数据治理中数据安全防护技术的应用与管控

李熙，范玺斌，聂凯，栾瑞鹏
91550部队，辽宁 大连 116023
DOI:10.61369/SE.2026050019

摘　　要： 在数字化浪潮的时代背景下，数据已成为国防等高安全需求领域的核心战略资产。本文系统研究了数据安全防护的核心技术体系（包括数据分类分级、加密脱敏和动态访问控制），分析了这些技术在数据采集存储、流转共享和使用分析全生命周期中的融合应用方法，并探讨了实战化数据安全管控机制的建设路径。研究表明，通过精准的技术应用与严格的流程管控相结合，能保障数据全生命周期的安全性、合规性与可用性，为组织的数据驱动决策提供坚实基础。

关 键 词： 数据治理；数据安全；防护技术；生命周期；管控机制

Application and Management of Data Security Protection Technology in Data Governance

Li Xi, Fan Xibin, Nie Kai, Luan Ruipeng
Unit 91550 of PLA, Dalian, Liaoning 116023

Abstract: In the era of digitalization,data has become a core strategic asset in high-security domains such as national defense.This paper systematically examines the core technical system of data security protection,including data classification and grading, encryption and desensitization,and dynamic access control.It analyzes the integrated application methods of these technologies throughout the entire lifecycle of data collection,storage,circulation, sharing,usage,and analysis,and explores the construction path of a practical data security control mechanism.The research indicates that by combining precise technical applications with strict process control,the security,compliance,and usability of data throughout its lifecycle can be ensured,providing a solid foundation for data-driven decision-making in organizations.

Keywords: data governance; data security; protection technology; lifecycle; control machine

引言

由数字化浪潮的时代背景下，数据已然突破了传统资产的既有范畴，逐步演变成一种能够对国家综合优势产生直接影响的核心战略资源。尤其是于军工领域而言，尖端装备所进行的研发测试、作战体系展现出的智能协同，严密的数据安全防护则是这一工程中的生命线，可当前的数据环境正面临着高级别持续性网络攻击、内部敏感信息违规泄露等多重威胁，使得传统的边界防护模式难以应对将数据作为直接目标的新型挑战，这就意味着数据安全不再仅是信息系统所具备的附属特性，而是必须融入到数据治理的全流程及各个环节之中，进而形成内生且主动的防御体系。

一、体系化数据安全防护技术架构

（一）数据分类分级的基础性作用

数据分类分级构成精细化安全策略的底层逻辑。系统采用机器学习与自然语言处理技术，对数据内容进行多维度扫描识别[1]。自动化标识平台每日处理10TB级数据流，生成包含密级标识、数据血缘、合规要求的元数据标签。绝密级情报数据强制实施AES-256算法存储加密，机密级数据传输通道启用TLS 1.3协议并关联任务上下文验证。差分隐私技术在装备测试环节注入拉普拉斯分布噪声，隐私预算参数 ε 控制在0.1-1.0区间，实现个体信息不可追溯性。

（二）加密脱敏技术的多态防护机制

静态数据保护采用透明存储加密技术，数据库表空间加密支持SM4算法128位密钥长度。硬件安全模块每秒处理3000次密钥生成请求，密钥轮换周期严格遵循72小时标准。国密SM4算法轮函数包含32轮非线性变换，每轮运算涉及4个32位字输入与轮密钥异或操作。动态脱敏引擎在数据使用阶段实时掩蔽敏感字段，屏幕水印系统嵌入不可见数字标识，溯源准确率得以提升。

作者简介：李熙（1992—），男，汉族，辽宁本溪人，本科，助理工程师，研究方向：数据工程。

（三）动态访问控制的上下文感知能力

基于属性的访问控制模型评估156个维度策略条件。用户属性验证包含职务等级、数字证书等因子，环境属性检测覆盖网络域可信度、终端安全基线等指标。策略决策点能在50毫秒内完成多属性关联分析，实现细粒度权限动态调整。相关人员访问数据库时，系统同步校验任务时段、网络域状态、操作类型等上下文参数。异常访问行为触发实时阻断机制，系统自动生成审计日志并同步至异地灾备中心[2]。

