数据应用中的数据安全治理技术分析

赵光灿 神应军 张 然 陈 军
山东中移通信技术有限公司，山东 济南 250004

[摘要]随着数字时代的迅猛发展，大数据应用成为推动创新和社会变革的引擎。与日俱增的数据规模和应用场景也带来了日益复杂的数据安全挑战，隐私泄露、数据篡改和网络攻击等问题不断凸显，为数据的安全性和隐私保护提出了更高的要求。数据安全治理成为确保数字社会稳定和可持续发展的迫切需求，数据安全治理致力于保护信息资产的安全性和维护用户隐私，并确保数据合法使用。深入研究数据安全治理技术，特别是在人员管控、生命周期治理、系统防护和事件处理等方面，对应对当今复杂的数据安全挑战具有重要意义。

[关键词]数据安全治理；数据应用；数字时代
DOI：10.33142/sca.v6i12.10643 中图分类号：TP311.13 文献标识码：A

Analysis of Data Security Governance Technology in Data Application

ZHAO Guangcan, SHEN Yingjun, ZHANG Ran, CHEN Jun
Shandong China Mobile Communication Technology Co., Ltd., Ji'nan, Shandong, 250004, China

Abstract: With the rapid development of the digital age, big data application have become the engine driving innovation and social change. The increasing scale and application scenarios of data have also brought increasingly complex data security challenges, such as privacy leakage, data tampering, and network attacks, which constantly highlight higher requirements for data security and privacy protection. Data security governance has become an urgent need to ensure the stability and sustainable development of the digital society. Data security governance is committed to protecting the security of information assets, maintaining user privacy, and ensuring the lawful use of data. In depth research on data security governance technology, especially in personnel control, lifecycle governance, system protection, and event processing, which is of great significance for addressing today's complex data security challenges.

Keywords: data security governance; data application; digital age

引言

在当今数字化浪潮的推动下，数据成为推动创新和发展的核心资源。大数据应用不仅为企业提供了更深刻的洞察力，也推动了社会的数字化转型，随之而来的是对数据安全性和隐私保护的日益严峻的挑战，个人隐私泄露、数据篡改和网络攻击等问题已成为数字时代的突出难题。

1 数据安全治理思路

1.1 基本治理原则

在数据安全治理中，基本原则是确保全面性、透明性和持续性。全面性要求治理措施覆盖从数据采集到处理、存储和传输的整个生命周期，透明性是指明确规定和向相关方通报数据使用规则，确保数据的合法性和合规性。同时持续性强调了治理的不间断性，要求随着技术和法规的变化不断更新和完善治理措施。

1.2 关键治理要点

在数据安全治理中，关键要点是确保严格的身份验证和访问控制机制。身份验证要求有效地确认用户身份，采用多层次的身份验证方法，如多因素身份验证，以提高安全性，访问控制则着眼于细粒度的权限管理，确保每个用户只能访问其工作职责所需的数据，最小化数据暴露的风险。此外数据分类与敏感信息标识也是治理的重点，通过明确对数据的分类，可以有针对性地采取相应的安全措施，同时对敏感信息的准确定义和标识，有助于及时识别和防范潜在的风险和威胁。建立完善的监管系统，能够实时监控数据的访问和处理活动，及时发现异常行为，同时建立审计机制，记录和追溯数据的使用历史，为事后的安全分析提供有力支持。

2 数据应用下的数据安全治理技术整体架构

2.1 人员安全管控

在数据应用的环境中，人员安全管控是确保整个数据处理过程安全性的核心要素之一。有效的身份验证机制是关键，通过采用多层次身份验证，加强密码、双因素认证等，确保只有授权人员能够访问敏感数据，严格的权限管理是另一个关键，通过细粒度的访问控制，确保每位员工只能访问其工作职责所需的数据，减小误操作和滥用的可能性。通过定期的培训，提高员工对数据安全的认识，使其能够正确处理敏感信息、遵循安全规范，并及时报告异常行为，建立安全文化，使每位员工都成为数据安全的守护者。此外离职员工的安全退出是人员安全管控不可忽视的一环，确保在员工离职时，及时收回其访问权限，防止敏感数据被滥用或泄露，审计和监控员工的活动，及时发现异常行为，采取必要的应对措施。

2.2 数据全生命周期安全治理

数据全生命周期安全治理着眼于数据从采集到最终销毁的整个过程，确保数据在每一个阶段都得到充分的安全保护。通过对数据进行明确地分类，可以为后续的安全措施提供有针对性的依据，确保对不同敏感级别的数据采取适当的安全策略。在数据采集阶段，包括对数据传输通道的加密，确保数据在传输过程中不被窃取或篡改，同时建立合规的数据采集规范，明确采集目的，最小化采集范围，降低潜在风险[1]。数据存储阶段要求采用安全的存储措施，包括对数据进行加密保护，实施细粒度的访问控制，确保只有授权人员能够访问敏感数据，定期的数据备份与恢复计划是防范数据灾难的有效手段，保障数据的可靠性和持续可用性。数据使用阶段通过强化用户身份验证，以及建立详细的访问控制策略，确保只有授权用户能够进行数据操作，在数据分享与传输中，采用加密和安全协议，保障数据在共享过程中的保密性和完整性。最终数据销毁阶段是整个治理过程的结束，但同样至关重要，建立安全的数据销毁策略，确保不再需要的数据能够被安全地清理，防止敏感信息的滞留。

