

# 大数据应用中数据安全治理技术研究

陈梓敬

武汉安桢瑞网络科技有限公司

**摘要：**随着大数据时代的迅猛发展，数据的规模和复杂性呈现爆炸式增长，对数据安全提出了更为迫切的需求。大数据应用不仅包含海量数据，还需要高效的管理和强大的安全保障机制。在这一背景下，数据安全治理成为大数据应用中不可或缺的关键环节。本文旨在通过系统研究大数据应用中的数据安全治理技术，从全局的概述、基本原则的明晰，技术架构的深入，一直到实际应用的具体操作，全面剖析大数据安全治理的核心要点。通过这一深入研究，我们将更好地理解在这个日益复杂和风险加大的大数据环境中，如何保障数据的安全、完整性和可用性，以应对未来不断演变的挑战。

**关键词：**大数据；数据安全治理；技术架构；基本原则；实际应用

【DOI】10.12252/j.issn.2096-6288.2022.11.029

## 引言

数据安全治理技术旨在通过系统的管理和控制手段，确保数据在其生命周期内受到有效的保护和监管。这包括数据的采集、存储、传输、处理和分析等各个环节，以及与之相关的人员、系统和流程。数据安全治理技术的研究不仅涉及技术层面的创新，还需要综合考虑组织结构、法规合规等多方面因素，以建立起全面、高效的数据安全保障体系。

### 一、大数据应用中数据安全治理概述

#### （一）大数据及大数据安全

大数据，作为当今数字化时代的显著特征，涵盖了规模庞大且类型多样的数据集合。这种数据规模之庞大，已超越了传统数据处理工具的能力范围，因此需要高度并行处理的技术来实现对其内在有用信息的提取。大数据的出现使得人们能够更全面地洞察和理解复杂的现实世界现象，为决策和创新提供了强大支持。

#### （二）大数据应用中数据安全治理的内涵

数据安全治理在大数据应用中具有丰富而深刻的内涵。它涉及建立一套系统性的管理体系，以规范和指导整个大数据处理的过程。这包括从数据的采集、传输、存储到处理和 analysis 的全方位监管，确保每个环节都符合法规和政策的要求。其次，数据安全治理注重规范化，即通过设定明确的标准和流程，确保大数据的使用符合一定的准则和标杆，从而降低数据被滥用或泄露的风险。控制也是数据安全治理的核心，包括对数据访问权限的严格控制，以及对数据流动和传输的有效管理，以防范未经授权的访问和使用。监督作为数据安全治理的另一支重要手段，通过实时监测和审计，可以及时发现并应对潜在的安全威胁，保障数据处理的透明度和可追

溯性。

### 二、数据安全治理基本原则

#### （一）经济性

经济性原则在数据安全治理中强调在数据安全的追求中，必须找到经济效益与安全性之间的平衡点，确保在提高安全水平的前提下，不会过度增加成本。这一原则的核心理念是通过最优的资源配置，充分实现数据安全所需的控制和保障，同时有效降低实施数据安全措施的经济负担。在制定数据安全治理策略时，需要综合考虑投入和产出的关系，以确保每一项安全措施都经济合理。

#### （二）可操作性

可操作性原则在数据安全治理中强调在制定和实施安全方案时需注重实际可行性。核心理念是确保安全措施能够在组织内轻松实施、监管和维护，以确保整体数据安全策略的无缝执行。这一原则的目标是实现安全策略的实际操作性的最大化，确保其在组织内广泛适用、易于执行。通过强调可操作性，机构能够更好地应对复杂的安全挑战，确保安全措施能够顺利融入业务流程，最终保障数据安全的有效实施。

#### （三）合规性

合规性原则在数据安全治理中强调数据处理必须符合相关法规和标准，确保数据的合法性和合规性。这一原则的核心理念是在数据安全措施的制定和实施中，必须对法律法规和行业标准有严格的遵循，以确保组织的数据处理活动是在法律框架和行业规范下进行的。

#### （四）完备性

完备性原则在数据安全治理中强调数据安全措施应构建一个全面的体系，覆盖数据生命周期的各个环节，确保数据的安全性得到全面而完备的保障。这一原则的

核心理念是将数据安全视为一项综合而全面的任务，不仅仅是在某一环节或阶段进行局部的保护，而是要贯穿整个数据处理流程。

### （五）可问责性

可问责性原则在数据安全治理中占据着至关重要的位置，强调建立明确的责任体系，以确保在面对数据安全问题时能够进行追溯和问责。这一原则的核心理念是通过规范的组织结构和流程，确保每个参与数据处理的环节都能够明确自己的职责，从而推动数据安全治理的真正落地。

