大数据应用中的数据安全治理技术

陈凯凯
杭州瑞检软件科技有限公司　浙江杭州　310000

摘　要：本文主要探讨了大数据应用中的数据安全治理技术，在数据安全治理技术的应用现状方面，介绍了数据安全治理技术的定义和分类，以及其在大数据应用中的应用情况。在存在的问题方面，分析了数据隐私保护问题、数据安全风险问题和数据安全治理技术本身存在的问题。在解决方案和建议方面，提出了采用数据脱敏技术、加强安全意识教育和限制数据共享范围等解决方案。同时，也提出了采用数据加密技术、加强访问控制管理和强化数据备份和恢复机制等解决方案。在未来发展趋势方面，探讨了大数据安全治理技术和数据安全法规和标准的发展趋势。

关键词：大数据；数据安全；治理技术

Data security governance technology in the application of big data

Kaikai Chen
Hangzhou Ruijian Software Technology Co., LTD., Hangzhou, Zhejiang, 310000

Abstract: This paper mainly explores data security governance techniques in the context of big data applications. Regarding the current application status of data security governance techniques, it introduces the definition and classification of these techniques, along with their application in big data scenarios. Addressing the existing issues, the paper analyzes problems related to data privacy protection, data security risks, and challenges within data security governance technologies themselves. As for solutions and recommendations, the paper proposes employing data anonymization techniques, strengthening security awareness education, and limiting data sharing scope. Additionally, it suggests utilizing data encryption methods, enhancing access control management, and reinforcing data backup and recovery mechanisms. Regarding future development trends, the paper delves into the evolution of big data security governance techniques and data security regulations and standards.

Keywords: big data; data security; governance technology

引言：

随着互联网和移动技术的迅速发展，大数据应用已经成为现代社会中的重要组成部分[1]。大数据的处理和分析能力可以为企业、政府、科研机构等提供更多的价值和优势。但是，大数据应用也带来了诸多安全风险和挑战，例如数据泄露、隐私泄露、数据滥用等问题，这些问题严重威胁着大数据应用的安全和稳定。因此，在大数据应用中，数据安全治理技术显得尤为重要。

一、大数据应用发展背景和重要性

随着互联网和移动技术的快速发展，人们可以产生和存储的数据量呈爆炸式增长[2]。这些数据包括个人信息、交易记录、社交媒体内容等，大量数据的存储和处理能力已成为企业、政府和科研机构等领域中获取竞争优势的重要手段。而大数据技术的快速发展和应用，也为数据分析、数据挖掘、机器学习、人工智能等领域提供了更加广泛和深入的探索和应用空间。

1.大数据应用的发展历程

大数据应用的发展历程可以大致分为以下三个阶段：首先是数据化阶段，20世纪90年代，企业和机构开始利用关系型数据库等技术进行数据管理和分析；接着是大数据阶段：2000年代，随着互联网、移动技术和传感器技术的迅速发展，数据量呈爆炸式增长，使得传统的数据管理和分析技术已经无法满足需求。此时，Hadoop、Spark等大数据技术的出现，为数据的存储、处理和分析提供了更加高效和可扩展的解决方案；当前为智能化阶段：人工智能、机器学习等技术的兴起，进一步推动了

大数据应用的智能化发展，使得大数据分析和挖掘的效率和精度进一步提升，为企业和机构带来更多的商业价值和社会效益。

2.大数据应用的重要性和优势

大数据应用的重要性和优势主要体现在以下几个方面：促进商业创新和增长：大数据技术可以挖掘出消费者需求和趋势，帮助企业开拓市场，推出新的产品和服务，提高企业的盈利能力和市场竞争力[3]；改善公共服务和决策：大数据技术可以帮助政府和机构实现更精准、更高效的公共服务，例如医疗健康、交通运输等领域。同时，大数据技术还可以为政策制定和决策提供更加科学、准确的依据；加速科学研究和技术创新：大数据技术可以帮助科研机构和企业更好地理解和利用数据，加速科学研究和技术创新的进程，推动新的发现和创新；提高生产效率和降低成本：大数据技术可以帮助企业优化生产流程，提高生产效率和产品质量，同时还可以降低生产成本和资源浪费；提升风险防控和安全保障：大数据技术可以帮助企业和机构更好地识别、预测和防范风险和安全威胁，保障数据和信息的安全和隐私。

