政务云和数据中心建设中的安全性与隐私保护机制探讨

王旭东　罗有喆
辽宁省大数据管理中心（辽宁省信息中心）

摘　要：政务云和数据中心作为现代政府信息化建设的重要组成部分，扮演着存储、处理和管理政府大量数据的关键角色。随着信息技术的快速发展和社会的数字化进程，政府部门在面对日益增长的数据量和复杂的信息系统时，迫切需要高效安全的存储和处理手段，以提升工作效率、加强服务能力，能够从根本上保障政府数据的安全性和隐私保护。本文旨在探讨政务云和数据中心建设中存在的安全隐患及其解决方案，为政府信息化建设提供参考和指导，推动政府信息化向着安全、高效、可靠的方向发展。

关键词：数据中心；政务云；安全性；隐私保护
【DOI】10.12252/j.issn.2096-627X.2022.11.223

前言

近年来，政府信息化建设已经取得了长足的进步，政务云和数据中心等新一代信息技术平台应运而生。政务云是基于云计算技术的专用云服务平台，旨在为政府部门提供安全、高效、可靠的信息化服务。而数据中心则是集中存储、处理和管理大量数据和信息的设施，为政府提供数据存储、应用部署和运行等关键服务。政务云和数据中心的建设，为政府信息化提供了新的解决方案和技术手段，为政府部门提供了强大的信息化支撑平台。随着政务云和数据中心的广泛应用和深入发展，政务云和数据中心存储着大量敏感数据，如政府文件、个人身份信息等，一旦发生数据泄漏或安全漏洞，往往会导致严重的信息安全和隐私泄漏问题，为了提升政府信息化建设的水平和能力，保障政府数据的安全性和隐私保护，迫切需要深入研究政务云和数据中心建设中的安全性与隐私保护机制

一、政务云与数据中心的功能概述

政务云与数据中心是现代政府信息化建设的重要组成部分，它们在提升政府管理效率、服务水平以及推动数字化转型方面发挥着关键作用。从本质上而言，政务云以及数据中心都是基于大数据技术以及云端储存管理技术相结合的数据化平台，能够实现对复杂的储存与管理数据的清洗与查询建设。

1.政务云

政务云是一种基于云计算技术的专用云服务平台，旨在为政府部门提供安全、高效、可靠的信息化服务。其功能概述如下：1）数据存储与管理：政务云提供可靠的数据存储与管理服务，包括数据备份、归档、检索和版本控制等功能，确保政府数据的安全性和完整性。2）应用部署与运行：政务云支持各种政府应用程序的部署与运行，包括公共服务平台、行政管理系统、电子政务应用等，提高了政府业务的灵活性和响应速度。3）资源共享与协作：政务云提供资源共享和协作环境，政府部门可以共享硬件资源、软件服务和数据，促进政府间的信息交流与合作。4）安全保障与监管：政务云具备严格的安全保障机制，包括身份认证、访问控制、数据加密等，同时配备安全监控和审计功能，确保政府数据和应用的安全。

2.数据中心

数据中心是一个集中存储、处理和管理大量数据和信息的物理或虚拟化设施，其功能概述如下：1）数据处理与分析：数据中心配备高性能的计算设备和数据处理系统，能够对海量数据进行实时分析、挖掘和计算，为政府决策提供数据支持和智能分析服务。2）应用部署与运行：数据中心为政府部门提供应用部署和运行环境，支持各类应用程序的部署、更新和运行，包括管理系统、业务应用、大数据应用等。3）安全保障与监控：数据中心具备严格的安全保障措施，包括物理安全、网络安全、数据加密等，同时配备安全监控系统，确保数据中心的安全稳定运行。4）能源管理与环保：数据中心采用先进的节能技术和绿色环保设施，实现能源的有效利用和环境的友好保护，降低能源消耗和碳排放。

二、政务云和数据中心建设中的安全性问题

1.数据泄漏风险分析

在政务云和数据中心建设中，数据泄漏风险是一个严重的安全性问题，可能影响政府部门的信息安全和隐私保护，数据存储环节存在泄漏风险。政务云和数据中

心作为数据的存储和管理中心，承载着大量的敏感信息，如政府文件、个人身份信息等，并且存储系统存在漏洞或未经充分加密保护，黑客或内部人员可能通过非法手段获取数据，导致数据泄漏风险增加。

