura at AIST and Nishida at Tokyo Institute of Technology, and the medical field under Tanaka at the National Cancer Center and Yamamoto at MEDIS. Concretely, both Kiyomoto and Miyaji have investigated the security infrastructure necessary for the utilization of big data. Based on this security infrastructure, Kitamura and Nishida made testbed systems in the living safety field; Tanaka and Yamamoto made testbed systems in the medical field. All studies combined aim to ensure the good working of the security infrastructure in the real world. Furthermore, after both Kitamura and Nishida will integrate the necessary big data excluding privacy information using our security infrastructure, they will analyze why serious injuries occur at elementary schools. In contrast, both Tanaka and Yamamoto have made an open medical network using our security infrastructure, which enables patients to check the usage of their medical records distributed in different hospitals.

One of the features of our project is that it builds security infrastructure for big data utilization based not on security researchers but on issues from the living safety and medical fields that actually use big data. In other words, it is an important feature that the required specifications do not deviate from actual problems. In addition, we report the results of actual research in both fields using the security infrastructure constructed according to their requirements. Thus, the analysis has been performed on only the available and acceptable data from the point of view of privacy policy until our security infrastructure was realized. Furthermore, the evaluation or analysis of security primitives is often based on dummy data. However, our security primitives have been evaluated by researchers who actually use big data. Furthermore, we clarify how to introduce such security solutions into living safety and medical fields. We also provide guidance on how to use the security infrastructure. We hope that this book will be used by companies, schools, and public organizations that are considering using big data.

Acknowledgements Finally, we would like to thank Prof. Masaru Kitsuregawa at the University of Tokyo who is a research supervisor of "Advanced Core Technologies for Big Data Integration" at JST. We would like to appreciate valuable comments given by Prof. Etsuya Shibayama at the University of Tokyo who is a deputy research supervisor. We also would like to extend our gratitude to useful advice by advisors in the research area: Prof. Kaoru Arakawa (School of Interdisciplinary Mathematical Sciences, Meiji University), Prof. Mitsuru Ishizuka (The University of Tokyo), Naonori Ueda Fellow, NTT Communication Science Laboratories, Hidehiko Tanaka, Director, IWASAKI GAKUEN, Jun'ichi Tsujii, Fellow of Advanced Industrial Science and Technology (AIST), Hideyuki Tokuda, President, National Institute of Information and Communication Technology, Prof. Takeshi Tokuyama, Kwansei Gakuin University, Prof. Teruo Higashino, Osaka University, Prof. Koichi Hori, the University of Tokyo, Prof. Hiroyuki Kitagawa, University of Tsukuba, Prof. Kenji Yamanishi, the University of Tokyo, Prof. Calton Pu, Georgia Institute of Technology, and Nozha Boujemaa, Median Technologies. Finally, we express thanks to our project members: Yuuki Takano, Shinya Okumura, Chen-Mou Cheng, Akinori Kawachi, Sinsaku Kiyomoto, Tomoaki Mimoto, Touru Nakamura, Yoshifumi Nishida, Koji Kitamura, Mikiko Oono, Katsuya Tanaka, and Ryuichi Yamamoto.

Osaka, Japan
January 2020

Prof. Atsuko Miyaji

Contents