二、数据安全治理技术在大数据应用中的应用现状

1.数据安全治理技术的定义和分类

数据安全治理技术是指在大数据应用过程中对数据进行安全保护和管理的技术手段和方法，包括数据保护、数据隐私保护、数据质量管理、数据合规性管理等多个方面[4]。数据安全治理技术可以分为以下几个方面：数据分类和分级：通过对数据的分类和分级，实现对不同等级数据的安全保护和管理；数据加密和解密：采用不同的加密算法对数据进行加密，确保数据传输和存储过程中的安全；数据备份和恢复：通过备份和恢复技术，确保数据在意外丢失或损坏时能够及时恢复；数据脱敏和匿名化：对敏感数据进行脱敏或匿名化处理，确保个人隐私的保护；数据访问控制：通过权限管理、身份认证等技术手段，控制不同用户对数据的访问权限；数据审计和监控：通过数据审计和监控技术，实现对数据访问、使用等行为的监测和记录。

2.数据安全治理技术在大数据应用中的应用情况

数据安全治理技术在大数据应用中具有重要的应用价值。随着大数据应用的不断发展，数据安全问题逐渐成为制约大数据应用的瓶颈之一。在实际应用中，数据安全治理技术被广泛应用于以下几个方面：数据隐私保护：在数据采集、存储、处理等环节中，通过数据脱敏、加密等技术手段，保护个人隐私；数据共享安全：在数据共享过程中，通过数据访问控制和审计监控等技术手段，确保数据共享的安全性和可控性；数据质量管理：通过数据质量管理技术，提高数据质量和可信度，降低数据误差和不确定性对应用的影响；数据合规性管理：在数据采集和处理过程中，确保数据的合规性和合法性，遵循相关法律和政策要求。

三、数据安全治理技术在大数据应用中存在的问题

1.数据隐私保护问题

在大数据应用中，个人隐私保护问题一直备受关注。尽管采用了数据脱敏、加密等技术手段进行保护，但仍然存在数据泄露、滥用等问题。具体表现为：数据安全意识不足：在大数据应用中，一些企业和个人对数据安全意识不足，导致数据保护措施不够完善；数据脱敏不彻底：一些数据脱敏技术难以做到完全脱敏，容易导致数据泄露；数据滥用和共享：在数据共享过程中，一些数据被滥用或用于非法用途，导致个人隐私泄露。

2.数据安全风险问题

由于数据来源的多样性、数据量的庞大、数据存储的多样性等原因，存在着一定的数据安全风险。具体表现为：数据存储不安全：由于数据存储方式的多样性，一些数据存储存在安全风险，如云存储等；数据传输不安全：由于数据传输过程中存在信息泄露的风险，因此需要采用数据加密等技术手段进行保护；数据处理不当：在数据处理过程中，由于人为因素、技术问题等原因，可能导致数据处理不当，进而影响数据安全。

3.数据安全治理技术本身存在的问题

数据安全治理技术在实际应用过程中，也存在一定的问题和挑战。具体表现为：技术手段不完善：当前数据安全治理技术还存在一些不足，如数据脱敏技术难以做到完全脱敏等问题；数据安全治理成本高：在数据安全治理过程中，需要投入大量的人力、物力和财力，成本较高；数据安全治理标准不统一：当前缺乏统一的数据安全治理标准，不同企业和组织对数据安全的要求不同，导致治理效果参差不齐。

四、数据安全治理技术在大数据应用中的解决方案和建议

1.数据隐私保护的解决方案

为了更好地解决数据隐私保护的问题，数据脱敏技术被广泛应用于大数据应用中。数据脱敏是指将敏感数据的部分内容或全部内容替换为不敏感的信息，以保护数据的安全性。在数据脱敏的过程中，需要考虑数据的脱敏算法、脱敏等级、脱敏效果等因素。数据脱敏技术可以采用匿名化、脱敏掩码、加密等多种手段来实现。

除了技术手段之外，加强安全意识教育也是非常重

要的。企业应该定期开展数据安全培训，增强员工和用户的安全意识，使他们更加重视数据安全和隐私保护。此外，企业还可以通过加强权限管理、实施访问控制等方式，限制敏感数据的共享范围，确保只有授权人员才能访问，从而降低数据泄露的风险。

