

专题：大数据隐私保护

Privacy Protection of Big Data

客座编辑



苏森(1971-),男,北京邮电大学教授,计算机学院执行院长,中国计算机学会理事,服务计算专业委员会秘书长,“数字中国产业发展联盟”副理事长。2005年入选教育部“新世纪优秀人才支持计划”,2017年入选国家“万人计划”科技创新领军人才。目前主要研究方向为智能数据服务、数据隐私保护、社交网络分析。获国家科技进步奖二等奖1次,中国通信学会科技进步奖一等奖1次,教育部科技进步奖二等奖1次。



程祥(1984-),男,北京邮电大学副教授、博士生导师,主要研究方向为数据挖掘、知识工程、隐私保护等。其研究成果已发表在包括IEEE ICDE、IEEE ICDM、AAAI、IJCAI、EMNLP、IEEE TKDE、IEEE TDSC、*IEEE TSC*等在内的国际会议和期刊上。主持与大数据隐私保护相关的国家自然科学基金青年科学基金项目1项、国家自然科学基金项目面上项目1项,并作为科研骨干参与多项国家级和部级科研项目。

导读

在大数据时代,数据的开放共享是发掘大数据中蕴含的巨大价值以及推动大数据发展的必要途径。然而,大数据中往往包含用户的大量敏感信息,一旦开放这些数据,会导致严重的个人隐私泄露问题。如果不能解决由于大数据共享导致的个人隐私泄露的问题,大数据的发展将受到严重阻碍。因此,对大数据隐私保护技术的研究具有十分重要的意义,只有在有效保护用户隐私的前提下进行数据的开放与共享,才能充分发挥大数据的应用优势。

近年来,大数据隐私保护技术的研究和应用受到了学术界和工业界的广泛关注。在学术界,针对大数据隐私保护技术进行的研究方兴未艾;在工业界,一些互联网公司已经尝试应用隐私保护技术收集某些特定类型的用户数据。为了探讨与大数据隐私保护相关的领域面临的挑战,本专题汇集了国内活跃在一线的大数据隐私保护研究者的4篇文章,从科学基础理论、关键技术方法与系统应用研究等方面,探索大数据隐私保护最新的研究进展及未来可能的研究方向,希望能引起读者兴趣,推动相关领域研究与实践的发展。

孙慧中等人撰写的《一种基于随机投影的本地差分隐私高维数值型数据收集算法》针对高维数值型数据收集过程中亟待解决的隐私问题,提出了一种基于随机投影

技术的满足本地差分隐私的高维数值型数据收集算法Multi-RPHM,并从理论上证明了该算法满足本地差分隐私的要求。

王平等撰写的《基于安全压缩感知的大数据隐私保护》结合压缩感知技术,提出了一种感知层内置的轻量级加密机制,其能够将保密性嵌入信息感知的过程中,以近乎零的成本为数据提供第一层安全防护。

卢文雄等人撰写的《基于同源策略的移动应用细粒度隐私保护技术》指出了Android等移动平台使用的基于权限的访问控制机制存在的不足,文章引入类似浏览器同源策略的控制机制,实现了比原有Android权限模型更加细粒度的访问控制。

孟小峰等人撰写的《人工智能时代的数据隐私、垄断与公平》指出当前的隐私问题不是通过扰动、匿名、差分等技术能够解决的小隐私问题,而是数据收集场景下的“大隐私”问题,涉及隐私、垄断、公平等伦理问题。为详细探究此类伦理问题,作者从数据发展的角度出发,探讨了人工智能时代隐私、垄断与公平问题的产生环境及独特性,并提出了解决这些问题的的重要举措。

由于篇幅有限,本专题不能涵盖大数据隐私保护研究中的方方面面。但仍然希望通过阐述大数据隐私保护的最新研究进展及未来可能的研究方向,推动大数据隐私保护研究的进一步发展。