大数据云计算网络环境下的数据安全问题探讨

赵振动
深圳市常行科技有限公司
DOI:10.12238/acair.v2i3.8603

[摘　要] 在信息技术高速发展的推动下,大数据与云计算已成为推动社会进步和经济发展的重要力量。大数据以其海量的数据处理能力,为企业决策、科学研究乃至日常生活提供了前所未有的洞察力和效率,而云计算则以其资源共享、弹性扩展和按需服务的特性,极大地降低了 IT 成本,促进了信息技术的普及与应用。但是,在享受大数据与云计算带来的便利与效益的同时,其网络环境下的数据安全问题也日益凸显,所以需要做好数据安全防护。
[关键词] 大数据；云计算；网络环境；数据安全
中图分类号：G623.58　文献标识码：A

Exploration of Data Security Issues in the Network Environment of Big Data Cloud Computing

Zhendong Zhao
Shenzhen Changxing Technology Co., LTD

[Abstract] Driven by the rapid development of information technology, big data and cloud computing have become important forces in promoting social progress and economic development. Big data, with its massive data processing capabilities, provides unprecedented insights and efficiency for enterprise decision-making, scientific research, and even daily life, while cloud computing, with its characteristics of resource sharing, elastic expansion, and on-demand services, greatly reduces IT costs and promotes the popularization and application of information technology. However, while enjoying the convenience and benefits brought by big data and cloud computing, the issue of data security in its network environment is becoming increasingly prominent, so it is necessary to do a good job in data security protection.
[Key words] big data; Cloud computing; Network environment; data security

大数据云计算网络环境下的数据安全,不仅关乎企业的核心竞争力与商业机密,更直接影响到广大用户的个人隐私与权益。在数据驱动的时代下,数据的价值被无限放大,如果数据泄露或被非法利用,则会引发严重的经济损失、社会信任危机乃至国家安全风险。因此,深入探讨大数据云计算网络环境下的数据安全问题,寻求有效的防护策略与解决方案,构建安全、可信、高效的大数据云计算网络环境,对于保障信息安全、促进技术健康发展具有深远的意义。

1 大数据云计算网络环境下的数据安全问题分析

1.1数据泄露与隐私保护问题

在大数据云计算环境中,由于数据被存储在云端,而非传统的本地服务器中,增加了数据被未授权访问的风险,黑客可以通过网络攻击、漏洞利用或弱密码等手段获取敏感数据,如个人身份信息、企业财务数据等,导致严重后果,且云服务提供商的安全管理和安全措施若存在漏洞或不足,也可能成为数据泄露的源头。用户数据在云端被集中存储和处理,使得用户的隐私容易被非法收集、使用和泄露,比如用户的个人信息可能被用于广告推送或其他商业用途,严重侵犯用户隐私[1]。

1.2数据完整性问题

大数据云计算环境中,数据通常存储在分布式系统中,增加了数据完整性的挑战,由于数据的复制和分散存储,数据可能会受到损坏、篡改或丢失的风险,黑客能够通过恶意软件或网络攻击手段对数据进行篡改,破坏数据的完整性,且系统内部故障或操作失误也可能导致数据损坏,影响数据的准确性和可用性。在数据迁移过程中,遗留数据可能得不到彻底清除,传输数据也得不到有效保护,备份数据也可能存在安全隐患。

1.3数据共享与访问控制问题

大数据云计算环境下,面临着数据泄露和滥用的风险,如果没有足够的安全机制来保护数据的共享过程,那么数据的安全性将受到威胁,比如不同用户之间共享数据时,若未采取适当的访问控制和加密措施,则会导致数据被未授权访问或滥用。同时,在大数据云计算环境中,访问控制机制存在不足,例如

系统可能无法准确识别用户的身份和权限,导致未授权用户访问敏感数据。

1.4法律法规与合规性问题

随着大数据和云计算技术的快速发展,相关法律法规的滞后性日益凸显,现有的法律法规难以全面覆盖大数据云计算环境下的数据安全问题,导致监管空白和执法难度加大,例如对于跨境数据传输、个人信息保护等方面的法律法规尚不完善,难以有效保护用户隐私和数据安全。合规性是大数据云计算环境下数据安全的重要方面,但是由于法律法规的复杂性和多样性,云服务提供商面临合规性挑战。

