政务数据共享平台的安全通信机制与隐私保护技术研究

陈宗胜[1]　易　达[2]
1. 数字广西集团有限公司　广西　南宁　530000
2. 广西数广全网融合科技有限公司　广西　南宁　530000

摘　要：随着数字政府建设的深入推进，政务数据共享已成为提升政府治理能力、优化公共服务和推动社会经济发展的重要支撑。然而，政务数据往往包含大量敏感个人信息、公共安全信息，其在跨部门、跨层级、跨区域共享过程中面临严峻的安全风险与隐私泄露隐患。本文聚焦于政务数据共享平台的安全通信机制与隐私保护技术，系统分析当前平台架构中存在的安全挑战，深入探讨基于零信任架构、国密算法、安全多方计算、差分隐私、联邦学习等前沿技术的综合防护体系，并提出一种融合多层次安全通信协议与动态隐私保护策略的新型平台架构。研究表明，通过构建“端-网-云”一体化的安全通信通道，结合细粒度访问控制与数据脱敏机制，可有效保障政务数据在传输、存储与使用全生命周期中的安全性与隐私性，为构建可信、高效、合规的政务数据共享生态提供理论支撑与实践路径。

关键词：政务数据共享；安全通信；隐私保护；零信任架构；国密算法；安全多方计算；差分隐私；联邦学习

引言

近年来，我国大力推进“数字政府”和“人工智能”建设，《“十四五”数字经济发展规划》《关于加强数字政府建设的指导意见》等政策文件明确要求打破“数据孤岛”，推动政务数据资源有序共享与开放利用。政务数据共享平台作为实现这一目标的核心基础设施，承担着汇聚、整合、交换与服务各类政务数据的关键职能。然而，政务数据具有高敏感性、高价值性和强关联性等特点，在共享过程中极易成为网络攻击、内部滥用或非法交易的目标。因此，如何在保障数据高效流通的同时，确保其安全性与个人隐私权益，已成为亟待解决的重大课题。本文旨在系统研究政务数据共享平台的安全通信机制与隐私保护技术，从理论基础、技术路径与架构设计三个维度展开，提出一套兼顾安全性、可用性与合规性的综合解决方案，以期为相关领域的研究与实践提供参考。

1 政务数据共享平台的安全挑战分析

1.1 数据共享场景复杂化

现代政务数据共享已从传统的“点对点”模式演变为“多源异构、跨域协同”的复杂网络。参与主体包括各级政府部门、公共服务机构、第三方合作企业等，数据流向呈现多向性、动态性特征。这种复杂性使得传统的边界防御模型（如防火墙、DMZ）难以有效应对内部威胁与横向移动攻击。

1.2 通信链路安全风险

政务数据在传输过程中需经过多个网络节点，包括政务外网、互联网等，存在被窃听、篡改、重放或中间人攻击的风险。尤其在跨区域共享场景中，数据常需穿越非受控网络环境，传统TLS/SSL协议若配置不当或使用弱加密算法，将导致通信内容暴露。

1.3 隐私泄露与滥用风险

共享数据中常包含身份证号、住址、健康状况、社保记录等敏感个人信息。即使经过匿名化处理，攻击者仍可通过关联分析、背景知识推断等方式实现“去匿名化”。此外，数据接收方可能超出授权范围使用数据，或将其二次转售，造成隐私侵犯。

1.4 合规性压力加剧

《中华人民共和国数据安全法》《个人信息保护法》《网络安全法》以及《信息安全技术 个人信息安全规范》（GB/T 35273）等法律法规对政务数据的处理提出了严格要求，包括最小必要原则、目的限定、用户同意、数据本地化等。平台若无法满足合规要求，将面临法律追责与声誉损失。

2 安全通信机制设计

2.1 基于零信任架构的通信模型

面对传统边界防御模型的局限性，零信任架构为政务数据共享平台提供了全新的安全范式。该模型摒弃了“专网即安全”的假设，转而坚持“永不信任，始终验证”的核心理念。在具体实施中，平台首先需建立统一的身份认证中心，集成数字证书、生物特征识别与多因素认证等多种手段，确保每个访问请求的发起者身份真实可信。其次，通过软件定义边界（SDP）或微分段技术，将庞大的政务网络划分为多个逻辑隔离的安全域，仅允许经过严格授权的通信流在最小必要路径上传输，

从而有效遏制攻击横向扩散[1]。更重要的是，访问控制决策不再仅依赖静态角色，而是引入属性基访问控制（ABAC），综合考量用户身份、设备安全状态、访问时间、地理位置及数据敏感级别等上下文信息，实现动态、细粒度的权限判定。这种持续验证与最小权限授予机制，显著提升了平台对内部威胁与高级持续性攻击的抵御能力。

