深圳大学计算机与软件学院
College of Computer Science & Software Engineering,
Shenzhen University

大数据技术与应用研究所 学术讲座

隐私保护下的数据价值挖掘：挑战与方法

报告人： 曹家浩

主持人： 王熙照 教授

日　　期： 12th Oct, 2020 （星期一）

时　　间： 14:30-15:30 PM

地　　点： 致腾楼623（线下）腾讯会议（线上）

会议号： 860 9252 28

演讲嘉宾简介

曹家浩，清华大学计算机科学与技术博士，导师徐明伟教授。2015年在北京邮电大学本科毕业后保送至清华大学，2018年在美国乔治梅森大学信息系统安全中心访问，2020年获得博士学位并被授予清华大学计算机系优秀博士毕业生称号。目前发表10余篇网络空间安全会议及期刊论文，包括安全顶级会议ACM CCS、USENIX Security、NDSS及顶级期刊IEEE TIFS，其中发表在顶级会议USENIX Security的论文是四大安全顶会录用的国内首篇关于软件定义网络（SDN）安全研究的论文，且获得Student Travel Grant奖励；发表在国际知名安全会议SecureComm的论文获得Best Paper Award奖励，是国内首次以第一单位获得该奖项；他发表在安全顶会NDSS的论文揭露了SDN协议重大漏洞，获得工业界相关厂商确认，并协助修补了该漏洞。

摘要

当前AI技术正在各行各业广泛应用，它通过挖掘海量的数据价值，可形成重要的生产决策，进而产生巨大的经济效益。然而，AI技术背后依赖的数据所产生的隐私泄露问题已不容忽视。面对频发的严重数据泄露事件，各国都逐步推出了严厉的数据隐私保护法律法规。而数据隐私保护的高要求在一定程度上对数据价值挖掘提出了新的挑战。本次报告将简明扼要介绍七大类隐私保护的数据价值挖掘方法：数据脱敏、匿名算法、差分隐私、同态加密、可信执行环境、多方安全计算、联邦学习，并分析各类技术方案的优缺点。最后重点介绍近年来在AI顶级会议上正在研究的一类前景广阔的隐私保护数据价值挖掘方法：隐私保护的数据中间表示（Privacy-Preserving Data Intermediate Representation）。

诚挚邀请全院感兴趣的老师同学参加