基于数据安全网关的信息化网络安全系统设计

张　洋[1]　张贵春[2]
1. 天津市数据发展中心　天津　300221
2. 天津市水文水资源管理中心　天津　300211

摘　要：本文围绕国产化智能数据安全网关，开展信息化网络安全系统设计与方案构建。先介绍新一代数据安全网关的技术内涵，包括智能拓展功能、核心技术支撑，对比其与传统设备的技术差异。结合信息化网络多场景业务特点，梳理新型安全风险与威胁，明确系统在政务国产化合规方面的功能与非功能指标。搭建“云管端”立体架构，设计国密全栈加密、自适应访问控制等核心模块，优化国产化数据库适配与接口设计。该系统采用分层架构、多模块协同，实现全方位、多层次安全防护，兼顾国产化合规与全流程数据管控，保障信息化网络稳定与数据安全。

关键词：数据安全网关；网络安全系统；加密传输；访问控制

引言：信息技术快速发展，全面融入政务协同、民生服务等社会治理领域，网络成为信息交互、业务处理与数据流通的核心。然而，网络安全问题频发，新型攻击手段不断出现，给政企单位带来信息泄露与财产损失风险。传统网络安全防护手段存在技术滞后、智能防护能力弱、国产化适配不足等问题，难以满足复杂网络环境需求。新一代国产化智能数据安全网关融合多种前沿技术，具有高适配性、多维度防护、动态智能管控等优势，是保障网络安全、推进政务系统国产化的关键载体，开展相关设计研究意义重大。

1 数据安全网关技术基础

1.1 数据安全网关的定义与功能

新一代国产化智能数据安全网关，以国产芯片、操作系统为基础，国密全栈算法为加密核心，部署于不同安全域网络边界。它是集多维防护、数据跨域管控、智能风险识别于一体的智能防护设备，是内外网安全屏障及政务数据跨域合规流通的核心枢纽，能适配政务信息系统国产化替代要求。相较传统网关，其核心功能实现智能化、多元化升级，契合“云管端”立体防护理念：依托国产化技术构建原生数据安全资源池，实现多租户环境下数据资产隔离与精细管理；智能过滤和实时监控进出数据，采用动态混淆算法变更数据包特征，规避特征化攻击；构建国密全栈协同防护机制，对数据进行加密；实施自适应访问控制，结合多维度信息进行动态授权；融入AI深度学习技术深度审计网络流量，记录全维度信息，实现安全事件可追溯核查，全方位保障政务数据安全[1]。

1.2 关键技术分析

1.2.1 加密技术

加密技术是数据安全网关实现数据安全防护的核心技术，目前已形成适配政务场景的国密全栈协同防护体系，全面替代国际算法，可无缝对接国产密码芯片与操作系统，实现算法与软硬件的深度融合。在政务数据共享场景中，它通过加密变换将明文转换为密文，仅授权主体可通过合法密钥完成解密，核心采用全系列国密算法，构建从数据传输到存储的全链路加密机制。其中，SM4算法凭借加密解密效率高、处理速度快的特点，用于政务数据批量传输场景，如跨部门人口信息、政务审批数据的批量同步；SM2算法以高安全性、高抗攻击性特征，用于密钥交换和数字签名验证，如政务公文流转中的身份确权与防篡改；SM3算法则专注于数据完整性校验，通过生成唯一哈希值精准识别数据篡改、伪造行为，筑牢文件传输的完整性防护防线。

1.2.2 身份认证

身份认证技术的核心是验证访问主体身份的真实性与合法性，目前已升级为多模态智能协同认证模式，适配政务高安全等级需求。数据安全网关整合多种认证技术形成协同体系，针对不同政务场景实现多维全方位核验：国产化数字证书认证基于国密体制构建，由国产CA机构签发，用于政务系统登录、涉密业务操作，从根源上保障证书的安全合法；多模态生物特征认证融合指纹、人脸等特征，结合AI活体检测技术，应用于政务服务大厅办件、线上审批的身份核验，防范身份伪造与冒用；终端可信认证模块与国产终端安全管理系统对接，对政务办公终端的国产化适配性、安全状态进行校验，杜绝非合规终端接入政务内网；动态令牌+扫码认证适配远程办公、移动政务访问场景，实现人员居家办公、外出执法时的安全便捷认证。