2.2 国产密码算法的应用

为响应国家关于关键信息基础设施必须采用自主可控商用密码的要求，政务数据共享平台应全面部署SM系列国密算法。在数据传输环节，可采用SM4对称加密算法对明文数据进行高效加解密，其128位密钥长度与AES相当，但算法设计完全自主，避免了潜在的后门风险。密钥的安全分发则由SM2非对称加密算法保障，通过椭圆曲线公钥体制实现密钥协商或封装，确保即使通信链路被监听，攻击者也无法获取会话密钥。同时，为保证数据完整性与来源真实性，所有关键数据包均需使用SM2私钥生成数字签名，并配合SM3哈希算法计算消息摘要[2]。接收方通过验证签名与摘要的一致性，即可确认数据未被篡改且确实来自合法发送方。在网络传输层，平台应部署支持GM/T 0024-2014标准的国密SSL网关，替代传统的国际标准TLS，构建从终端到服务端的全链路国密加密通道，从根本上满足国家密码合规要求。

2.3 安全通信协议栈优化

为实现端到端的安全保障，政务数据共享平台需构建覆盖“终端—网络—云端”的一体化安全通信协议栈。在终端侧，轻量级安全代理软件应嵌入各类数据采集与访问设备，负责本地数据的预加密、身份绑定及安全日志记录，防止数据在源头泄露。在网络传输层，可依托现有政务专网基础设施，叠加IPSec over MPLS或SRv6+IPSec等隧道技术，形成高强度的加密传输管道，有效隔离公网风险。在应用交互层面，所有服务间通信（尤其是API调用）必须强制实施双向mTLS（mutual TLS）认证，即客户端与服务器端均需验证对方证书的有效性，杜绝伪造服务或中间人冒充。此外，API网关作为流量入口，还需集成速率限制、异常行为检测与请求内容深度解析功能，对可疑调用进行实时拦截，从而在协议栈的每一层都构筑起纵深防御屏障。

3 隐私保护关键技术

3.1 安全多方计算

安全多方计算为解决“数据可用不可见”这一核心矛盾提供了理论可行的路径。其基本思想是允许多个互不信任的参与方在不透露各自私有输入的前提下，共同计算一个约定函数的结果。在政务场景中，这一技术尤其适用于跨部门联合统计分析任务。例如，税务部门掌握居民收入信息，医保部门掌握医疗支出记录，双方可通过SMPC协议协同计算收入与医疗支出的相关性系数，而彼此无法获知对方的具体数据条目。尽管当前SMPC方案在计算效率上仍面临挑战，特别是对于大规模数据集，但随着基于混淆电路或秘密共享的优化算法不断涌现，以及GPU、FPGA等硬件加速技术的引入，其实用性正在稳步提升。未来，SMPC有望成为政务数据融合分析的标准工具，既释放数据价值，又严守隐私底线。

3.2 差分隐私

差分隐私通过在查询结果中注入精心校准的随机噪声，为个体隐私提供严格的数学保障。其核心优势在于，无论攻击者是否掌握除目标个体外的所有背景知识，都无法通过观察输出结果显著提高其对目标个体是否在数据集中存在的判断置信度。在政务数据开放发布场景中，差分隐私可广泛应用于统计报表的生成。例如，当发布某区域的平均月收入或某种疾病的发病率时，系统可自动根据预设的隐私预算（ε值）添加拉普拉斯或高斯噪声。较小的ε值意味着更强的隐私保护，但会带来更大的统计误差；反之，较大的ε值则保留更高数据效用，但隐私风险上升[3]。实践中，需根据具体应用场景在二者间寻求平衡。研究表明，当ε设定在0.5至2之间时，多数宏观统计指标的误差可控制在业务可接受范围内，同时有效抵御差分攻击。

3.3 联邦学习

联邦学习作为一种分布式机器学习范式，允许各参与方在本地保留原始数据的前提下，仅交换模型参数（如梯度）以协同训练全局模型。这一特性使其天然契合政务领域对数据主权与隐私保护的双重需求。例如，在跨城市交通流量预测任务中，各市交通管理部门可在本地利用自身历史数据训练神经网络模型，定期将加密后的梯度上传至中央聚合服务器，服务器汇总后更新全局模型并下发，如此迭代直至收敛。为防止中央服务器或恶意参与方从梯度中反推原始数据，可进一步结合同态加密技术，使梯度在加密状态下完成聚合运算。联邦学习不仅避免了大规模原始数据的集中存储风险，还降低了跨域数据传输带宽压力，是构建隐私优先型智能政务应用的理想选择。