### （六）可追溯性

可追溯性原则在数据安全治理中强调建立一套能够追踪数据处理每一个环节的系统，以便发现和处理安全问题。这一原则的核心理念是通过记录和监测，确保数据处理过程的透明度和可溯源性，使得在发生数据安全问题时能够快速定位问题源头，从而更有效地进行安全应对。

## 三、数据安全治理技术架构

### （一）数据全生命周期安全治理

数据全生命周期安全治理构建了一个全面而系统的数据安全框架，从数据的采集、传输、存储、处理到分析，确保每个环节都拥有相应的安全措施。首先，数据采集阶段要求实施合适的控制措施，包括身份验证、加密传输等，以防止未经授权的数据采集和操纵。传输环节注重数据传递的加密和安全通道的确立，防范数据在传输过程中的窃听和篡改。数据存储阶段强调对存储设备的物理和逻辑安全性，采用加密、访问控制等手段，以防止未授权访问和数据泄漏。在数据处理和分析阶段，全生命周期安全治理强调在处理过程中采取适当的访问控制和权限管理，确保只有授权人员能够访问敏感信息。分析环节需要强调数据匿名化、脱敏等隐私保护措施，以平衡数据分析的需求与隐私保护的要求。此外，对于废弃或过期数据的处理，也需要采取相应的安全手段，如安全销毁或归档，防止废弃数据被滥用。

### （二）事件分析与处置

事件分析与处置构架旨在通过实时监控和分析数据使用过程中的异常事件，以及在发现安全威胁时能够及时而有效地处置，从而防范潜在风险。实时监控采用先进的安全信息与事件管理系统，通过实时数据流的监测，能够及时捕获任何可能的异常活动，包括不寻常的数据访问、登录行为或系统操作。监控系统与日志分析

技术相结合，能够对数据使用情况进行全面追踪和审计。一旦监测到异常事件，事件分析与处置构架迅速介入，进行深入分析事件的性质、来源和威胁级别。这一过程需要利用先进的威胁情报和分析工具，确保对安全事件的准确判断。同时，系统还需要与其他安全防护措施（如入侵检测系统）集成，以获取更全面的安全事件信息。基于对异常事件的准确分析，事件处置环节迅速采取相应的措施，包括隔离受影响的系统、加强访问控制、阻止威胁传播等。

## 四、数据安全技术应用

### （一）数据采集与存储环节

数据采集与存储环节在数据生命周期中需要采取有效的安全措施以防范数据泄漏风险。在数据采集阶段，加密和脱敏技术是两个重要的手段，可有效保护数据的机密性和隐私性。数据采集中的加密技术通过对传输通道和数据本身的加密，确保数据在采集过程中不容易被恶意截取或篡改。采用传输层加密等协议，可以在数据从源头传输到采集点的过程中，将数据加密，防止被未经授权的第三方访问。此外，对于敏感信息，如身份证号、信用卡号等，可以在采集时采用字段级别的加密，确保即便在传输过程中被截获，也难以解密和识别敏感内容。在数据存储环节，采用加密和脱敏手段也是必要的。加密存储可以在数据库或存储设备层面对数据进行加密，确保即便存储介质被非法获取，数据也无法轻易解读。脱敏技术则通过替换、删除或模糊敏感信息，保留数据的格式和结构的同时，降低了敏感信息的泄漏风险。例如，可以对数据库中的姓名、地址等字段进行脱敏处理，以保护用户的隐私。举例来说，一家医疗机构在进行患者数据采集时，可以采用字段级别的加密技术，对患者的个人身份信息进行保护。同时，将患者病历等敏感数据在存储时进行整体加密，确保即便数据库被攻击，也难以获取敏感的病患信息。

### （二）数据发布

数据发布需要在确保数据可用性的同时，对敏感信息进行充分保护，以防止泄漏风险。在数据发布过程中，严格的控制措施是至关重要的。通过对敏感信息姓名、地址、身份证号等字段进行模糊、替换或删除，确保发布的数据不包含真实身份信息。例如，一家电商公司在发布销售数据时，可以对购买者的具体姓名和地址信息进行脱敏，仅展示地域或匿名标识，以保护用户的

