

# 大数据时代数据安全发展分析

严伟

中国联合网络通信有限公司温州市分公司 浙江 温州 325000

**摘要:** 本文深入探讨了大数据时代数据安全的发展。先概述了大数据的概念,接着分析了数据安全面临的挑战,如数据量巨大且复杂、多样性与来源广泛、处理速度和实时性要求高以及价值高吸引力大等。阐述了网络攻击、内部违规、隐私保护和云环境风险等主要威胁,并介绍了关键技术。最后提出了包括完善管理制度、加强员工培训、定期评估修复以及构建应急响应机制等防护策略。

**关键词:** 大数据; 数据安全; 防护策略; 发展趋势

引言: 在当今数字化迅猛发展的时代,大数据已成为推动社会进步和经济增长的重要力量。然而,伴随着大数据的广泛应用,数据安全问题日益凸显。数据量的爆炸式增长、来源的多元化以及处理的高速化,都给数据安全带来了前所未有的挑战。了解这些挑战,对于保障大数据的安全、促进其健康发展至关重要。

## 1 大数据概述

大数据是指规模极其庞大、复杂多样的数据集合,这些数据的规模和复杂性超出了传统数据处理技术的能力范围。大数据的定义不仅仅在于数据的数量巨大,更重要的是其包含了各种各样的数据类型,如结构化数据(如数据库中的表格数据)、半结构化数据(如XML、JSON格式的数据)以及非结构化数据(如文本、图像、音频、视频等)。

大数据具有几个显著的特点。一是数据量巨大,通常以PB甚至EB为单位来衡量。例如,大型互联网公司每天产生的用户行为数据、交易数据等都达到了惊人的规模。二是数据的多样性,不同来源和形式的数据相互交织,这增加了数据处理和分析的难度。三是大数据的产生和更新速度极快,要求能够实时或近乎实时地进行处理和分析,以便获取有价值的信息。尽管大数据中包含着丰富的信息,但价值密度相对较低,需要运用先进的技术和算法来挖掘其中的有用部分。大数据的应用领域也十分广泛。在商业领域,企业可以通过分析消费者的购买行为、偏好等大数据,精准地进行市场定位和营销策略制定,提高市场竞争力。在医疗行业,对海量的医疗数据进行分析,能够辅助疾病诊断、药物研发,为患者提供更个性化的医疗服务。交通管理部门可以利用大数据优化交通流量,减少拥堵,提高道路安全性。科研领域也得益于大数据,科学家们能够处理和分析大量的实验数据,加速研究进程,推动科学的发展。

## 2 大数据时代数据安全面临的挑战

### 2.1 数据量巨大与复杂性增加

在大数据时代,数据量呈爆炸式增长,这给数据安全带来了巨大的挑战。海量的数据使得安全防护的范围和难度大幅增加。传统的安全策略和技术在处理如此大规模的数据时往往力不从心,容易出现漏洞和疏忽。而且,大量的数据相互交织、关联复杂,使得数据的管理和追踪变得异常困难。例如,在一个大型电商平台上,每天产生的交易数据、用户浏览数据等庞大而复杂,要确保这些数据的安全性,需要投入大量的资源和精力来进行防护和监控。

### 2.2 数据多样性与来源广泛

大数据不仅规模大,还具有多样性和来源广泛的特点。数据可能来自内部的业务系统、移动设备,也可能来自外部的合作伙伴、社交媒体等。不同来源和类型的数据在格式、结构和安全性要求上存在差异,这增加了数据整合和保护的难度。同时,由于数据来源众多,难以对其进行全面的审查和验证,可能导致恶意数据或虚假信息混入,威胁数据的完整性和可靠性。比如,企业在进行数据分析时,如果引入了不可信的外部数据,可能会影响决策的准确性和安全性。

### 2.3 数据处理速度快与实时性要求

随着业务的发展,对数据处理速度和实时性的要求越来越高。这意味着数据在快速流动和处理的过程中,安全防护措施必须能够实时响应,确保数据的安全。然而,快速处理和实时分析可能导致安全检查的时间被压缩,容易忽略一些潜在的安全威胁。此外,为了满足高速处理的需求,可能会采用一些简化的安全策略,从而降低了安全防护的强度。例如,在金融交易中,需要在瞬间完成大量数据的处理和决策,如果安全机制不能及时跟上,就可能给黑客攻击留下可乘之机。

## 2.4 数据价值高与吸引力大

大数据中蕴含着巨大的价值,包括商业机密、个人隐私等敏感信息。这使得大数据成为了黑客、犯罪分子等不法分子的重点攻击目标。他们不惜投入大量的资源和精力来获取这些有价值的信息,从而导致数据泄露、篡改等安全风险增加。例如,一些知名企业的用户数据泄露事件,不仅给企业带来了巨大的经济损失,还严重损害了用户的信任和权益。<sup>[1]</sup>

