 DOI: https://doi.org/10.26549/bdai.v4i2.13134

Data Field Development Trend and Security Application Technology Research

Yuting Ma

Shenzhen Zaitian Biotechnology Co., Ltd., Shenzhen, Guangdong, 518000, China

Abstract

With the wide application of big data in social life, the commercial value contained in it is more and more difficult to estimate. Enterprises have been able to carry out large-scale and accurate research, and carry out a comprehensive investigation of personal consumption habits and tendencies, which brings huge business potential and market demand to enterprises. In this context, the security of data becomes more prominent, and the importance of information security technology. This paper will study the data security technology, and the security risks and security protection technology are discussed in detail, and the future of big data and information security development trend, in order to make big data users of security protection technology, and to change the new way of security thinking.

Keywords

big data; data security; development trend

数据领域发展趋势与安全应用技术研究

马玉婷

深圳栽田生物科技有限公司，中国·广东 深圳 518000

摘　要

随着大数据在社会生活中的广泛应用，其所蕴含的商业价值越来越难以估计，企业已经能够进行大规模、准确的研究，并对个人消费习惯和倾向行为展开全面的调查，这给企业带来巨大的业务潜力和市场需求。在此背景下，数据的安全问题变得更加突出，也更加突出了信息安全技术的重要性。论文对数据安全保障技术进行了研究，以及各个环节中存在的安全风险及安全保护技术进行详细的探讨，并展望了未来的大数据和信息安全发展趋势，以期让大数据使用者对有关的安全保护技术有一个粗略的认识，并以此来转变新的安全思考方式。

关键词

大数据；数据安全；发展趋势

1 引言

随着大数据技术的飞速发展，我们面临着更多的机会与挑战，我们的社会正在经历着翻天覆地的变革，智能终端的不断更新，无线网络的无处不在，交互的平台的独特性，使得我们这些平凡的公司与个体呈现出一种丰富多彩的立体感。随着大数据的深度开发与利用，新的经济正在蓬勃发展。随着大数据在社会生活中的广泛应用，其所蕴含的商业价值越来越难以估计，数据的安全问题也越来越突出，这就为信息安全技术的发展提供了新的契机和新的挑战。论文以大数据全生命周期为主线，对大数据各环节所存在的安全风险进行深入研究，提出大数据安全保护的关键技术 [1]。

【作者简介】马玉婷（1996–），女，中国广东深圳人，从事项目转化落地、优化内部结构研究。

2 大数据应用中的数据安全保障技术

2.1 数据采集过程的安全保障技术

随着大数据的不断增长，各种类型的数据在收集时也会出现诸如破坏、丢失、泄密、被盗等问题，需要采用一定的技术措施来保障收集时的数据安全性。常见的 VPN 技术，可以很好地解决对数据的安全传输的需求，充分地保障被传输数据的机密性、完整性、真实性，并防止回放攻击等。它的基本原则是：隧道技术、协议封装技术、密码技术和配置管理技术，在源端和目标端使用一个虚拟的数据传输专用通道，将源数据进行加密封装，嵌入另外一种协议的数据报文，将其伪装成一个正常的数据报文，然后在网络中进行传输，当达到目标之后，使用者可以对该恢复通道中的嵌套信息进行分析 [2]。

数据采集过程的安全保障技术见图 1。

图 1 数据采集过程的安全保障技术

2.2 数据存储过程的安全保障技术

要想对大数据进行有效处理，就必须保证其对大数据的存储安全性。由于数据生命周期长、使用频率高等特点，在当前的大数据背景下，各种云计算服务的大量使用，使得数据的安全性问题日益突出，尤其是个人隐私信息的泄露和被盗用的风险也随之增大。此外，随着大数据价值的日益提高，一些重要数据被国外的黑客所觊觎，企图盗取并获取巨额利润，这些数据一旦泄漏，将给公司和用户带来重大损失。大数据的深度应用和迅速发展离不开数据的安全性。论文针对大数据存储中存在的隐私保护、数据加密和数据备份和恢复等问题开展研究 [3]。

