

大数据应用中数据安全治理技术研究

范吟雪

兴安盟大数据中心 内蒙古 乌兰浩特 137400

摘要: 随着大数据技术的迅猛发展,其在各行各业的应用日益广泛,成为推动社会进步和经济发展的重要力量。数据安全治理作为保障大数据应用安全的重要手段,旨在通过一系列的策略、技术和措施,确保数据在采集、存储、处理、分析和应用等各个环节的安全性。随着大数据技术的不断发展和应用领域的不断拓展,数据安全治理的重要性也日益凸显。然而,由于大数据的复杂性和多样性,数据安全治理面临着诸多挑战和困难。因此,研究大数据应用中数据安全治理技术,对于保障数据安全、促进大数据技术的健康发展具有重要意义。

关键词: 大数据应用; 数据安全; 治理技术; 研究

引言:在信息化、数字化的时代背景下,大数据作为一种新型的信息资源,正在深刻改变着人们的生活方式和社会运行模式。大数据应用中数据安全治理技术不仅是保障数据资产安全的关键,也是提升大数据应用效果的重要保障,也是应对网络安全威胁的重要手段,更是促进数字经济健康发展的关键因素。因此,我们应该高度重视数据安全治理技术的研究和应用,为大数据应用的健康发展提供有力支持。

1 大数据应用中数据安全治理技术的重要性

在数字化浪潮的推动下,大数据应用已渗透到社会生活的方方面面,无论是商业决策、公共服务,还是科学研究,都离不开大数据的支持。然而,随着大数据应用的深入,数据安全治理技术的重要性也日益凸显。首先,大数据应用中的数据安全治理技术是保障数据资产安全的关键。数据作为一种新型生产要素,具有显著的规模经济和范围经济效应,是推动产业数字化转型升级以及构建国家数字竞争力的关键。然而,随着数据量的急剧增长和数据流动性的不断提升,数据泄露、数据滥用等风险也随之增加。数据安全治理技术能够通过数据的加密、脱敏、访问控制等手段,确保数据在存储、传输和使用过程中的安全,防止数据被非法获取或滥用。其次,数据安全治理技术是提升大数据应用效果的重要保障。大数据应用的核心在于数据的分析和挖掘,而数据的准确性和完整性是分析结果可信度的前提。数据安全治理技术可以通过数据清洗、数据校验等手段,确保数据的准确性和完整性,从而提升大数据应用的效果。数据安全治理技术还可以对数据的来源和流向进行追踪,为数据溯源和追责提供技术支持,进一步增强了大数据应用的可信度。此外,数据安全治理技术也是应对网络安全威胁的重要手段。在网络空间,大数据成为

网络攻击的重要目标。攻击者往往通过窃取、篡改或破坏数据来达成其目的^[1]。数据安全治理技术能够及时发现和应对网络攻击,保护数据的完整性和可用性,防止因数据安全问题导致的业务中断或损失^[1]。最后,数据安全治理技术对于促进数字经济健康发展具有重要意义。随着数字经济的不断发展,数据安全已成为影响数字经济稳定和健康发展的重要因素。数据安全治理技术能够为数字经济的健康发展提供有力保障,推动数字经济持续、稳定、健康发展。

2 大数据应用中数据安全治理的关键技术

2.1 数据加密技术

数据加密技术是大数据安全保障体系中的基石,其重要性不言而喻。在数字化日益普及的今天,数据的安全问题显得尤为突出,而数据加密技术则是解决这一问题的关键所在。数据加密的核心思想是将原始数据(明文)转化为无法直接读取的形式(密文),这种转化依赖于特定的算法和密钥。没有相应的密钥,即使数据被截获,攻击者也无法还原出原始数据,从而保障了数据的机密性。在大数据的应用场景中,无论是数据的传输还是存储,都可能面临安全风险。在数据传输过程中,使用加密技术可以确保数据在网络中的安全流动,防止数据泄露或被篡改。在数据存储阶段,加密技术同样发挥着不可替代的作用,它可以保护存储介质中的数据不被非法访问和篡改,确保数据的完整性和真实性。随着技术的不断进步,数据加密技术也在不断发展和完善。从最初的简单加密方法,到如今的对称加密、非对称加密等复杂算法,数据加密技术已经能够应对各种复杂的安全挑战。