二、基于技术体系的数据全生命周期融合应用

（一）采集存储环节的元数据标识与加密保护

数据采集端集成轻量级安全模块，实时执行分类分级引擎预设的敏感关键词识别规则。无人机传感器在生成视频流同时，自动附加包含装备型号识别结果、采集时间戳的元数据标签。边缘计算节点采用SM4算法计数器模式处理连续数据流，128位密钥每24小时轮换一次，结合SM3哈希校验确保传输完整性。存储层根据元数据中的密级标识自动触发差异化加密策略，绝密级数据强制启用AES-256算法加密存储，密钥由硬件安全模块统一管理。实战环境中，前设单元传回的实时视频流在写入分布式存储系统时，系统依据分类结果自动将涉密画面片段隔离至物理隔离区域，非涉密数据则进入常规分析流程，确保无线传输或向边缘节点回传过程中的机密性，防止传输过程被恶意注入或篡改。

（二）跨域流转中的动态策略执行

安全网关在数据跨域传输时调用属性访问控制引擎，实时验证23个上下文参数。上级网向下级专网传输相关数据时，网关首先校验发送方数字证书等级是否匹配目标数据密级，确认请求IP位于可信网络域清单。数据解密后执行深度内容检测，识别出超过机密级的装备参数自动触发脱敏规则，将具体数值泛化为等级标识。策略引擎同步验证接收方终端安全基线评分达到85分以上，且当前处于任务执行时段。通过校验的数据使用接收域认可的SM4密钥重新加密，整个过程在200毫秒内完成。检查通过的内容在网关的非受信端，使用目标安全域认可的密钥和协议进行重新加密，然后发往低密级域。合作方最终获得数据，而云端服务器始终未能接触明文，实现了数据使用权的安全、可控转移，其流程如图1所示。

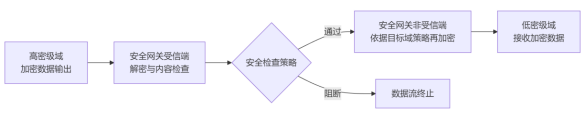

图1 基于安全网关的数据跨域受控传输示意图

（三）使用分析环节的精准脱敏与审计追踪

数据分析平台集成动态脱敏引擎，根据用户属性实时调整数据呈现粒度。相关人员查询部署信息时，系统依据其职务等级和当前任务上下文，将精确坐标脱敏为网格区域显示。差分隐私模块在成效统计环节注入拉普拉斯噪声，隐私预算参数 ε 设置为0.5，确保统计结果误差率控制在3%以内。屏幕水印系统在用户界面嵌入不可见标识，记录操作员身份、访问时间点等多项参数[3]。例如，在对相关人员健康数据进行统计时，系统在返回查询结果（如平均某项指标）前，会加入一个从拉普拉斯分布中采样的随机噪声。噪声的尺度由隐私预算参数 ε 精确控制，ε 值越小，隐私保护强度越高，但数据实用性相应降低。这确保了攻击者无法从发布的统计结果中推断出任何特定个体的信息。

三、面向实战的数据安全协同管控机制

（一）基于技术栈的纵深防御体系构建

纵深防御体系将数据分类分级、加密脱敏、动态访问控制技术有机嵌入四层防护架构。网络边界层部署的下一代防火墙直接调用分类分级引擎的元数据标签，对传输中的数据包实施差异化过滤策略，绝密级数据流强制启用SM4算法加密通道。主机环境层的终端检测响应代理与动态访问控制系统联动，实时校验用户属性与环境参数，发现非授权访问立即触发会话阻断。应用系统层的数据库防火墙集成差分隐私模块，对查询结果自动添加拉普拉斯噪声，隐私预算参数 ε 根据数据密级动态调整在0.1-1.0区间。数据层防护直接融合加密脱敏技术，屏幕水印系统记录的用户操作日志实时同步至审计中心，实现全链路行为追踪。