2.3 系统安全防护

系统安全防护是数据应用中的关键环节，保障数据存储和处理系统的完整性和可用性。网络安全通过建立坚固的防火墙和入侵检测系统，及时发现和阻止潜在的网络攻击，采用虚拟专用网络（VPN）等安全通信协议，确保数据在传输过程中的安全性。终端安全是系统防护的另一层面，通过强化用户终端的安全性，包括定期的终端安全更新、反病毒软件的使用和强密码政策，减少恶意软件和未经授权的访问。应用程序安全也是系统安全的核心，采用安全编码实践，防范常见的应用层攻击，确保应用程序不容易受到注入、跨站脚本等漏洞的攻击。及时更新和修补系统和应用程序，弥补已知漏洞。身份验证与访问控制是系统安全的最后一道防线，通过建立细粒度的身份验证机制，确保只有授权人员能够访问系统，采用最小权限原则，即给予用户最小必需的权限，降低系统被滥用的概率。

2.4 事件分析与处理

事件分析与处理是数据安全治理中的关键环节，迅速识别、应对和修复潜在的安全威胁。建立实时监控系统记录关键数据操作和系统活动，通过监测异常行为和不寻常的数据访问，能够迅速发现潜在的安全风险。一旦发现异常事件，建立明确的安全事件响应计划是至关重要的，计划应包括紧急联系人、响应步骤和协同团队，对不同类型的安全事件，制定相应的处置流程，确保团队能够有序、迅速地应对。实施事件响应时，追求及时的分析和决策，通过使用安全信息与事件管理（SIEM）工具，对事件进行实时分析，确定是否涉及真实威胁，及时的决策和行动有助于最小化潜在损失。在事件处理的过程中，确保团队成员之间的有效沟通，协同应对不同层面的威胁，同时根据事件的性质，可以采取适当的法律和合规措施，确保整个处理过程合规可追溯。对事件进行事后分析，找出处理中的不足和改进的空间，以不断完善安全事件响应计划，提高团队的应对能力。

3 数据安全治理技术分类

3.1 完整监管安全技术

完整监管安全技术旨在建立全方位的数据监控体系，确保对数据的细致入微地观察和记录。通过使用审计工具和技术，记录数据的访问、修改和共享情况，追踪数据流向，实现对数据操作的全程监管。行为分析与监控是通过分析用户和系统的行为模式，及时发现异常活动，基于行为分析的监控系统能够识别不寻常的数据访问、大规模的文件传输和其他可能的风险行为，提高对潜在威胁的感知。数据的全程监管需要结合安全信息与事件管理（SIEM）系统，通过集成各类日志和事件信息，形成全面的数据安全画像，SIEM 系统能够实时分析和识别潜在威胁，提供及时的警报和通知，以便安全团队迅速做出反应。细粒度的访问控制是完整监管安全技术中的另一要点，通过建立细致的权限策略，确保每位用户只能访问其职责范围内的数据，从而减少滥用和误操作的可能性，包括对数据的读、写、修改等各项权限的详细控制。

3.2 数据使用安全技术

数据使用安全技术侧重于确保在数据处理和分析过程中的安全性。强化用户身份验证，采用双因素认证等手段，确保只有授权人员能够访问敏感数据，细粒度的访问控制进一步限制用户对数据的操作权限，确保数据仅被授权人员使用。对于敏感信息，采用脱敏技术，将数据中的关键信息进行处理，以降低隐私泄露的风险，匿名化则通过删除或替换个人身份信息，保护用户的隐私[2]。对于传输中的数据，采用加密协议确保数据在传输过程中不被窃取或篡改，在数据存储和处理环节，采用数据加密技术，提高数据的安全性。建立实时监控系统，记录数据访问和处理的活动，及时发现异常操作，审计系统能够提供对数据使用历史的详细追溯，为事后的安全分析提供有力支持。

3.3 数据存储与销毁安全技术

数据存储与销毁安全技术着眼于对数据的存储阶段进行全面安全管控。首先通过对存储的数据进行加密，确保即便存储介质被非法获取，数据也能保持机密性，细粒度的访问控制策略进一步限制对存储数据的访问权限，保障数据的安全性。通过定期备份关键数据，以应对意外数据丢失或损坏的情况，备份数据需要存储在安全可靠的位置，并经过加密保护，以确保备份数据本身不成为潜在的安全漏洞。在数据销毁方面通过彻底清除不再需要的数据，确保敏感信息不被滞留，采用数据销毁工具和方法，包括物理销毁和逻辑销毁，以防止数据被恢复或恢复至不安全