2.数据安全风险的解决方案

针对数据安全风险问题，可以采取以下解决方案：首先，采用数据加密技术。在大数据应用中，数据传输和存储中存在着安全隐患。因此，采用数据加密技术可以在一定程度上减少数据在传输和存储过程中的风险。数据加密技术可以将数据转化为密文，只有经过授权的用户才能够解密获取其中的内容。这样可以有效避免未经授权的用户获取敏感数据的风险。其次，加强访问控制管理。在大数据应用中，为了确保数据安全，需要对访问数据的人员进行身份验证，只有经过授权的用户才能够访问相关数据。访问控制技术可以实现对用户身份的识别和认证，以及对用户访问权限的控制。这样可以有效避免未经授权的用户访问敏感数据的风险。此外，强化数据备份和恢复机制。在大数据应用中，为了确保数据的可用性和完整性，需要建立完善的数据备份和恢复机制。通过定期备份数据可以确保数据的安全性，同时在数据异常或者数据丢失时可以及时进行数据恢复，减少数据损失的风险。

3.数据安全治理技术的提升方案

在提高数据安全治理技术的水平和应用效果方面，可以采取加强技术研究的措施。随着大数据应用的不断发展，数据安全治理技术也在不断更新和迭代，需要加强研究和创新，探索更加先进的技术手段，提高技术水平和应用效果。

在确保数据安全的标准化方面，可以制定统一的数据安全标准和规范。可以为企业和组织提供一个共同的参考框架，使得它们能够更加有针对性地实施数据安全管理。这些标准和规范可以包括数据分类、加密、备份、恢复、访问控制、身份认证、审计和监控等方面的要求和实践。通过统一标准，企业和组织可以更好地应对不同类型的数据安全风险，避免不必要的安全漏洞和损失。此外，可以建立数据安全治理机构，加强数据安全监管和管理，提高数据安全保障水平。数据安全治理机构可以负责统筹规划、协调实施数据安全治理工作，加强数据安全的监管和管理，从而提高数据安全保障水平，减少数据泄露和滥用的风险。

五、数据安全治理技术在未来的发展趋势

面向智能化的技术发展：未来的大数据安全治理技术将更加智能化，如采用人工智能、机器学习等技术，从而更好地识别和预测安全威胁；融合多种技术的集成应用：大数据安全治理技术将会融合多种技术，如区块链技术、物联网技术等，以满足更加复杂多变的数据安全需求；安全攸关的数据安全治理技术：随着大数据应用领域的不断拓展，越来越多的数据将成为安全攸关数据，因此大数据安全治理技术将更加注重数据隐私和安全保障。

由于国家法规和标准的出台：随着大数据应用领域的不断发展，各国政府将会加强对数据安全的管理和监管，逐步建立完善的数据安全法规和标准；行业标准的不断完善：随着不同行业对数据安全的需求不断增加，各个行业将会制定更加细化的数据安全标准和规范，以满足各自的数据安全需求；国际标准的不断推广：数据安全是一个全球性的问题，因此国际标准的推广将会成为一个趋势，以便不同国家和地区之间更好地协作和合作，共同应对数据安全的挑战。

六、结论

本文对大数据应用中的数据安全治理技术进行了深入的研究和探讨，分析了数据安全治理技术在大数据应用中的应用现状和存在的问题，并提出了解决方案和建议。本文指出，在大数据应用中，数据安全治理技术是确保数据安全的关键，要求相关机构和企业加强数据安全治理技术的应用和研究，建立健全的数据安全保障体系，同时还需要加强数据安全法规和标准的制定和执行。未来，大数据安全治理技术将进一步发展，为大数据应用的安全和发展提供更加全面和有效的保障。

参考文献：

[1]王英，张睿婵，王铖.我国大数据应用中的数据伦理风险及其治理研究进展[J].图书馆工作与研究，2023（04）：39-47.

[2]刘沛汐，李鑫，苏伟光，张冬冬.大数据应用中的数据安全治理技术分析[J].网络安全技术与应用，2022（12）：43-45.

[3]高磊，赵章界，宋劲松，翟志佳，杨芬，蒋宋.大数据应用中的数据安全治理技术与实践[J].信息安全研究，2022，8（04）：326-332.

[4]任勇，刘乐明.大数据应用中的风险防控与国家治理效能的提升[J].江西师范大学学报（哲学社会科学版），2020，53（03）：14-19.