國立臺北大學統計學系

專題演講

講題：Privacy-preserving Data Mining

主講人：王紹睿 研究員 (中華電信研究院資通安全所)

時間：106 年 12 月 6 日 (星期三，13：00~15：00)

地點：三峽校區商學大樓商 7F01

Abstract

In recent years, with AI and big data technology changing the whole world, data mining has become one of the important applications in the industry. However, more and more people care about its privacy issue, because there is usually a huge amount of personal data stored in this kind of system. For example, Google's AI firm DeepMind, which develops the famous AI system AlphaGo, was accused by UK government against their privacy law in the cooperation with U.K.'s National Health Service (NHS) in 2016. The main reason is DeepMind illegally uses the patient's health information, including their HIV reports. By the way, practitioners and theorists gradually focus on the research area of privacy-preserving data mining (PPDM). In this talk, I will introduce several important PPDM theorems and their experimental results: Randomization, K-anonymity, Differential Privacy, and Secure Multi-party Computation. Furthermore, I will give my thoughts and experiences of them, such as the feasibility, the trade-off between privacy and accuracy, and etc.

~歡迎參加~

國立臺北大學統計學系　敬邀

106.11.30