Seiichi Ozawa
Professor of Electrical and Electronic Engineering,
Graduate School of Engineering,
Kobe University, Japan

Topic: **An Introduction to Privacy-Preserving Machine Learning for Big Data Analysis**

Abstract:

Since the advancement of AI brings us various smart services that are strongly linked to our lives, the value of personal data is rapidly increasing year by year. On the other hand, there is also an increasing risk that privacy invasion and leakage could cause serious damages to ordinal users. Concerning such privacy risk, even though a secure cloud computing environment is available for analyzing such sensitive data, it might not be accepted by data holders because data could be viewed by a cloud owner, so-called “semi-honest setting”. Therefore, the expectation for new data processing technologies that can analyze data securely are raising recently. This tutorial presents some of the latest technologies for privacy-preserving data analysis that enables us to analyze data securely while protecting privacy. In particular, I will give a brief explanation on k-anonymity, differential privacy, privacy-preserving machine learning using homomorphic encryption, and federated learning that allows us to analyze/share personal information on edge devices without revealing the contents each other.

Bio:

Seiichi Ozawa received Dr. Eng. in computer science from Kobe University. He is currently the deputy director of The Center for Mathematical and Data Sciences and full professor with Department of Electrical and Electronic Engineering, Graduate School of Engineering, Kobe University, Japan. His current research interests are deep learning, machine learning, pattern recognition, incremental learning, big data analytics, cybersecurity, text mining, computer vision, and privacy preserving data mining. He published more than 160 journal and conference papers, and book chapters/monographs. He is currently an associate editor of IEEE Trans. on Neural Networks and Learning Systems, IEEE Trans. on Cybernetics and 2 international journals. He is the President-Elect of Asia Pacific Neural Network Society, vice-president for Membership of International Neural Network Society, and board of governor of Japan Neural Network Society. He is a member of Neural Networks TC and Smart World TC of IEEE CI Society.