大数据时代的政务数据共享安全研究

刘润华
商水县行政审批和政务信息管理局　河南　周口　466000

摘　要：大数据时代，政务数据共享成为提升政府治理效能的关键路径，但数据安全风险严重制约其发展。研究发现，数据泄露、完整性破坏及访问控制失效等问题频发。通过深入剖析安全威胁根源，针对性提出强化加密防护、构建完整性验证机制、完善访问控制体系与实施安全监测预警等策略，为保障政务数据共享安全、推动数字政府建设提供理论支撑与实践指导，助力实现数据价值释放与安全保护的动态平衡。

关键词：大数据时代；政务数据共享；安全

引言

在数字技术迅猛发展的当下，政务数据共享已成为优化政府服务、提升决策科学性的核心驱动力。然而，海量数据在跨部门、跨层级流动过程中，面临着前所未有的安全挑战。数据泄露可能导致公民隐私暴露、国家机密泄露，完整性破坏会干扰决策准确性，访问控制失效则为非法入侵提供可乘之机。本文聚焦政务数据共享安全问题，系统分析风险成因，探索有效保障策略，旨在为筑牢政务数据安全防线、推动数字政务高质量发展提供有益参考。

1 大数据时代的政务数据共享概述

大数据时代，数据成为关键生产要素，政务数据共享作为数字化进程中的重要一环，深刻影响着社会治理效能与公共服务质量。海量政务数据涵盖经济、民生、交通等多领域信息，其价值挖掘与有效共享是实现社会高效协同发展的核心路径。政务数据共享基于先进的信息技术架构，通过构建统一的数据资源池与标准化接口，打破各部门、各系统间的数据壁垒。分布式存储、云计算等技术的应用，为数据的集中管理与灵活调用提供支撑，使分散在不同业务系统中的数据能够汇聚整合，形成具有完整性与关联性的数据集。这种共享模式，改变了以往数据孤立、重复采集的局面，提升数据获取效率与准确性，避免资源浪费。在实际应用场景中，政务数据共享为智慧城市建设、精准社会服务等提供强大的数据驱动力。以智慧交通为例，通过整合交通流量、道路监控、车辆行驶轨迹等数据，运用大数据分析模型，能够实时优化交通信号灯配时、预测拥堵路段，提升城市交通通行效率。在公共卫生领域，共享的医疗健康数据可助力疾病监测与预警，通过对人口健康信息、医疗就诊记录等数据分析，及时发现疾病传播趋势，为疫情防控、疾病预防等提供科学依据。从技术发展角度看，政务数据共享持续向智能化、安全化方向演进。人工智能技术的融入，可实现数据的自动分类、清洗与关联分析，降低人工处理成本；区块链技术的应用，则为数据共享提供可信的安全保障，确保数据在共享过程中的完整性、可追溯性，有效防范数据泄露与篡改风险，为政务数据共享构建安全稳定的运行环境。

2 大数据时代的政务数据共享面临的安全问题

2.1 数据泄露风险

在大数据时代，政务数据共享过程中数据泄露风险如同悬于头顶的达摩克利斯之剑。随着政务数据规模呈指数级增长，其涵盖内容广泛且复杂，从公民个人身份信息、财产状况到城市基础设施运行数据等，每一项都具有极高的价值，吸引着众多恶意攻击者觊觎。政务数据共享往往涉及多个系统与平台之间的数据交互，这种跨系统的数据传输使得数据在不同的网络环境与存储介质间频繁流动。数据在传输过程中，若采用的加密算法强度不足或存在漏洞，攻击者便可利用网络监听、中间人攻击等手段截取数据。例如，在开放的公共网络环境中，若数据传输未进行有效的加密保护，黑客能够轻易获取传输中的数据包，通过技术手段解析出其中包含的敏感信息。数据存储环节也存在诸多安全隐患。存储设备的物理安全防护若不到位，可能会面临被非法访问的风险；数据库管理系统若存在未及时修复的漏洞，也会成为攻击者入侵的入口，导致数据被窃取。数据共享过程中，由于参与主体众多，数据使用权限管理难度加大。一旦某个参与方的权限管理出现疏忽，内部人员恶意泄露数据或因操作失误导致数据不当流出，都将引发严重的数据泄露事件。随着人工智能与机器学习技术的发展，攻击者可以利用这些先进技术对窃取到的零散数据进行分析整合，挖掘出更有价值的敏感信息，进一步扩大数据泄露带来的危害[1]。