2.2 数据脱敏技术

数据脱敏技术是在不影响数据分析结果的前提下,

对敏感数据进行处理,使得处理后的数据不再包含敏感信息,从而降低数据泄露的风险。在大数据应用中,数据脱敏技术可以广泛应用于数据共享、数据发布等场景。通过对敏感数据进行脱敏处理,可以在保护数据隐私的同时,满足数据分析的需求。例如,在医疗领域,通过对患者个人信息、疾病诊断等敏感数据进行脱敏处理,可以在保护患者隐私的同时,为医学研究和公共卫生管理提供有价值的信息支持。数据脱敏技术可以分为静态脱敏和动态脱敏两类。静态脱敏是在数据发布前对数据进行脱敏处理,生成不包含敏感信息的数据集^[2]。动态脱敏则是在数据访问过程中实时对数据进行脱敏处理,确保敏感信息不会被泄露。

2.3 数据访问控制技术

数据访问控制技术是通过实施精细化的数据访问控制策略,限制对数据的访问权限,防止数据被滥用或非法访问。数据访问控制技术可以有效地保护数据的机密性和完整性。通过设定访问权限、角色管理等措施,可以确保只有经过授权的用户才能访问特定的数据资源。访问控制技术还可以记录用户的访问行为,为后续的安全审计和事件追溯提供依据^[2]。常见的数据访问控制技术包括基于角色的访问控制(RBAC)、基于属性的访问控制(ABAC)等。这些技术可以根据用户的角色、属性等信息,动态地调整用户的访问权限,实现更加灵活和精细化的数据访问控制。

2.4 安全审计技术

在大数据应用中,安全审计技术可以记录用户的访问行为、数据操作等信息,形成完整的审计日志。通过对审计日志的分析和挖掘,可以发现异常访问、数据泄露等安全事件,及时采取相应的应对措施。安全审计技术还可以为数据安全提供数据支持,帮助组织了解数据的安全状况和风险分布,为制定更加有效的安全策略提供依据。此外,安全审计技术还可以与其他安全技术相结合,形成更加完善的安全防护体系^[3]。例如,可以将安全审计技术与数据加密技术相结合,对加密数据的访问和使用进行审计和监控;或者将安全审计技术与数据脱敏技术相结合,对脱敏数据的处理和使用进行记录和追溯。

3 大数据应用中数据安全面临的挑战

3.1 数据流转的不可控性

在大数据的采集、存储、处理和分析过程中,数据往往需要在多个系统和平台之间进行流转。这种流转的不可控性增加了数据泄露和滥用的风险。一方面,数据在流转过程中可能经过多个中间环节,每个环节都可能

存在安全漏洞,黑客可以通过这些漏洞窃取敏感数据。另一方面,数据的流转也可能导致数据被不当使用,例如,未经授权的数据共享和滥用,都可能对个人隐私和企业机密造成威胁。

3.2 攻击手段的多样化

随着黑客技术的不断发展,针对大数据的攻击手段也日益多样化。传统的安全防护手段往往难以应对这些新型攻击。黑客可以利用各种技术手段,如钓鱼攻击、恶意软件、DDoS攻击等,对大数据系统进行攻击。这些攻击可能导致数据泄露、系统瘫痪等严重后果。此外,黑客还可能利用大数据的复杂性和隐蔽性,进行隐蔽的数据窃取和篡改,使得数据失去真实性和可信度。

3.3 数据安全的滞后性

目前,关于大数据安全的规定和标准还不够完善,这在一定程度上制约了数据安全治理的发展。由于大数据技术的快速发展,现有的法规往往难以适应新的安全需求^[4]。不同国家和地区在数据安全方面的法规也存在差异,这给跨国企业和组织的数据安全管理带来了困扰。此外,数据安全规定的执行和监管也存在一定的难度,如何确保法规的有效实施和监管的到位,也是当前亟待解决的问题。

4 数据安全治理的策略

4.1 建立完善的数据安全管理制度

数据安全管理制度是数据安全治理的基石,它规定了数据安全的目标、原则、责任和义务。应明确数据安全政策,确立数据安全的重要性和战略地位,为数据安全治理提供明确的方向。其次,制定详细的数据操作流程,规范数据的采集、存储、处理、共享和销毁等各个环节,确保数据的合规性和安全性。此外,还应建立数据安全责任体系,明确各级组织和人员的职责和权限,形成齐抓共管的良好局面。在制度建设中,应注重制度的可操作性和实用性,避免形式主义。还应根据业务发展和技术变革的实际情况,及时对制度进行修订和完善,确保其始终适应数据安全治理的需要。