2.2.1 隐私保护

在大数据环境下，数据的高速传递与高效利用是数据隐私保护的最终目标。当前的隐私保护技术主要有：一是以数据转换为基础的，具有更高的计算效率，但是不能确保数据的完整性，并且有一定的数据损失。二是以数据加密为基础的隐私保护技术，其优点在于可以保证数据的完整性和安全性，但是需要耗费大量的计算资源。三是以匿名化为基础的隐私保护技术，可以确保所发表的信息的真伪，但是所发布的信息会有一些数据的损失。各种类型的信息安全技术都有其各自的优势和不足，需要使用者结合自己的业务需求，来选择适合自己的信息安全技术 [4]。

2.2.2 数据加密

通过 VPN 信道，可以将这些信息安全地传送给接收方，接收方在接收到这些信息后，需要对这些信息进行解密，然后再将这些信息传送给接收方。由于数据是以明文存储的，一旦被入侵，其脆弱程度将会大大降低，所以，在存储过程中，必须经过加密处理才能保证数据的安全性，而只有对重要的核心数据才能使用存储加密技术。资料的加密方式按资料的种类可分为静态资料的加密方式与动态资料的加密方式 [5]。

2.2.3 备份与恢复

为了避免灾难的出现，必须在存储系统中建立数据的备份与恢复机制。在数据保存良好的情况下，启动备份机制，在数据发生意外损失或损坏的情况下，启动备份机制，保证数据的可用性和完整性。常用的备份与还原方法有离线备份，Raid 备份，数据镜像与快照等。在大数据环境中，通常采用 Hadoop 自主开发的 HDFS 数据备份和恢复技术，并针对一些关键数据进行远程容灾备份，如图 2 所示。

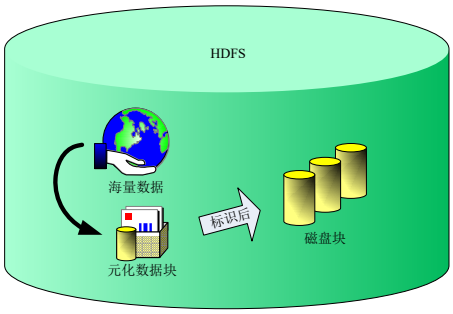

图 2 HDFS 数据备份技术

2.3 数据分析过程的安全保障技术

数据分析就是对大量数据进行分析，从中提炼出有意义的信息，从而使大数据的价值得到最大程度的发挥。在对数据进行处理时，将结合人工智能、云计算、检索引擎、统计应用、生物识别等多个学科的知识与技术。复杂的交叉学科应用，导致了一个具有庞大基础大数据的机构，不可能是一个万能的、专业的、全面的、专业的、对数据进行分析的专家，因此，在进行数据分析的过程中，必然会遇到一些安全问题。因此，如何才能确保第三方在利用数据的时候，不会在数据中植入恶意代码，并且在提取数据之后，不会被泄露出去，这是一个值得重视的问题。

2.4 数据发布过程的安全保障技术

大数据在进行分析处理之后，就会进入到数据发布的流程中，这个流程就是数据的开放和利用，所以它的安全性就变得更加重要。在资料公布之前，必须全面审查资料，确保资料的保密性、合规性等。不过，即使是最严密的审查程序，也不可能万无一失，所以在数据公布后，一旦发生数据机密外泄、隐私泄露等意外事件，就必须立即启动追踪系统，快速找到数据泄露的关键节点，并在第一时间进行应对。

2.5 防范 APT 攻击

APT 攻击是指攻击者利用物联网、欺诈等手段，盗取或摧毁（封锁）被攻击对象（机构）的核心系统，或者寄宿于该机构的内网，等待下一次攻击。现有的探测与防御技术无法全面有效地应对 APT 网络中的各种攻击，有的甚至在很久以后才被侦测到，有的则根本没有被侦测到。然而，现有的 APT 网络安全监测与防御技术无法全面有效地解决全部的 APT 网络安全问题，有的网络安全问题需要经过一段时间的潜伏期，有的网络安全问题尚未得到解决。针对这一现状，我们必须改变对所有数据进行保护的惯性安全思维，将安全重心放在对关键资源的保护上，在每一个重要环节上都要进行检测和防护，对采集行为进行完整的记录，构建一种新的安全防护体系。

