IoT Machine Learning on Differentially Private Data

Yuichi Sei
The University of Electro-Communications, Japan

Abstract

IoT technologies have greatly improved people's convenience, and in recent years, the sharing of such IoT data has been promoted. At the same time, however, privacy leaks due to unexpected combinations with several data, and the existence of sensor data with errors are major issues. In this research study, we develop an IoT privacy-protection data analysis platform that can grasp and control privacy risks, as well as perform machine learning and statistical data analysis both safely and precisely. The goal of this study is the development of software that can safely handle large amounts of data with missing or erroneous data. The existing methods guarantee privacy protection within the range of data assumed beforehand, but in this research study, privacy protection is provided for combinations with unexpected data. Although the previous privacy protection data mining fields have targeted accurate data, this research study targets a large number of types of data: data that change dramatically in terms of type, accuracy, and quantity, and data with errors. A major challenge lies in targeting open, unmaintained, and dynamic data, rather than static data sets maintained in a closed world.

Biography

Yuichi Sei received a Ph.D. degree in information science and technology from the University of Tokyo in 2009. From 2009 to 2012, he was with the Mitsubishi Research Institute. He joined the University of Electro-Communications in 2013 and is currently an associate professor in the Graduate School of Informatics and Engineering. He is also a visiting researcher at Mitsubishi Research Institute and an adjunct researcher at Waseda University. His current research interests include artificial intelligence, privacy-preserving data mining, and software engineering.