## 3 大数据时代数据安全的主要威胁

### 3.1 网络攻击与黑客入侵

在大数据时代,网络攻击和黑客入侵的威胁日益严峻。随着数据价值的不断提升,黑客们有了更强烈的动机去突破企业和组织的网络防线,以获取有价值的信息。分布式拒绝服务(DDoS)攻击是常见的网络攻击手段之一。攻击者通过控制大量的傀儡机向目标服务器发送海量的请求,导致服务器瘫痪,正常用户无法访问。这不仅会影响业务的正常运行,还可能为后续的黑客入侵创造条件。例如,一家电商网站在促销活动期间遭受DDoS攻击,导致用户无法下单,造成了巨大的经济损失。另外,SQL注入攻击也是黑客常用的手段。通过在网页输入框中提交恶意的SQL语句,黑客能够绕过网站的验证机制,直接获取或篡改数据库中的数据。对于存储着大量用户信息和交易记录的大数据平台来说,这种攻击的危害极大。高级持续性威胁(APT)则更加隐蔽和危险。黑客组织会长长期潜伏在目标网络中,收集情报,寻找系统漏洞,然后在关键时刻窃取重要数据。这种攻击往往针对具有高价值数据的企业、政府机构等,一旦成功,后果不堪设想。

### 3.2 内部人员违规与数据泄露

内部人员违规操作和数据泄露是数据安全的一大隐患。内部员工由于熟悉企业的网络架构和数据存储方式,一旦出现违规行为,可能造成严重的数据安全问题。有些员工可能因为疏忽大意,将包含敏感数据的文件发送到错误的收件人,或者在未加密的设备上存储重要数据,从而导致数据泄露。还有些员工可能受到利益的诱惑,主动将企业的信息出售给竞争对手或其他非法组织。此外,离职员工也可能带走公司的重要数据。如果在离职流程中没有做好数据交接和权限回收工作,离职员工可能利用其之前掌握的权限访问和窃取数据。

### 3.3 数据隐私保护问题

随着大数据技术的广泛应用,个人数据的收集和分析变得越来越普遍,数据隐私保护问题也日益突出。许多应用程序在用户不知情的情况下收集大量的个人信

息,如位置、浏览记录、通讯录等。这些数据如果被不当使用或泄露,可能会对个人的生活造成严重影响,如遭遇骚扰、诈骗等。例如,一款健身应用收集了用户的详细运动轨迹和健康数据,却没有采取足够的安全措施保护这些数据,导致用户的隐私被泄露,个人生活受到干扰。而且,大数据分析技术能够通过关联和整合不同来源的数据,轻易地识别出个人的身份和行为模式。这就使得个人在大数据面前几乎毫无隐私可言。

### 3.4 云环境下的数据安全风险

随着云计算的广泛应用,数据存储和处理更多地依赖于云服务提供商。然而,云环境下的数据安全面临诸多挑战。一方面,用户对云服务提供商的信任至关重要,如果云服务提供商的安全措施不到位,可能导致数据泄露。另一方面,多租户的云环境中,不同用户的数据可能存储在同一物理设备上,如果隔离措施不完善,可能会造成数据的交叉感染和泄露。此外,数据在云端的传输和存储过程中,如果加密措施不当,也容易被窃取或篡改。<sup>[2]</sup>

## 4 大数据时代数据安全的关键技术

(1) 加密技术:加密技术是保护数据机密性的核心手段。它通过对数据进行编码和变换,使得只有拥有正确密钥的授权方能够解密并理解数据内容。在大数据环境中,加密技术不断演进,如采用高强度的加密算法对海量数据进行加密处理,确保数据在传输和存储过程中的安全性。同时,同态加密等新型加密技术的出现,使得在加密数据上进行计算成为可能,兼顾了数据处理的效率和安全需求。(2) 访问控制与身份认证:访问控制明确规定了谁可以在什么条件下访问哪些数据资源。通过设置严格的访问权限策略,限制用户对敏感数据的操作。身份认证则是确认用户身份的真实性,常见的方式包括密码、令牌、生物识别等。多因素身份认证结合多种验证方式,大大提高了身份验证的准确性和安全性。(3) 数据脱敏与匿名化:数据脱敏针对敏感数据进行处理,如遮盖、替换或修改部分内容,使敏感信息在特定场景下不可见。匿名化则是去除能直接关联到个人身份的标识信息,从而保护个人隐私。这两种技术在数据共享和分析中广泛应用,既满足了数据使用需求,又降低了隐私泄露风险。(4) 安全审计与监测:安全审计记录系统中的各种活动和事件,包括用户操作、系统运行状态等。监测则实时监控数据的访问和流动情况,通过对审计数据和监测信息的分析,可以及时发现异常行为和潜在的安全威胁,如非法访问、数据篡改等,并采取相应的应对措施。(5) 数据备份与恢复:数据备份是定期将重要