3 数据安全的未来发展趋势

3.1 人工智能助力数据安全新生态

习近平总书记指出，要在国际科技竞赛中取得主动，就必须加快发展新一代的人工智能，这是一项非常重要的战

略。随着 AI 技术的不断发展，AI 产业也在不断发展，基于人工智能的数据安全保护应用已经成为我国数据安全产业发展的一个重要方向。由于网络攻击具有持续演化性，在进行数据安全防护时，往往要面对各种未知的恶意攻击。但是，人工智能技术可以利用其庞大的计算能力，快速地对数以百万计的事件进行筛查，从而找到各种异常行为、风险和威胁的信号，并在此之前对其进行预警。

3.2 IT 和 OT 加速融合加强数据安全防护

信息技术和 OT 技术的联接为工控系统的发展提供广阔的发展空间，同时也带来各种各样的数据安全问题。计算机网络技术为数据安全防护奠定技术基础，再将其与管理手段以及传统的工业技术进行融合，将 IT 与 OT 相结合，构建出一个全面的信息防御体系，在这种方式下，所形成的数据安全解决方案是切合现实的，也是比较适合的。目前，公司普遍趋向于推动生产执行系统的发展，在工业控制网与信息管理网之间进行数据交换与系统整合，以达到提高公司的生产管理效益与效率的目的。于是，本来是一个封闭的 OT 体系，通过管理体系与 Internet 相连接，给 Internet 方面带来各种网络攻击的风险。这就要求企业在信息技术和 OT 技术相结合时，加强对信息技术和 OT 技术的保护，提高信息技术的安全性。

3.3 情报分析共享构筑威胁情报生态圈

面对各类新类型的信息安全威胁，威胁情报的涌现促使传统的被动防御方式逐步向全程主动、智能化防御方式转变。分散的情报收集工作造成了“信息孤岛”，增加收集成本，降低不同机构之间的信息流动，给建立一个健全、有效的威胁情报生态体系带来困难。唯有提升社会治安信息的互联共享水平，促进不同类型的信息系统之间的合作，才能提升对各种网络治安威胁的即时探测与应对能力。为了构建一个健康、高效的网络威胁情报生态，必须结合其现实的安全需求和业务过程的要求，积极运用大数据、人工智能、云计算等先进的前沿技术，构建一个网络威胁与弱点的深度探测与分析体系，对其可能存在的安全风险进行深入的挖掘与评价，并对其进行有效的应对，从而为网络威胁情报的感知、共享与分析提供一种有效的手段。

3.4 以攻促防提升数据安全防护能力

“以攻促防”是一种很有实际意义的方法，也是一种切实可行的方法。“攻”就是利用各种方法，对软件、硬件和系统结构等方面的恶意攻击进行仿真，从而找出当前的安全防御体系中存在的漏洞。“防”是指对网络系统设备的安全和网络数据的安全进行保护，以及对网络中存在的缺陷进行修复等。在进行日常实战攻防演练的过程中，能够帮助防护人员及时发现和修护企业重要基础设施中存在的安全漏洞，提高企业数据安全防护、组织指挥、应急响应等能力，实现对系统漏洞与故障的快速定位、快速业务系统恢复。

4 结论

当前，随着科技的发展，数据安全制度也在飞速地发生着变化，对公共数据的安全进行强化，这就需要加速建立一个可以有效地适应前期、中期、后期全周期的安全监控管理体系。论文面向数据安全的关键技术，形成数据安全监控与管理系统，并对其进行实际应用验证，而我们也将基于这一点，不断推进大数据的发展。

参考文献

[1] 湛炜标.强化金融数据安全制度与技术保障[J].中国金融,2021(15):39-40.

[2] 程啸.我国网络安全法律规范体系逐步形成[J].服务外包,2022(7):38-39.

[3] 代明,巫媛.计算机网络安全中数据加密技术的应用[J].信息记录材料,2022,23(1):161-163.

[4] 毛华斌,吴园涛,殷建平,等.海洋环境安全保障技术发展现状和展望[J].中国科学院院刊,2022,37(7):870-880.

[5] 王丹,赵文兵,丁治明.大数据安全保障关键技术分析综述[J].北京工业大学学报,2017,43(3):335-349.