首先，政务云和数据中心作为数据的传输通道，数据在传输过程中可能受到黑客攻击、窃听等威胁。其次，政务云和数据中心通常涉及多个部门、多个用户的数据共享与访问，若共享权限设置不当或者缺乏有效的访问控制机制，会导致未授权的用户获取敏感信息，从而造成数据泄漏风险的增加。

2.网络攻击威胁评估

政务云和数据中心建设的过程中，往往会受到网络攻击威胁的影响，政务云以及数据中心的安全性会受到多方面因素的影响，对政府信息系统造成严重影响。首先，网络攻击可能针对政务云和数据中心的网络基础设施展开，例如网络设备、防火墙等，通过网络漏洞或弱点进行入侵，破坏网络的稳定性和可用性。

一方面，应用程序漏洞是网络攻击的另一主要威胁，政务云和数据中心承载着各类政府应用程序，若这些应用程序存在安全漏洞，黑客可利用漏洞进行注入攻击、跨站脚本攻击等，获取敏感信息或控制系统。

3.其他安全隐患分析

在政务云和数据中心建设中，除了数据泄漏和网络攻击等常见的安全问题外，还存在着其他安全隐患，存在的安全隐患往往会对系统的安全性和稳定性构成威胁，政务云以及数据中心相关的硬件设备的安全隐患是一个重要问题。

政务云和数据中心所依赖的硬件设备包括服务器、存储设备、网络设备等，若这些硬件设备存在制造缺陷或后门程序，可能被黑客利用进行恶意攻击或数据窃取，从而影响系统的正常运行。其一，政务云和数据中心的操作人员可能因为疏忽、不当操作或安全意识不足而引发安全事件，例如误删除重要数据、配置错误导致系统漏洞等，这些人为操作失误可能导致系统故障或数据泄漏。其二，供应链安全问题也值得关注。政务云和数据中心的供应链涉及硬件设备、软件服务、第三方服务提供商等多方，若供应链环节存在安全漏洞或恶意植入，在很大程度上会对对系统的整体安全构成威胁。其三，缺乏灵活的安全策略和应急响应机制也是一个安全隐患，并且政务云和数据中心缺乏及时有效的安全策略和应急响应机制，一旦发生安全事件，可能导致应对不及时、不够灵活，进而造成更严重的安全后果。

三、政务云和数据中心建设中的安全性与隐私保护机制的构建方法

1.构建身份认证与访问控制机制

构建身份认证与访问控制机制是确保政务云和数据中心安全性与隐私保护的重要步骤，对于身份认证，可采用多因素认证方式，结合用户账号和密码、生物识别信息、硬件令牌等多种因素进行身份验证，提高身份认证的安全性和可靠性，需要建立完善的用户身份管理系统，包括用户注册、身份验证、权限分配等环节，确保每个用户都具有唯一身份标识，并根据用户角色和权限分配相应的访问权限。

具体而言，在访问控制方面，可以采用基于角色的访问控制（RBAC）或基于策略的访问控制（ABAC）等模型，根据用户所属角色或指定策略控制其对系统资源的访问权限，可以在此基础上建立细粒度的权限管理机制，对不同的资源和功能进行精细化的权限控制，实现权限的最小化原则，即用户只拥有其工作所需的最低权限，以减少安全风险。除此之外，技术人员还需要引入动态访问控制技术，根据用户的行为特征和环境情况动态调整访问权限，及时应对潜在的安全威胁。与此同时，应该建立审计日志系统，记录用户的登录、访问和操作行为，定期审查和分析审计日志，发现异常行为并及时采取相应的安全措施，在此基础上加强对身份认证与访问控制机制的监管和审计，定期对系统进行安全评估和漏洞扫描，及时修复安全漏洞，确保身份认证与访问控制机制的有效性和稳定性。

2.数据加密与传输安全

在政务云和数据中心建设中，数据加密与传输安全是确保信息安全和隐私保护的关键环节，实际应用的过程中应该采用强加密算法对数据进行加密是保障数据安全的关键手段，相应的政务云和数据中心中的敏感数据应采用对称加密或非对称加密等加密算法进行加密处理，确保数据在存储和传输过程中的机密性，技术人员需要按照数据权限以及规划要求对密钥管理进行严格控制，确保密钥的安全性和保密性，避免密钥泄漏导致加密数据被解密。