1.2.3 访问控制

访问控制技术通过制定规范化的权限管理策略，限制访问主体对网络资源与数据资产的访问范围，目前已升级为动态自适应精细化管控模式，适配政务数据分级分类管理要求。数据安全网关基于政务业务场景制定动态策略，结合AI算法实时审核访问行为、动态授权，实现按需授权、动态调整。在控制模型方面，融合RBAC与ABAC模型的核心优势，融入政务数据分级分类理念，替代传统静态访问模型。例如，针对政务数据分级管理场景，融合模型按业务岗位分配角色与基础权限，实现权限规范化管理；针对跨部门协作场景，结合人员岗位、操作时间、数据密级等多维度属性，通过AI动态判断访问权限，实现一人一权、一事一权，相较于传统模型，更适配政务业务的灵活性与安全性需求。

1.2.4 流量审计

流量审计技术核心是融合AI深度学习技术，实现网络流量的全维度采集、深度解析与智能分析，大幅提升分析精准度与实时性。数据安全网关通过分布式采集节点，记录政务网络流量的来源、目的地、传输内容等信息，应用于政务内网安全监控场景，借助深度学习算法实时分析，快速区分正常与异常流量，精准检测AI入侵、隐蔽式数据泄露等新型威胁，提升政务数据泄露与网络攻击的应急响应速度。通过深度挖掘审计数据，可提前发现内网异常访问、违规数据传输等潜在威胁，为安全事件预警与处置提供支撑。同时，审计日志采用国密算法加密存储、时间戳全程标记，确保不可篡改、可追溯，满足政务领域安全审计合规要求，适配政务安全检查、事件溯源等场景。

1.3 数据安全网关与传统安全设备的对比

防火墙、入侵检测系统（IDS）等传统安全设备，是早期网络安全防护体系的基础组成部分，在基础网络层防护中发挥了一定作用，但受技术架构和设计理念的限制，存在功能短板，难以应对当下新型安全威胁，无法匹配政务领域国产化适配需求。其中，防火墙的防护核心主要聚焦于网络层访问控制，通过制定IP地址、端口等规则实现访问限制，对应用层、数据层的防护能力较弱。IDS则主要基于已知攻击特征库进行威胁检查，仅能识别已发现的攻击行为，对未知、隐蔽攻击缺乏检测能力，且缺乏数据加密、精细化访问控制、全流程审计等核心功能，防护维度单一。

新一代数据安全网关则大不相同，它集成国密全栈防护、多模态智能认证、AI流量审计、新型威胁防御等前沿安全技术，可实现对网络层、应用层、数据层、行为层的全方位、全流程闭环防护。且它从硬件到软件全面适配国产芯片、操作系统与政务信息系统，支持与其他国产安全设备的无缝对接与协同联动，具备更高的灵活性、可扩展性与智能化水平。另外，设备支持根据政务不同业务场景的安全需求，进行安全策略的定制化配置与功能模块的灵活组合，真正实现按需防护、精准管控。

2 信息化网络安全系统需求分析

2.1 业务场景与安全威胁

当前政务信息化业务场景呈现多元复杂、智能跨域、线上线下融合的特征，核心涵盖政务协同办公、线上业务办理、跨部门数据交互、远程移动办公等场景，不同场景的数据传输、访问主体、资源类型差异显著，安全防护重点难点各不相同。同时，网络安全威胁呈现新型、隐蔽、AI化的特征，给政务网络安全带来严峻挑战。内部协同办公易出现越权访问、违规传输敏感数据等问题；线上业务办理面临公网数据窃取、篡改、恶意攻击等威胁；跨部门数据交互存在传输不安全、脱敏不彻底等隐患；远程移动办公则有身份伪造、传输通道监听等风险，加之攻击手段持续升级，对防护体系的智能化、动态化能力提出更高要求。

2.2 功能需求

结合政务信息化网络业务场景、主流安全威胁及新一代数据安全网关核心技术，以政务国产化合规为准则，安全系统需具备七大核心功能。一是国密协同加密传输，全场景采用国密算法加密，支持软硬双模切换，高安全场景可融合量子加密技术[2]。二是多模态智能身份认证，整合多种认证方式，精准校验访问主体身份与终端合规性。三是自适应访问控制，结合数据分级分类要求，实现权限精细化、动态化管控。四是AI智能流量审计，全维度采集分析流量，生成可追溯日志。五是新型威胁防御，快速识别处置AI入侵、零日漏洞利用等威胁。六是敏感数据智能脱敏，结合AI实现数据分级分类与脱敏。七是国产化协同管理，对接国产安全设备，构建国产化防护生态。