状态。数据生命周期管理是整个存储过程的管理基础，通过清晰的数据分类与标记，对不同敏感级别的数据采取相应的安全措施，合规性的数据存储管理，确保数据存储符合法规和行业标准。

4 大数据中数据安全及时的应用

4.1 隐私保护策略

隐私保护策略确保在数据应用中处理个人敏感信息时，充分尊重和保护用户隐私。首先通过脱敏技术，将个人身份信息等关键数据进行处理，以减少隐私泄露的风险，脱敏的方法包括部分脱敏、匿名化和泛化，以便在数据分析中仍能保持有效性。建立细粒度的访问权限，确保只有经过授权的人员能够访问包含敏感信息的数据，采用最小权限原则，即给予用户最小必需的权限，以降低敏感数据被滥用的风险。对于在传输和存储中的敏感信息，采用强加密算法，确保数据在传输和存储过程中得到充分的保护，同时采用端到端加密，确保即便数据在处理过程中也不易被窃取。确保隐私保护策略符合相关法规和法律要求，包括但不限于《个人信息保护法》等隐私保护相关法规，及时更新隐私政策，明确数据使用目的和范围，获得用户的明示同意。

4.2 数据采集与存储的安全实践

在数据应用中，数据采集与存储的安全实践是确保数据初始获取和长期保存过程中的安全性的关键环节。对于在传输过程中的数据，采用安全的加密协议，以保障数据在传输过程中不被窃取或篡改，在数据存储阶段，对敏感信息采用数据加密技术，确保数据在存储介质上的安全性[3]。建立强化的身份验证机制，确保只有授权人员能够进行数据采集和存储的相关操作，采用多因素身份验证，提高身份验证的安全性。通过定期备份数据，保障数据的可恢复性，备份数据需要存储在安全可靠的位置，并经过加密保护，以防备份数据本身成为潜在的安全漏洞。仅收集和保存必要的数据，避免采集过多的冗余信息，以降低数据泄露的风险，同时采用匿名化和脱敏技术，保护用户的隐私。

4.3 数据分析中的安全措施

数据分析中的安全措施至关重要，旨在确保对数据进行深入分析时的安全性和隐私保护。建立细粒度的访问权限，确保只有经过授权的分析人员可以访问敏感数据，采用单一登录、强化的身份验证等技术，防止未授权人员的访问[4]。对于在分析过程中的敏感信息，采用强加密算法，确保数据在处理和传输过程中得到充分的保护，此外采用端到端加密技术，保障在分析环境中的数据隐私。建立实时监控系统，记录数据分析的操作活动，以便追踪和审计每一步的数据处理，监控系统能够及时发现异常行为，提供实时的安全警报，增强对潜在威胁的感知。脱敏和匿名化技术有助于在数据分析中平衡数据的有效性和隐私保护，通过对敏感信息进行脱敏处理，降低隐私泄露的风险，匿名化则通过删除或替换个人身份信息，保护用户的隐私。确保分析过程符合相关法规和法律要求，及时更新隐私政策，明确数据使用目的和范围，获得用户的明示同意。

4.4 安全发布数据的方法

安全发布数据是确保数据在向外部共享时仍能保持机密性和完整性的关键步骤。通过脱敏技术将敏感信息进行处理，减少数据的隐私泄露风险，脱敏的方法包括部分脱敏、匿名化和泛化，以便在共享数据中仍能保持有效性。对于在传输和存储中的共享数据，采用强加密算法，确保数据在传输和存储过程中得到充分的保护。采用端到端加密，防止数据在共享过程中被未经授权地访问。建立明确的访问权限策略，确保只有授权用户能够访问共享的数据，采用细粒度的访问控制，根据用户角色和需求限制其对数据的操作权限。对数据进行数字签名，接收方可以验证数据的来源和完整性，确保数据在传输过程中未被篡改，这为共享数据提供了可靠的验证机制。确保共享数据的发布符合相关法规和法律要求，明确数据使用目的和范围，获得用户的明示同意。

5 结语

数据安全治理是数据应用中的关键环节，通过细粒度的访问控制、加密技术、备份与监控、脱敏与匿名化等手段，确保数据机密性和完整性，同时尊重用户隐私。随着技术和威胁的不断演变，持续更新策略、遵循法规、引入先进技术是保障数据安全的不二之选。全面的数据安全治理不仅促进科技创新，更是保障用户和组织权益的重要保证。

[参考文献]

[1]张万里.大数据应用中数据安全治理技术研究[J].信息系统工程,2023(11):125-128.
[2]田五星.提升数据安全治理效能[J].中国报业,2023(17):5.
[3]丑则静.大数据时代下数据安全问题与治理体系优化[J].新安全,2023(9):63-67.
[4]张楠.数据安全治理体系及关键技术研究[J].软件和集成电路,2023(8):28.

作者简介：赵光灿（1981.10—），男，中级职称，工作专业：大数据安全，大学专业计算机科学与技术，学历：大学本科。