2 大数据云计算网络环境下的数据安全问题的解决措施

2.1加强数据隐私防护

数据加密是保护数据隐私的基础措施,在大数据云计算环境中,需要采用先进的加密算法,对数据进行加密存储和传输,即使数据在传输过程中被截获,攻击者也无法轻易解读其中的内容,并实施严格的访问控制策略,确保只有授权用户才能访问敏感数据,通过多因素身份验证、权限分配和审计日志等手段,我们可以有效防止未授权访问和数据泄露。为了更有效地保护数据隐私,需要对数据进行分类,并根据其敏感程度制定相应的保护策略,通过建立数据分类体系,可以明确敏感数据,且利用敏感数据识别技术,可以自动检测和分类敏感数据,如个人身份信息、财务信息等,以便更好地对其进行保护[2]。隐私保护技术是加强数据隐私防护的重要手段,比如可以采用差分隐私、同态加密等隐私保护技术,对数据进行处理和分析,同时保护数据的隐私性,从而可以在不暴露原始数据的情况下,进行数据的挖掘和分析,从而有效保护用户的隐私。与此同时,数据生命周期管理是指对数据从创建到销毁的全过程进行管理,需要加强数据生命周期的各个阶段的管理,以确保数据隐私得到持续保护,应该制定数据保留政策,明确数据的保留期限和销毁方式;实施数据备份和恢复策略,以防止数据丢失和损坏,还需要对数据的使用和共享进行监控和审计,确保数据的合法使用。

2.2确保数据完整性

数据加密是保护数据完整性的基础,通过对数据进行加密,可以确保数据在传输和存储过程中不被未授权访问和篡改,还可以采用完整性校验机制,如哈希函数和数字签名,来验证数据的完整性;在数据传输和存储过程中,通过对数据进行哈希计算并生成数字签名,可以在数据接收方验证数据的完整性和真实性。在云计算环境下,应该制定完善的数据备份策略,定期对数据进行备份,并确保备份数据的可用性和一致性,并建立快速有效的数据恢复机制,以便在数据丢失或损坏时能够及时恢复数据,保证数据的完整性和业务连续性[3]。

分布式存储是云计算环境下的常见数据存储方式,为了确保数据的完整性,可以采用分布式存储技术,将数据分散存储在多个节点上,并通过冗余技术来增加数据的可靠性,通过在不同的节点上存储相同的数据副本,即使部分节点发生故障或数据丢失,也能够从其他节点上恢复数据,保证数据的完整性。为了及时发现数据完整性问题,需要建立数据完整性监测与报警机制,通过对数据进行实时监测和定期检查,可以发现数据的不一致性和异常变化,并及时采取相应的修复措施,同时建立报警机制,当监测到数据完整性问题时,能够及时通知相关人员并进行处理,防止问题进一步扩大。

2.3优化数据共享与访问控制

在数据共享过程中,需要采用先进的加密技术对敏感数据进行加密处理,确保数据在传输和存储过程中不被未授权访问和篡改,针对需要共享但又不希望完全暴露的数据,可以采用数据脱敏技术,通过去除、替换或掩盖敏感信息,降低数据泄露的风险,数据脱敏可以保护数据隐私,保留数据的使用价值,从而促进数据的合法共享。传统的访问控制机制通常基于角色或用户组进行权限分配,粗粒度的访问控制,难以满足大数据云计算环境下复杂多变的安全需求,所以需要建立细粒度的访问控制机制,根据数据的敏感性、用户的职责和需求等因素,设置精确的访问权限,通过基于属性的访问控制(ABAC)、基于角色的访问控制(RBAC)等高级访问控制模型,可以实现更加灵活和细致的权限管理,确保只有经过授权的用户才能访问特定数据[4]。

身份验证是确保数据访问安全的第一道防线,在大数据云计算环境下,需要采用多因素身份验证机制,结合密码、生物识别、动态令牌等多种身份验证方式,提高用户身份的真实性和可靠性,多因素身份验证可以有效防止密码泄露、钓鱼攻击等安全威胁,确保只有合法用户才能访问共享数据。在大数据云计算环境下,数据共享需要通过特定的协议和接口实现,为了确保数据共享的安全性,应采用安全的数据共享协议和接口,如OAuth、OpenID Connect等,可以提供标准化的认证和授权流程,支持细粒度的权限管理和数据访问控制,从而能够降低数据共享过程中的安全风险。

