

数据安全:保障数据高效合理 开发利用的基石

随着信息技术的发展和应
用,人们的生产生活与数据已密
不可分。从飞机、汽车的设计制
造,到个人生活点滴的记录,数
据已渗透到人类社会的各个方
面。数据是资源、是钻石矿、是
未来的新油田,数据意味着财
富、意味着知识与信息、意味
着企业甚至国家在科技浪潮中
的核心竞争力。

科学技术是一把双刃剑。
数据在带来巨大价值的同时,也
引入了大量的安全风险与挑战。
合理利用数据首先必须满足其
安全需求。数据的生命周期包
括数据产生、采集、传输、存
储、分析、使用、共享、销毁
等诸多环节,每个环节都面临
着不同的安全威胁,需要进行
全链条创新研究。其中安全问
题较为突出的环节是数据采
集、数据传输、数据存储、数
据分析与使用。

数据采集是指采集方对用
户终端、智能设备、传感器等
产生的数据进行记录和预处理
的过程。一般无需预处理直接
上传,但在某些特殊场景下,例
如传输带宽受限或采集精度受
约束时,数据采集方需要先进
行数据压缩、变换甚至加噪等
处理,以降低数据大小或精度。
一旦真实数据被采集,就完全
脱离用户自身控制,因此,数
据采集是数据安全的第一道屏
障。需要不断创新和发展对称
密码、轻量级密码、安全多方
计算、隐私保护与管控等保证
数据采集安全的技术。

数据传输是指将采集到的
大数据由用户终端、智能设备、
传感器等传送到大型集中式数
据中心的过程。为了避免数据
在传输过程中不被攻击者收集
或破坏,可采用传统密码技术保



冯登国,中国科学院院士,现任
北京信息科学技术研究院院长、中
国科学院软件研究所研究员,主要研
究方向为网络与信息安全。

证数据的机密性和完整性。但
在数据处理时必须对其进行解
密后才能进行,尤其在云计算
和大数据时代,数据的处理经
常发生在云服务器中,在处
理过程中以明文形式存在的数
据无法抵御来自好奇或恶意云
的窥探,因此,需要不断创新
和发展同态加密、外包计算、
密文检索等新型安全技术。

数据被采集后常汇集存储
于大型数据中心,而大量集中
存储的有价值数据容易成为高
水平黑客团体的攻击目标。因
此,数据存储面临的安全风险
不仅包括来自外部黑客的攻
击和内部人员的信息窃取,还
包括不同利益方对数据的超权
限使用等。在云计算环境中,
越来越多的数据存储云端,脱
离数据拥有者的直接物理控
制。需要不断创新和发展身份
认证与访问控制、存储加密、
密文计算、密钥管理、终端安
全、冗余备份等保证数据存储
安全的技术。近年来,区块链
技术得到了快速发展,作为一
种新的分布式账本技术,为数
据安

全存储尤其是交易数据的安全
存储带来了新的前景和独特优
势,应予以重视。

数据采集、传输、存储的主
要目的是为了分析与使用,通
过数据挖掘、机器学习等算法
处理,可提取出所需的知识。这
一环节关注的主要安全问题如
何实现数据挖掘中的隐私保
护,降低多源异构数据集成中
的隐私泄露。防止数据使用者
对用户数据挖掘,得出用户刻
意隐藏的知识;防止分析者在
进行统计分析时,得到具体用
户的隐私信息。因此,需要不
断创新和发展用户身份、社交
关系、属性、轨迹、差分等隐
私保护技术。

总之,我们首先要深刻认识
数据安全的内涵。大数据时代
的数据安全不仅包括传统的机
密性、完整性、可用性,也包
括隐私保护;不仅包括防止数
据泄露的隐私保护,也包括数
据分析意义下的隐私保护。其
次,要紧跟国际数据安全技
术发展趋势。大数据时代的数据
安全技术成为国际学术界关注
的热点,聚集了大量的科研投
入,新技术、新突破层出不穷,
我们在进行原始创新和集成
创新的同时,应充分借鉴国际
先进成果。然后,要加强数据
安全法律法规研究与制定。通
过法律手段规范市场、强化监
管,合理平衡数据管制与自由
流动,营造良好的法治环境。最
后,要紧密结合产业和应用实
际,自主掌控一批核心关键技
术和产品,推出切实可行的安
全解决方案和标准规范,为保
障数据产业健康稳定发展保
驾护航。



(中国科学院软件研究所,北京 100190)