2.3 非功能需求

非功能需求，是保障其稳定、高效、安全、合规运行的重要支撑，涵盖多方面要求。可靠性上，系统基于国产软硬件构建，稳定性高、连续运行时间长，故障恢复快，具备国产化冗余备份功能。可用性上，操作界面简洁直观，适配国产操作系统，操作便捷，响应时间短，不影响业务开展。安全性上，系统自身安全性高，可抵御多种常见网络攻击，审计日志不可篡改、可追溯，加密算法符合国家安全标准。扩展性上，采用模块

化设计，可灵活增加模块、扩展功能范围。易用性上，提供完善的用户手册与指引，支持人员培训，具备故障自诊断等功能。

3 基于数据安全网关的系统设计

3.1 总体架构设计

基于新一代数据安全网关的信息化网络安全系统总体架构，遵循“国产化适配+分层协同+智能防护”设计模式，契合政务国产化要求与网络安全发展趋势，自上而下分为四层。终端接入层作为前端入口，涵盖各类政务接入终端，需安装国产安全客户端保障接入合规；安全网关层为核心防护层，部署国产化智能数据安全网关，实现全流程流量与数据访问管控；核心服务层负责业务处理与集中管理，基于国产中间件构建，实现策略配置、权限管控与威胁处置；数据存储层采用国产化方案，融合区块链技术，通过国密加密、冗余备份等手段保障数据安全。各层次通过标准化国产接口交互，确保协同高效[3]。

3.2 核心模块设计

3.2.1 数据加密模块：集成于数据安全网关，支持国密全栈算法协同，高安全场景可集成量子加密，支持软硬加密双模切换。数据传输环节用SM2协商密钥、SM4加密数据、SM3校验完整性；存储环节对敏感数据与审计日志进行加密，构建国产化密钥全生命周期管理体系，辅以加密状态监测等功能提升系统灵活性。

3.2.2 访问控制模块：基于数据安全网关，遵循“最小权限”原则，采用RBAC与ABAC融合模型。可按岗位分配角色与权限，结合多属性通过AI动态判断访问权限，实现精细化管控，具备权限申请、审批、预警等功能，实时拦截非法操作，适配政务数据分级分类要求。

3.2.3 流量审计模块：集成于数据安全网关，融合AI深度学习技术，实现流量全维度采集、智能解析与日志管理。可采集流量各类详细信息，通过AI精准区分正常与异常流量，检测新型攻击，生成国密加密、时间戳标记的可追溯审计日志，支持多维度检索。

3.2.4 威胁防御模块：集成于数据安全网关，结合多种新型检测技术，可自动更新威胁特征库，精准检测拦截已知与未知攻击，实时监测异常行为并分级告警，集成国产化恶意代码查杀引擎，辅以威胁分级分析、应急联动等功能，提升处置效率。

3.3 数据库与接口设计

数据库设计遵循政务国产化要求，采用国产关系型数据库存储结构化数据、非关系型数据库或分布式系统存储非结构化数据，通过国密加密敏感数据，采用国产冗余备份机制保障数据可恢复[4]。接口设计遵循标准化、国产化原则，内部接口采用国产通信协议，外部接口支持多种主流协议，可无缝对接各类国产设备与系统，远程运维采用国密协议，通过国密加密认证与安全启动机制保障接口安全。

结束语

本文围绕新一代数据安全网关，完成信息化网络安全系统的全流程设计研究。从技术基础分析出发，结合政务业务场景与安全威胁，明确系统需求，搭建“云管端”立体化总体架构，设计核心功能模块，以及国产化数据库与接口方案。未来，将结合政务实际应用反馈优化系统功能，提升系统智能化与国产化适配能力，探索前沿技术融合应用，完善防护体系，为政务信息化网络安全稳定运行提供有力保障。

参考文献

[1]侯龙.基于数据安全网关的信息化网络安全系统设计[J].通信电源技术，2025，42(14):47-50.

[2]马翔明,穆炜,董文清.基于数据安全网关的医院信息化网络安全防御系统设计[J].微型电脑应用,2022,38(7):99-101,113.

[3]洪宝惜.基于安全网关技术谈网络安全设计分析[J].网络安全和信息化，2023(02)：127-129.

[4]陈立军,廉成绪.基于安全网关技术的网络安全设计分析[J].网络安全技术与应用,2022(11):4-6.