2.4完善数据相关法律法规

首先,针对大数据云计算环境下的数据安全问题,应制定专门的数据安全法律,明确数据处理的基本原则、数据安全保护义务以及违法行为的法律责任,比如我国已经实施的《数据安全法》就是一部针对数据安全领域的专门法律,规范了数据处理活动,保障数据安全,促进数据开发利用,保护个人、组织的合法权益,维护国家主权、安全和发展利益,未来需要继续完善相关法律,根据技术发展和社会需求的变化,适时修订和补充相关条款[5]。

其次,个人数据是数据安全保护的关键所在,在大数据云计算环境下,个人数据的收集、存储、处理和共享更加便捷,但同时也更容易遭受泄露和滥用的风险,所以需要加强个人数据保护立法,明确个人数据的收集、使用、共享等各个环节的法律规范,保障个人数据权益,例如《个人信息保护法》就是一部专门保护个人信息的法律,规定了个人信息处理的基本原则、个人信息权益的保护以及个人信息处理者的法律责任等内容,因此需要继续强化法律的执行力度,加大违法行为的惩处力度,形成有效的震慑作用。

第三，大数据云计算环境下的数据安全问题涉及多个领域和部门，所以需要建立跨部门的数据安全监管机制，形成合力，明确各部门的监管职责和权限范围，避免监管空白和重复监管，同时加强部门之间的信息共享和协作配合，形成联动监管效应。

最后，随着全球化的不断深入，数据跨境流动日益频繁，加强与国际数据保护法律的衔接显得是一项重要工作，为此我国需要积极参与国际数据保护规则的制定和谈判，推动建立公平、合理、透明的国际数据流动规则，并加强与主要国家和地区的数据保护合作，建立互信机制，共同应对跨国数据安全挑战，从而可以提升我国在国际数据安全领域的话语权和影响力，为我国企业“走出去”提供有力保障。

3 大数据云计算网络环境下数据安全未来发展趋势

首先，技术创新是推动数据安全发展的重要动力，未来大数据、云计算、人工智能、区块链等新技术将与数据安全深度融合，为数据安全提供更加强有力的技术支撑。例如，人工智能和机器学习技术，将在数据安全领域发挥越来越重要的作用，通过深度学习、大数据分析等方法，AI能够实时检测异常情况，有效识别和阻断数据泄露和滥用行为，且生成式人工智能的发展将进一步推动数据安全技术的创新，使其在内容策略、产品设计等领域发挥更大作用。其次，随着数据量的激增和数据类型的多样化，数据全生命周期的安全管理将成为未来数据安全发展的重要趋势，从数据的生成、存储、处理、传输到销毁等各个环节，都需要采取严格的安全措施来保障数据的安全性。最后，随着数据上云趋势的加速发展，云端数据安全将成为未来数据安全领域的焦点，云端数据安全不仅涉及云服务商自身的安全能力，还涉及客户数据在云端的存储、处理和传输过程中的安全性。云服务商将不断提升自身的安全能力，包括加强基础设施安全、完善安全管理体系、提升应急响应能力等，且云服务商还将加强与第三方安全机构的合作，共同提升云端数据的安全性。

4 结束语

综上所述，在信息技术发展的推动下，大数据、云计算等技术已经在诸多领域得到广泛应用。但是同时也暴露出了一定的数据安全问题，所以需要加强数据安全防护，采用科学的数据安全防控技术，确保数据安全性得到充分保障。

[参考文献]

[1]陈晓慧,郭琳.大数据云计算环境下的数据安全问题与防护研究[J].互联网周刊,2022(23):78-80.

[2]武岳.云计算中的大数据安全挑战与策略研究[J].科技创新与生产力,2022(12):21-23,27.

[3]刘晓东.大数据云计算环境下的数据安全问题与防护举措探究[J].物联网技术,2022,12(7):77-79.

[4]邓浩.解析大数据云计算网络环境的数据安全问题[J].通信电源技术,2023,40(6):208-210.

[5]危志军.基于云计算的大数据环境网络信息数据安全传输与共享方法[J].信息与电脑,2023,35(11):233-235.

作者简介：

赵振动(1987--),男,汉族,甘肃陇南人,本科,高级工程师,网络与数据安全。