隐私。另外，进行数据权限控制。发布数据时，应根据用户或用户组的权限，仅开放其有权访问的部分数据。例如，在一个企业内，对于不同部门的员工，发布的数据应根据其工作职责进行权限划分，确保只有合适的人员能够获取相关信息。加强数据的元数据管理也是数据发布的必要环节。通过定义和维护数据的元数据，包括数据的来源、用途、质量等信息，有助于更好地理解数据的敏感性和可用性。在数据发布时，可根据元数据信息制定相应的发布策略，确保数据在合规的范围内得到利用。综合应用这些措施，可以有效地保障数据发布环节的安全性。例如，一家金融机构发布贷款业务统计数据时，采用脱敏技术对客户身份信息进行处理，同时根据不同部门的业务需求设置差异化权限，以确保敏感信息仅对具备授权的人员可见，从而在提供数据可用性的同时，最大程度降低潜在泄漏风险。

### （三）数据分析

在数据分析过程中，通过权限控制和数据审计等手段，可以有效防止未经授权的数据访问和使用，保障敏感信息不被滥用。通过权限控制，数据分析人员仅被授予特定的数据访问权限，确保他们只能获取和使用与其工作职责相关的数据。例如，在一家零售公司，销售团队可能只需要访问销售数据，而财务团队可能只需要访问财务报表。通过设置不同的权限，可以避免敏感信息被不相关的人员访问。其次，数据审计是防止未经授权访问的关键步骤。通过记录数据访问事件，包括时间、地点、用户等信息，可以随时监测和审计数据的使用情况。如果一名数据分析人员尝试访问与其职责范围无关的敏感数据，系统会生成审计日志并向管理员发出警报，及时发现和应对潜在的安全威胁。使用数据脱敏技术也是在数据分析中保护隐私的有效手段。在进行数据分析之前，对敏感信息进行脱敏处理，以降低敏感数据的风险。例如，一家健康科技公司在进行研究时，通过对患者的个人身份信息进行脱敏处理，确保在数据分析过程中既保持科学性和准确性，又平衡了患者隐私的合理保护。这种措施有助于促进医疗研究的进行，同时遵循隐私保护原则，建立了安全可信的数据分析环境。

## 五、加强数据安全治理的建议

安全培训和意识提升是保障数据安全的关键战略之一，通过培训员工了解数据安全的基本原则、法规要求

和操作规程，可以显著降低因员工错误或疏忽导致的数据安全问题。通过定期的安全培训课程，组织可以向员工传递最新的数据安全知识。这些培训课程可以涵盖数据的敏感性、合规性要求、安全操作规程等方面的内容。例如，一家金融机构可以组织培训课程，介绍有关客户隐私、金融交易安全等方面的最新法规和政策，帮助员工更好地理解和遵守相关法规，从而保护客户数据的安全。另一方面，通过模拟演练和实际案例分析，让员工更直观地理解潜在的数据安全威胁和应对措施。例如，在一个制造业企业中，可以模拟针对恶意软件攻击的演练，让员工了解如何辨别可疑邮件、采取紧急措施等，提高应对紧急情况的能力。再一方面，建立内部的数据安全社区和在线平台，促进员工之间的经验交流和知识分享。通过分享真实的数据安全案例和解决方案，员工可以从彼此的经验中学到更多实际操作的技能。例如，一个科技公司可以创建内部论坛，促使员工分享设备安全、软件漏洞修复等经验。培训中强调日常工作中的责任和义务，激发员工对数据安全的责任心。通过这种方式，公司能够建立起内部学习平台，提高员工在数据安全领域的专业素养，共同维护公司信息安全。最后，确立定期的数据安全知识检测和评估机制，采用测验和考核方式检查员工对数据安全知识的掌握水平。这可以通过在线测试、定期安全意识问卷等形式进行，以确保员工对数据安全的了解程度得到持续监测和提高。

### 结束语

数据安全治理技术在大数据应用中扮演着至关重要的角色，对于保障数据的安全性和合规性具有重要意义。通过对大数据应用中数据安全治理概念、基本原则、技术架构、实际应用的系统研究以及加强数据安全治理的建议，可以为相关领域的研究和实践提供有力支持。在未来，随着技术的不断发展和数据应用的深入，数据安全治理技术也将不断完善和创新，以更好地适应复杂多变的大数据环境。

### 参考文献

- [1] 马晨, 赵慧广. 总体国家安全观视域下公安大数据安全治理的挑战与应对[J]. 武警学院学报, 2021, 37(12): 52-56.
- [2] 许杰, 张锋军, 陈捷等. 面向大数据环境下的数据安全治理技术[J]. 通信技术, 2021, 54(12): 2659-2665.