2.2 数据完整性破坏

政务数据的完整性对于数据共享的有效性和准确性至关重要，然而在实际共享过程中，数据完整性面临着诸多威胁。数据在多个系统间流转时，不同系统的数据格式、存储规则和处理方式存在差异，这可能导致数据在转换和传输过程中出现丢失、错误或被篡改的情况。例如，当数据从一种数据库格式转换为另一种格式时，可能会因为数据结构不兼容，使得部分数据无法正确转换，从而造成数据缺失；或者在数据传输过程中，受到网络干扰、信号不稳定等因素影响，导致数据在传输过程中发生错误。恶意攻击者也会采用多种手段破坏数据完整性。他们可能通过注入攻击，向数据处理系统中插入恶意代码或数据，篡改原有数据内容，使得数据失去真实性和可用性。比如在政务数据的统计分析环节，攻击者通过注入虚假数据，改变统计结果，误导决策制定。分布式拒绝服务（DDoS）攻击也可能间接导致数据完整性被破坏。当系统遭受DDoS攻击时，大量的非法请求会使系统资源被耗尽，无法正常处理数据，进而在数据存储、更新等操作过程中引发数据错误或丢失，破坏数据的完整性。数据在共享过程中，由于缺乏有效的数据验证和校验机制，很难及时发现数据完整性被破坏的情况。当错误或被篡改的数据被用于后续的决策支持、业务处理等环节时，将引发一系列连锁反应，导致政务工作出现偏差，甚至造成重大损失。

2.3 访问控制失效

政务数据共享中的访问控制旨在确保只有合法的用户和系统能够访问相应的数据资源，但在实际运行中，访问控制失效问题频发。随着政务数据共享范围的不断扩大，数据访问主体数量大幅增加，访问场景变得复杂多样，这给访问控制带来了巨大挑战。传统的访问控制模型在面对海量的用户和复杂的访问需求时，难以精准地分配和管理访问权限。例如，在一些大型的政务数据共享平台中，用户角色众多，权限划分不够细致，可能会出现部分用户拥有超出其工作需求的过高权限，从而增加了数据被非法访问和滥用的风险。身份认证机制的不完善也是导致访问控制失效的重要因素。如果身份认证过程存在漏洞，攻击者可以通过伪造身份、窃取用户凭证等手段绕过认证机制，以合法用户的身份访问数据资源。比如，利用社会工程学手段获取用户的账号密码，或者通过破解简单的验证码等方式，获取对数据的访问权限。在数据共享过程中，跨系统、跨平台的访问频繁发生，不同系统之间的身份认证和权限管理缺乏有效的协同机制，使得访问控制难以实现统一和有效的管理，进一步加剧了访问控制失效的风险。随着技术的不断发展，新型的攻击手段也对访问控制构成了威胁。例如，攻击者可以利用零日漏洞，在系统尚未发现和修复漏洞之前，突破访问控制的限制，非法访问数据。内部人员滥用权限的情况也时有发生，由于缺乏有效的权限审计和监督机制，内部人员的违规操作行为难以被及时发现和制止，从而导致访问控制失效，造成数据泄露和滥用等安全问题[2]。

3 大数据时代的政务数据共享安全保障策略

3.1 强化数据加密防护

（1）在大数据时代的政务数据共享场景中，数据加密作为核心防护手段，通过复杂的算法将原始数据转换为密文形式，确保数据在存储与传输过程中即使被非法截获，攻击者也难以解读其真实内容。采用先进的对称加密与非对称加密相结合的混合加密模式，利用对称加密在数据处理速度上的优势，对大量政务数据进行快速加密，同时运用非对称加密安全分发对称加密密钥，保障密钥传输的安全性。（2）对于不同敏感度级别的政务数据，实施差异化的加密策略。对涉及公民隐私、商业秘密等高敏感数据，采用高强度的AES-256、RSA-4096等加密算法，确保数据具备极高的破解难度；对于一般性的政务公开数据，可选用相对轻量级的加密算法，在保障数据安全的同时，降低加密解密过程对系统性能的影响。（3）持续关注密码学领域的技术发展，定期更新加密算法与密钥管理机制。随着计算能力的提升和新型攻击手段的出现，旧的加密算法可能面临被破解的风险，通过及时更新算法与密钥，能够有效抵御潜在的安全威胁，维持数据加密防护体系的有效性和安全性，为政务数据共享筑牢加密防线。

