Dr. Kwangjo Kim (https://ircs.re.kr/)

Emeritus Prof.@KAIST, IACR Fellow
President of International Research ins. for Cyber Security(IRCS)

An invited talk on AI-security

supported by JSAI/SIG-SEC

[https://conferenceservice.jp/www/ai-sig-sec/]

-Date: 30th (Mon) Jan. 2023

-Time: 13:00----15:00

-Style: Hybrid

In_Person: Kyushu Univ.

Ito-campus, West-2, Room725

Online: Zoom

- **Your further Contact: The local host,**

Kouichi SAKURAI,

(sakurai [at] inf.kyushu-u.ac.jp)

supported by The Telecommunication Advancement Foundation of JAPAN

AI for Intrusion Detection and Privacy-Preserving

Abstract: Based on his co-authored two books published by Springer in 2018 and 2021, his presentation consists of two parts:

The 1st half presents recent advances in Intrusion Detection Systems (IDS) using the state-of-the art deep learning methods, which have achieved great breakthrough recently, particularly in the field of computer vision, natural language processing and image processing from the point of detection performances. We discuss a systematic and methodical overview of the latest developments in deep learning and makes a comprehensive comparison between shallow machine learners and deep learning methods. A general overview of deep learning applications to IDS followed by a novel deep feature extraction and selection(D-FES) is suggested. Further challenges and research directions will be suggested.

The 2nd half provides fundamental insights into privacy-preserving and deep learning, offering a comprehensive overview of the state-of-the-art in PPDL methods. It discusses practical issues, and leveraging federated or split-learning-based PPDL. Covering the fundamental theory of PPDL, the pros and cons of current PPDL methods, and addressing the gap between theory and practice in the most recent approaches, it is a valuable reference resource for a general audience, undergraduate and graduate students, as well as practitioners interested learning about PPDL from the scratch, and researchers wanting to explore PPDL for their applications.