FACULTAD DE CIENCIAS
FÍSICAS Y MATEMÁTICAS
UNIVERSIDAD DE CHILE

CMM
Center for
Mathematical
Modeling

cmm.uchile.cl

Beauchef 851, edificio norte, piso 7
Santiago, CHILE
CP 837 0456

tel +56 2 2978 4870

Seminario Aprendizaje de Máquinas

Expositor

Abelino Jiménez

(PhD student, Carnegie Mellon University)

Título:

"Privacy Preserving Machine Learning"

Abstract:

Los diversos avances en cloud computing y aprendizaje automático han permitido difundir el uso de modelos cliente-servidor, donde un cliente proporciona sus datos y un servidor tiene un modelo de aprendizaje automático para hacer alguna inferencia sobre los datos del cliente. Sin embargo, dado distintos aspectos de la privacidad de los datos, el cliente puede no querer revelar la información requerida por el servidor o incluso dejar que el servidor conozca el resultado del modelo. Esta es una situación común cuando el tipo de información involucrada corresponde a datos médicos, financieros o gubernamentales, entre otros.

Una solución es enviar el modelo directamente al cliente, permitiendo hacer cálculos localmente, evitando que el cliente envíe sus datos a una parte externa. Sin embargo, en general, esta acción no es considerada principalmente por asuntos de propiedad intelectual que considera el proveedor del modelo. Así, tenemos un conflicto entre dos partes; por un lado, el cliente que tiene datos pero que no quiere revelarlos para obtener el resultado de un modelo, mientras que por otro lado tenemos al servidor, que ofrece el servicio de evaluar un modelo sin revelarlo. En esta charla discutiremos distintas maneras de resolver este conflicto. Mostraremos estrategias para evaluar distintos modelos de Aprendizaje Automático, tales como modelos lineales, bayesianos y redes neuronales, discutiendo el estado del arte de distintas técnicas, analizando sus beneficios y limitaciones, así como algunas herramientas para su implementación.

Jueves 11 de enero del 2018 a las 16:00 hrs., en la sala John von Neumann (CMM piso 7).

CONICYT
Ministerio de Educación
Gobierno de Chile

cnrs