3.2 构建数据完整性验证机制

（1）为确保政务数据在共享过程中不被篡改、伪造或损坏，构建可靠的数据完整性验证机制至关重要。哈希函数在其中发挥着关键作用，通过对原始数据计算生成唯一的哈希值，该哈希值具备数据唯一标识特性，可唯一表征数据状态，任何对数据的细微修改都会导致哈希值发生显著变化。在数据存储时记录哈希值，数据传输前后分别计算并比对哈希值，可快速判断数据是否完整。（2）引入区块链技术，利用其分布式账本和共识机制，为政务数据完整性验证提供更高的可靠性和公信力。将数据的关键信息及哈希值记录在区块链上，多个节点共同维护和验证数据记录，一旦数据被篡改，区块链网络中的节点将无法达成共识，从而及时发现数据异常。这种去中心化的验证方式，避免了单一验证中心可

能存在的安全风险和信任危机。（3）针对数据在不同平台和系统间的流转，建立数据完整性验证的全流程追溯体系。从数据的产生源头开始，在数据采集、处理、存储、传输和共享的每一个环节，都进行哈希值计算和记录，形成完整的验证链条。当出现数据完整性争议时，能够通过追溯验证链条，快速定位问题环节，确保数据的真实性和准确性，保障政务数据共享的质量[3]。

3.3 完善访问控制体系

（1）在政务数据共享环境下，完善的访问控制体系是保障数据安全的重要屏障。基于角色的访问控制（RBAC）模型是一种有效的实现方式，根据用户在政务数据处理过程中的不同职责和任务，划分相应的角色，如数据管理员、数据查询员、数据分析师等，为每个角色分配特定的访问权限，确保用户只能访问与其工作相关的数据资源，避免越权访问。（2）结合多因素认证技术，提升访问控制的安全性。除了传统的用户名和密码认证方式外，增加生物特征识别（如指纹、面部识别）、动态令牌等认证因素，通过多种认证方式的组合，降低因密码泄露导致的非法访问风险。只有当用户通过所有认证因素的验证后，才允许其访问相应的数据资源，从而有效保护政务数据的访问安全。（3）实施最小权限原则，严格限制用户的数据访问范围。在分配权限时，仅赋予用户完成特定工作任务所必需的最小权限集合，避免赋予过多不必要的权限。定期对用户权限进行审查和调整，根据用户工作岗位的变动或数据安全需求的变化，及时更新用户权限，确保访问控制体系始终与实际需求相匹配，最大限度减少数据泄露风险。

3.4 实施数据安全监测与预警

（1）建立全面的数据安全监测系统，实时收集和分析政务数据在存储、传输和使用过程中的各类安全相关信息。通过部署网络流量监测工具、主机日志分析系统等，对数据的访问行为、传输路径、异常操作等进行全方位监控。利用机器学习和人工智能技术，对收集到的海量数据进行深度分析，识别其中潜在的安全威胁模式和异常行为。（2）制定科学合理的安全预警规则，基于对历史安全事件和正常数据操作模式的分析，设定各类安全指标的阈值。当监测到的数据访问频率、数据传输量、异常操作次数等指标超过预设阈值时，系统自动触发预警机制，及时向安全管理人员发出警报，并提供详细的异常信息，包括发生时间、涉及数据、操作来源等，以便管理人员快速做出响应。（3）构建数据安全应急响应体系，与安全监测和预警系统紧密结合。一旦接收到预警信息，应急响应团队能够迅速启动应急预案，采取相应的处置措施，如隔离受威胁的数据资源、阻断异常访问行为、进行数据恢复等。对安全事件进行深入调查和分析，总结经验教训，不断优化安全监测与预警机制和应急响应流程，提高政务数据共享的安全防护能力和应对突发事件的能力[4]。

结语

综上所述，大数据时代政务数据共享安全是数字政府建设的重要保障。通过强化数据加密防护、构建完整性验证机制、完善访问控制体系及实施安全监测预警等策略，可有效应对数据泄露、完整性破坏与访问控制失效等风险。但随着技术演进与应用场景拓展，数据安全挑战持续升级。未来需持续深化技术创新与管理模式变革，探索多维度协同防护体系，为政务数据共享营造安全、可靠的生态环境，释放数据要素价值潜能。

参考文献

[1]苏婷.大数据时代的政务数据共享安全研究[J].大科技,2023(20):160-162.

[2]刘爽.大数据时代政务信息安全建设探析[J].电脑高手(电子刊),2021(3):1465.

[3]王娟,杨现民,郑浩,等.大数据时代教育政务数据开放的风险分析及防控策略研究[J].中国电化教育,2020(6):95-103.

[4]魏源锋.电子政务数据信息共享安全风险及应对策略[J].计算机产品与流通,2022(9):170-172.