4.2 加强数据访问控制和身份认证

建立严格的数据访问控制机制,通过权限管理、角色划分等手段,对不同用户设置不同的访问权限和操作范围。其次,采用先进的身份认证技术,如多因素认证、生物识别等,确保用户身份的真实性。此外,还应定期对访问控制和身份认证系统进行审查和更新,确保其有效性和安全性。在加强数据访问控制和身份认证的同时,还应注重平衡数据安全和业务效率的关系。既要保障数据安全,又要避免过于繁琐的认证和授权流程影

响业务的正常开展。

4.3 强化数据加密和传输安全

在数字化时代，数据已然成为企业的核心资产，其安全性直接关系到企业的运营稳定与业务发展。因此，强化数据加密和传输安全显得尤为关键。（1）数据加密是确保数据安全的核心手段。通过采用先进的加密算法和技术，对敏感数据进行加密处理，可以有效防止数据在存储和传输过程中被非法获取或篡改。对于不同级别的数据，应实施不同级别的加密措施，确保数据的机密性和完整性。（2）网络传输的安全性同样不容忽视。在数据传输过程中，应采用安全的通信协议和加密技术，确保数据在传输过程中的安全。还应建立安全的传输通道，防止数据在传输过程中被截获或篡改。除了技术和协议的应用，加密密钥的管理也至关重要。密钥的安全性直接关系到加密数据的防护能力。应定期对加密密钥进行更换和管理，防止密钥被破解或泄露。还应建立严格的密钥管理制度，确保密钥的安全存储和使用。

4.4 定期进行数据备份和恢复

数据备份和恢复是保障数据安全的重要措施。应建立完善的备份机制，定期对重要数据进行备份，并确保备份数据的完整性和可用性。制定详细的恢复计划，明确在数据丢失或系统故障时的恢复流程和责任分工^[5]。还应定期对备份数据和恢复计划进行审查和测试，确保其有效性和可靠性。在数据备份和恢复方面，应注重备份策略的合理性和恢复能力的建设。根据数据的重要性和业务的需求，制定合适的备份周期和备份方式。加强恢复能力的培训和演练，提高组织和人员在数据丢失或系统故障时的应对能力。

4.5 加强数据安全监测和应急响应

建立全面的数据安全监测体系，实时监测和分析大数据系统的运行状态和安全状况。制定完善的应急响应预案，明确在发生安全事件时的处理流程和应对措施。此外，还应加强应急响应团队的建设和培训，提高其在处理安全事件时的专业能力和响应速度。在数据安全监测和应急响应方面，应注重预警机制的建立和响应流程的优化。通过实时监测和分析大数据系统的安全日志和

事件信息，及时发现潜在的安全威胁并进行预警。优化应急响应流程，简化决策和协调环节，提高响应的效率和准确性。

4.6 提升员工数据安全意识和技能

员工是数据安全治理的重要参与者和执行者，其数据安全意识和技能水平直接关系到数据安全治理的效果。因此，应定期开展数据安全培训和教育活动，提高员工对数据安全的认识和重视程度。培训内容应包括数据安全基础知识、安全操作规范、应急处理流程等方面，帮助员工全面了解数据安全的重要性和应对方法。加强员工的技能培养和实践操作，使其在日常工作中能够自觉遵守安全规范，防范安全威胁。此外，还应建立激励机制和奖惩制度，鼓励员工积极参与数据安全治理工作，对在数据安全工作中表现突出的员工给予表彰和奖励；对违反安全规定或造成安全事件的员工进行严肃处理，形成有效的约束和激励机制。

结语

综上所述，大数据应用中数据安全治理涉及多个方面，需要从制度、技术、监测和人员等多个角度进行综合考虑。通过建立完善的数据安全管理制度、加强数据访问控制和身份认证、强化数据加密和传输安全、定期进行数据备份和恢复、加强数据安全监测和应急响应以及提升员工数据安全意识和技能等措施，可以全面提升大数据应用的数据安全保障能力，确保数据的机密性、完整性和可用性，为企业的持续发展提供有力的支撑。

参考文献

- [1]贾若飞.大数据应用中数据安全治理技术研究[J].中国设备工程,2023(2):26-28.
- [2]陈鹏东.大数据时代数据安全治理的网络安全研究[J].数字通信世界,2021(2):167-169.
- [3]韩应升.大数据时代下的数据安全治理措施研究[J].电脑爱好者(普及版),2023(1):16-18.
- [4]徐双,刘文斌,李佳龙,等.大数据背景下的数据安全治理研究进展[J].太原理工大学学报,2024,55(1):127-141.
- [5]姜涛,李浩鑫.基于精准治理的大数据安全治理体系创新研究[J].中国高新科技,2021(23):45-46.