数据复制并存储到其他位置,以防止数据丢失。恢复则是在数据遭受损坏或丢失时,能够迅速从备份中还原数据。完善的数据备份策略包括选择合适的备份介质、确定备份频率和保留周期等,确保数据的可用性和完整性。<sup>[3]</sup>

## 5 大数据时代数据安全的防护策略

### 5.1 建立完善的安全管理制度

在大数据时代,建立完善的安全管理制度是确保数据安全的基本。先要明确数据的所有权和责任归属,确定谁对数据的安全性负有最终责任。这有助于在出现问题时能够迅速找到责任人并采取相应的措施。制定详细的数据分类和分级政策至关重要。根据数据的敏感性、重要性和价值,将其分为不同的级别,如绝密、机密、秘密和公开等。对于不同级别的数据,应实施不同程度的保护措施,例如对绝密数据采取最高级别的加密和访问控制。访问控制策略需要精确而严格。通过身份验证、授权和访问权限管理,确保只有经过授权的人员能够访问特定级别的数据。同时建立严格的账号管理机制,包括账号的创建、变更和删除,以及定期审查账号的权限,及时撤销不必要的权限。此外,还应建立数据的存储和传输规范。规定数据在存储过程中的加密方式、备份策略以及在传输过程中的加密和完整性验证方法,确保数据在任何环节都得到充分的保护。

### 5.2 加强员工安全意识培训

员工是数据安全链条中的关键环节,因此加强员工的安全意识培训刻不容缓。培训应涵盖多个方面,让员工充分认识到数据安全性的重要性和自身在保护数据安全中的责任。向员工普及常见的数据安全威胁,如网络钓鱼、恶意软件、社会工程学攻击等,使他们能够识别这些威胁的特征和手段。通过实际案例分析,让员工了解数据泄露可能带来的严重后果,从而增强他们的警惕性。教导员工如何正确处理和保护敏感数据,包括如何设置强密码、避免在不安全的网络环境中传输敏感信息、妥善保管工作设备等。同时,培养员工良好的工作习惯,如定期更新密码、不随意分享账号信息、及时报告可疑的安全事件等。定期组织模拟演练,让员工在实际场景中应对可能出现的数据安全问题,提高他们的应

急处理能力和团队协作能力。

### 5.3 进行定期的安全评估与漏洞修复

定期的安全评估是发现潜在安全隐患的重要手段。利用专业的安全评估工具和技术,对大数据系统的各个层面进行全面的检查,包括硬件设施、软件系统、网络架构、数据库等。通过漏洞扫描,及时发现系统中存在的安全漏洞,并对其进行风险评估,确定漏洞的严重程度和可能造成的影响。根据评估结果,制定优先级,优先修复高危漏洞。同时对系统的配置进行审查,确保其符合安全最佳实践。例如,检查服务器的安全设置、网络设备的访问控制列表、数据库的权限配置等,及时纠正不合理的配置。还应关注新兴的安全威胁和技术发展,不断更新安全评估的方法和标准,确保能够及时发现新出现的安全问题。<sup>[4]</sup>

### 5.4 构建应急响应机制

尽管采取了各种预防措施,数据安全事件仍有可能发生。因此,构建高效的应急响应机制是必不可少的。制定详细的应急预案,明确在发生数据泄露、系统故障等安全事件时的应对流程和责任分工。建立应急响应团队,包括技术专家、法务人员、公关人员等,确保在事故发生时能够迅速行动,采取有效的措施降低损失。

结束语:总之,大数据时代数据安全的发展是一个复杂且关键的议题。虽然面临诸多挑战,但通过关键技术的应用和有效的防护策略,我们有望为大数据构建一个安全可靠的环境。建立完善的安全管理制度、加强员工培训、定期评估修复以及构建应急响应机制等措施的协同作用,将为大数据的发展保驾护航。

## 参考文献

- [1]吕丰秀.大数据时代下计算机网络安全防御系统设计与实现分析[J].电子世界,2020(21):177-178.
- [2]王杨.浅析大数据背景下的信息安全隐患及防范措施[J].网络安全技术与应用,2020(11):9-11.
- [3]宋明武,王芳.大数据环境下数据安全问题分析与对策研究.现代情报,2022.42(2),114-120.
- [4]刘伟,钟玲玉,刘佳怡.大数据时代数据安全与隐私保护研究进展.计算机工程与设计,2024.43(8),432-436.