3.4 数据脱敏与匿名化增强

尽管高级隐私计算技术前景广阔，但在大量常规数据共享场景中，高效的数据脱敏与匿名化仍是不可或缺的基础手段。传统的掩码、泛化等方法虽简单易行，但

难以抵御复杂的关联攻击。因此，平台应引入k-匿名、l-多样性、t-接近性等更严格的匿名化模型。k-匿名要求每条记录在准标识符（如年龄、邮编、职业）组合上至少与k-1条其他记录不可区分；l-多样性则进一步确保这些等价类中敏感属性具有足够多样性；t-接近性关注敏感属性值的分布相似性。此外，脱敏策略应具备上下文感知能力，对身份证号、银行卡号等超高敏感字段实施不可逆哈希加盐处理，彻底消除还原可能；而对性别、年龄段等低敏感字段，则可保留部分语义信息以维持后续分析的价值[4]。动态脱敏引擎应能根据访问者的权限级别实时调整数据呈现形式，实现“按需披露”。

4 综合安全架构设计

4.1 架构组成

为系统性应对前述挑战，本文提出一种“三层四维”政务数据共享平台安全架构。该架构以基础安全层为根基，集成国密算法库、硬件安全模块（HSM）用于密钥安全存储、以及基于Intel SGX或ARM TrustZone的可信执行环境（TEE），为上层应用提供硬件级安全保障。通信安全层则由零信任网关、国密SSL代理、API安全网关等组件构成，负责实现身份认证、加密传输与流量管控。数据安全层是隐私保护的核心，包含隐私计算引擎（支持SMPC、FL、DP等多种模式）、智能脱敏系统、以及基于数字水印与区块链的数据溯源模块，确保数据在使用过程中可追踪、可审计、不可抵赖。

4.2 核心机制

在该架构下，动态权限管理机制融合了基于角色的访问控制（RBAC）与基于属性的访问控制（ABAC），既能满足组织架构的常规授权需求，又能根据实时上下文进行精细化策略调整。所有权限变更操作均通过区块链进行存证，确保操作日志不可篡改，为事后审计提供坚实依据。同时，平台内置自动化隐私影响评估（PIA）模块，在每次数据共享请求发起时，自动分析数据敏感度、接收方资质、使用场景等因素，量化隐私风险等级，并智能推荐相应的脱敏或加密策略。此外，安全监控与响应体系利用AI驱动的安全信息与事件管理（SIEM）系统，对海量访问日志进行实时分析，一旦检测到异常模式（如高频访问、非常规时段操作、越权尝试），立即触发告警、自动阻断连接，并启动应急响应流程。

4.3 全生命周期保护

安全与隐私保护必须贯穿政务数据的整个生命周期。在数据采集阶段，严格遵循最小必要原则，明确限定数据收集范围、用途及留存期限，并获取必要的用户授权。传输阶段强制实施端到端加密与完整性校验，杜绝窃听与篡改。存储阶段采用加密存储技术，辅以严格的访问控制列表与定期漏洞扫描。使用阶段则将数据分析任务限制在受控的沙箱环境中执行，禁止原始数据下载或导出。最后，在数据达到留存期限或完成使命后，平台依据预设策略自动执行安全擦除，并生成带有数字签名的销毁证明，确保数据彻底不可恢复，形成闭环管理。

5 结语

政务数据共享是数字政府建设的核心环节，其安全与隐私保障关乎国家安全与公民权益。本文系统分析了当前平台面临的安全挑战，提出融合零信任架构、国密算法、安全多方计算、差分隐私与联邦学习的综合防护体系，并通过架构设计与实证案例验证了其有效性。研究表明，只有将安全通信机制与隐私保护技术深度嵌入数据共享全生命周期，才能实现“数据高效流通”与“安全隐私可控”的双重目标。未来需进一步加强技术标准化、制度协同与人才培养，共同构建可信、韧性、合规的政务数据共享新生态。

参考文献

[1]李鑫,史伟进.政务数据共享交换平台安全问题探究[J].网络安全技术与应用,2025,(06):72-74.

[2]陈静,白洁.面向全国一体化政务服务平台的科技政务数据资源安全共享体系研究[C]//中国计算机学会.第38次全国计算机安全学术交流会论文集.科学技术部信息中心;,2023:90-93.

[3]沈博,杨军,王福喜,等.政务云环境下的数据共享隐私保护增强方案[J].沈阳师范大学学报(自然科学版),2025,43(01):28-36.

[4]白航.面向政务大数据开放共享的隐私保护方法研究与实现[D].西安电子科技大学,2023.13(02):22-28.