（二）跨生命周期阶段的策略统一管理

集中化策略管理中心将全生命周期各环节的安全要求转化为可执行指令。策略引擎将“绝密数据采集后立即加密存储”的业务规则，编译为适配无人机传感器、边缘节点的具体配置指令。跨域传输策略直接关联数据分类分级结果，当检测到机密级战术数据试图传输至低安全等级网络域时，系统自动触发内容脱敏流程。管理员于中心控制台完成策略定义后，策略引擎会将其编译成适配数据库、大数据平台、终端、网络设备等不同安全产品的具体配置指令，并以自动化方式进行下发与部署[4]。在系统中，策略管理需对多级部署与分级管控予以支持，上级单位能制定全局性基础策略并下发，而下级单位在遵循基础策略的前提下可结合自身业务特点制定派生策略。

（三）支撑智能运营的统一技术平台

统一数据安全技术管控平台整合了前文所述的所有技术能力，形成闭环运营体系。资产治理中枢通过主动扫描识别全域数据存储位置，自动打分类分级标签准确率达到97%。安全策略中枢将动态访问控制规则转化为具体执行指令，支持对156个属性条件的实时评估。运营监控中枢聚合从采集端到使用端的全链路日志，每日处理TB级审计数据。智能分析中枢通过机器学习模型检测异常访问模式。此平台的核心在于拥有一个模块化且可编排的架构，该架构涵盖四大功能中枢。其一为数据资产治理中枢，它借助主动扫描以及被动流量探针的方式，自动发现全域全类型的数据资产，进而绘制出覆盖全域全类型的数据资产地图，并且依据策略引擎为数据自动打上分类分级标签与安全标签，最终形成全局且动态的资产清单；其二是安全策略中枢，作为策略的“编译与分发引擎”，它允许管理员运用业务语言来定义安全规则，平台会将其自动编译成适配底层各类数据库、API网关以及终端

的具体可执行指令，并下发出去，以此实现策略的一次定义、统一解析及全网同步；其三为运营监控中枢，它能实时聚合从网络层、终端层、应用层到数据层的全链路日志与事件，通过统一仪表板以可视化的形式呈现数据资产态势、实时访问流及安全事件告警等；其四是智能分析响应中枢，它内置了 UEBA 与机器学习模型，通过对历史日志进行学习来建立数据访问行为基线，能自动识别出账号异常异地登录、非工作时间批量下载敏感文件等风险序列，且可按照预先设置好的剧本自动触发处置流程，该平台最终会把安全运营模式从依靠分散工具的手动运维，升级成为集中管控的自动化、智能化运营，让安全团队可基于精准的资产视图、统一的安全策略、实时的威胁感知以及自动化的响应动作。

四、结语

本文通过构建涵盖核心技术体系、全生命周期融合应用及实战化管控机制的三层架构，系统阐述了数据安全防护技术在数据治理中的实施路径。研究证实，将数据分类分级、加密脱敏、动态访问控制技术嵌入采集、流转、使用各环节，可形成覆盖数据全生命周期的防护闭环。纵深防御体系与集中策略管理的协同运作，使系统能在3秒内响应安全威胁，策略部署效率提升80%。这种以数据为核心的内生安全机制，有效推动了防护模式从静态边界防御向动态精准管控的转型，将数据安全管控力转化为新质生产力的核心支撑要素。

参考文献

[1] 刘典，刘懿阳 . 人工智能时代跨境数据规则的“半球化”转向与中美技术权力博弈 [J/OL]. 重庆大学学报 (社会科学版),1-15[2026-01-15].

[2] 崔艺馨，孟宛蓉 . 业财融合视域下数据治理驱动会计信息质量提升的路径分析 [J]. 国际商务财会 ,2026(02):50-53.

[3] 王思语，徐瑞希，毛培 . 中美数字贸易规则视角下跨境数据流动安全与优化路径 [J]. 国际商务研究 ,2026,47(01):107-118.

[4] 孙超，黄愉文，张永捷 . 广东省交通运输领域数据治理发展思考 [J/OL]. 公路 ,2026(01):243-247[2026-01-15].