一方面，政务云和数据中心应采用安全传输协议，如SSL/TLS协议，建立安全的通信通道，对数据在网络

传输过程中进行加密和认证，防止数据被窃听、篡改或劫持，可以采用虚拟专用网络（VPN）等技术手段，建立安全的远程访问通道，实现远程用户对政务云和数据中心的安全访问。另一方面，在数据加密与传输安全的构建过程中，还需加强对加密算法和安全协议的更新和维护，及时修补已知漏洞，确保其安全性和可靠性，在此基础上建立完善的访问控制机制，限制对加密密钥和安全通信协议的访问权限，防止未经授权的操作对系统安全造成威胁。除此之外，还应加强对数据传输过程中的中间人攻击、重放攻击等安全威胁的防范和检测，采用数字签名、消息认证码等技术手段，确保数据传输的完整性和真实性。总而言之，政务云和数据中心建设中的数据加密与传输安全需要采用多层次、多方面的安全措施，包括数据加密、安全传输协议、访问控制、漏洞修补和安全检测等，以确保政务云和数据中心中的数据在存储和传输过程中的安全性和隐私保护。

3.建立安全审计与监控机制

安全审计与监控机制是确保政务云和数据中心安全性与隐私保护的关键步骤，单位需要建立全面的安全审计系统，通过记录和分析系统的操作日志、安全事件和异常情况，及时识别和响应潜在的安全威胁，并且安全审计系统应覆盖系统的各个关键环节，包括用户登录、数据访问、系统配置变更等，确保对系统和数据的所有操作都能够进行全面监控和审计。

其一，建立实时的安全监控系统，对政务云和数据中心的网络流量、系统性能、安全配置等进行实时监测和分析，及时发现并应对网络攻击、恶意软件、异常访问等安全事件。除此之外，安全监控系统应具备自动化报警和应急响应能力，一旦发现异常情况，能够及时发出警报并采取相应的安全措施，防止安全事件进一步扩大和造成损失。其二，在建立安全审计与监控机制的过程中，需要针对不同的安全事件和威胁制定相应的监控指标和警报规则，确保能够全面覆盖可能的安全风险。同时，建立专门的安全运维团队，负责对安全审计和监控系统进行管理和维护，及时更新安全规则和策略，提高安全事件的检测和响应效率。其三，加强对安全审计与监控数据的分析和利用，通过对安全事件的趋势分析和统计，发现安全威胁的潜在规律和漏洞，及时调整安全策略和加强安全防护，提高系统的整体安全性和抗攻击能力。

总而言之，建立安全审计与监控机制是确保政务云和数据中心安全性与隐私保护的重要手段，通过建立全面的安全审计系统和实时的安全监控系统，及时发现和应对安全威胁，提高系统的安全防护能力和应急响应水平，确保政务云和数据中心的安全稳定运行。

结语

综上所述，随着数字化政务转型与发展效率的不断提高，政务云和数据中心不断普及，政务云与数据中心的应用日趋广泛。由于政务云以及数据中心均基于互联网框架构建，基于互联网框架下的系统化应用，安全性与隐私保护机制的构建尤为关键，通过对身份认证与访问控制、数据加密与传输安全以及安全审计与监控机制等关键方面进行分析。建立严格的身份认证与访问控制机制是确保政务云和数据中心安全性的基础，需要采用多因素认证、细粒度权限控制等技术手段，有效限制用户对系统资源的访问权限，防止未经授权的访问和恶意操作。此外，加强数据加密与传输安全是保障政务云和数据中心信息安全的关键措施，运用强加密算法和安全传输协议，对数据进行加密和认证，保障数据在存储和传输过程中的机密性和完整性，通过记录和分析系统操作日志、实时监测网络流量和安全事件，及时发现并应对潜在的安全威胁，提高系统的安全防护能力和应急响应水平，确保政务云和数据中心安全性与隐私保护的关键措施，综合运用上述安全机制，可以有效保障政务云和数据中心的安全稳定运行，提升政府信息化建设的水平和能力。

参考文献

[1]汪涛.云政务数据中心建设浅析[J].科技创新与应用，2016.

[2]汪涛.云政务数据中心建设浅析——以南京为例[J].科技创新与应用，2016（29）：1.

[3]关迎宾.关于电子政务云数据中心安全方案的讨论[C]//辽宁省通信学会通信网络与信息技术年会.辽宁省通信学会，2016.

[4]陈方亮.电子政务云计算数据中心网络组网研究[J].华东科技：综合，2019（12）：2.

[5]赵晟杰，罗海涛，覃琳.云计算网络安全现状与思考[J].大众科技，2014（12）：1-4.