云计算技术在高校网络安全态势感知中的应用研究

高 磊
新疆天山职业技术大学 新疆 乌鲁木齐 830017

摘 要：本文聚焦云计算技术在高校网络安全态势感知中的应用。先分析云计算与高校态势感知在算力、成本、扩展性上的适配性及局限性规避措施。接着阐述基于云计算的体系设计，包括核心原则、整体架构与核心功能模块。随后对云计算技术在体系中的关键应用进行优化，涵盖弹性计算、分布式存储、云原生安全、大数据分析等方面。旨在通过云计算技术提升高校网络安全态势感知能力，保障校园网络安全，为高校网络安全建设提供理论支持与实践参考。

关键词：云计算技术；高校网络安全；态势感知

引言：在高校数字化转型背景下，网络安全至关重要。高校校园网络规模庞大、终端多样，每日产生海量数据，传统网络安全态势感知模式面临算力不足、成本高、扩展性差等问题。云计算技术凭借弹性算力、低成本、高扩展性等优势，为高校网络安全态势感知带来新契机。本文深入探讨云计算技术与高校网络安全态势感知的适配性，设计基于云计算的体系，并优化关键应用，以提升高校网络安全防护水平，适应不断变化的网络安全形势。

1 云计算与高校态势感知的适配性分析

1.1 算力适配

云计算与高校态势感知在算力层面具备高度适配性，这一适配性源于高校网络安全态势感知的核心算力需求与云计算的算力供给特性的精准契合。高校校园网络覆盖范围广，连接终端数量多，涵盖教学终端、科研设备、行政系统及师生个人设备等，每日产生超10TB网络行为数据、设备运行数据及安全日志数据。态势感知需对这些多源异构数据进行实时采集、清洗、分析及威胁研判，对算力的瞬时峰值需求高且存在显著波动性，如新生入学季网络流量较平日激增3-5倍，算力需求随之攀升。云计算通过分布式算力集群构建弹性算力池，可根据高校态势感知的实时算力需求动态分配计算资源，峰值时段可在5分钟内完成10倍算力扩容，保障威胁研判延迟控制在500ms内，非峰值时段自动缩容至基础算力的20%，避免资源闲置，有效解决传统本地算力部署难以应对算力波动、易出现算力不足或资源浪费的问题。

1.2 成本适配

云计算在成本方面与高校有限的经费预算需求高度契合，相较于传统本地部署模式优势显著。传统模式下，高校构建态势感知系统时，前期需投入巨额资金购置服务器、存储等硬件设备，这还不包括后续的场地租赁、电力消耗以及人员运维等费用。随着系统的发展，后续的升级扩容还需持续投入大量资金。而云计算采用“按需付费”的创新模式，高校无需在前期投入巨额资金购置硬件，只需根据自身实际需求，灵活选择合适的云服务套餐。如此一来，年均成本可大幅降低。同时，云服务提供商会负责云端基础设施的维护、升级以及安全防护等工作，高校可减少运维人员投入[1]。另外，云计算支持资源弹性伸缩，高校能够根据需求逐步扩容，有效避免了资金闲置，实现了成本的精细化管控，让有限的经费能更高效地投入到态势感知的核心功能优化上。

1.3 扩展性适配

云计算分布式架构特性适配高校态势感知系统扩展性需求，支撑长期迭代升级。高校数字化转型使态势感知覆盖范围延伸至智慧教室、校园物联网等新兴场景，数据采集维度从传统5类增至12类以上，对系统功能与数据处理扩展性要求提高。传统本地部署系统扩展性差，新增功能或扩大范围需升级改造硬件甚至重构架构，耗时超3个月且影响运行。云计算基于虚拟化等技术，横向可在1周内增加节点、扩展存储提升数据处理能力，纵向能快速集成新功能模块，无需大规模调整核心架构。云端资源共享便于高校与其他机构数据共享与协同研判，拓展应用边界，满足系统持续升级需求。

1.4 局限性与规避

云计算与高校态势感知适配但有局限性，需科学规避。数据安全风险是核心，高校态势感知数据含大量敏感信息，云端存储面临泄露、篡改等威胁，传输有被拦截风险。高校还依赖云服务提供商，其服务中断等可能影响系统运行。规避措施如下：构建数据加密体系，对传输和存储数据端到端加密，脱敏处理敏感信息；建立多云备份机制，同步备份核心数据至不同云端和本地

备份中心；签订规范云服务协议，明确提供商安全责任等；保留核心研判功能本地应急部署能力，云端服务中断时可切换至本地，确保态势感知连续性。

2 基于云计算的高校网络安全态势感知体系设计

2.1 体系设计核心原则

基于云计算的高校网络安全态势感知体系设计有四大核心原则，保障其科学、安全与实用。其一，安全优先。以保障校园网络安全、保护敏感数据隐私为首要目标，将云原生安全技术融入各层级架构，构建全方位、多层次防护体系，防范云端资源滥用等风险，确保态势感知可靠[2]。其二，精准适配。结合高校网络特性、数据规模和需求，合理选云服务与资源配置，使体系功能与实际高度匹配，避免冗余或不足，且与现有系统兼容，实现数据无缝对接。其三，实时高效。依托云计算弹性算力，优化数据处理流程，提升效率，实时捕捉安全态势变化，快速识别威胁，为决策提供及时支撑，降低损失。其四，可扩展可维护。架构设计灵活可扩展，适应网络规模扩大等需求，便于新增模块与扩容；简化运维流程，依托云服务提供商降低维护难度，提升运维效率。

2.2 体系整体架构设计

该体系采用“云-边-端”三级架构，实现全流程协同。终端层是数据采集端，覆盖校园内超10万台各类设备、系统及物联网设备，部署轻量级代理，实时采集多源异构数据，经初步处理后传至边缘层。边缘层部署在校园网络边缘节点，承担数据预处理与本地应急响应功能。利用边缘计算资源清洗、脱敏、聚合数据，过滤60%以上无效信息，减少云端传输量，降低带宽压力；具备本地简单威胁研判能力，响应时间控制在1秒内，快速响应紧急事件。云端层是核心处理中心，依托公有云或混合云构建，含算力、存储集群及核心分析引擎，深度分析数据、研判态势，利用弹性算力挖掘威胁、评估态势，通过分布式存储安全存储数据；还部署可视化与决策支持模块，直观呈现结果，提供决策支撑。

2.3 核心功能模块设计

基于云计算的高校网络安全态势感知体系核心功能模块围绕数据处理全流程设计，涵盖数据采集、数据预处理、态势分析研判、态势可视化及应急响应五大核心模块。数据采集模块采用分布式采集架构，通过在校园网络各终端、设备及系统部署采集代理，支持对网络流量、安全日志、设备状态、用户行为等多源数据的实时采集，具备协议适配能力，可兼容TCP/IP、SNMP、Syslog等多种数据传输协议，数据采集覆盖率达99%以上，确保全面性与实时性。数据预处理模块部署于边缘层与云端，边缘层负责数据清洗、脱敏与聚合，剔除噪声数据、敏感信息脱敏处理并按数据类型聚合；云端负责数据标准化与特征提取，将不同格式的数据转换为统一标准格式，提取数据中的安全特征。态势分析研判模块是体系核心，依托云端弹性算力，集成机器学习、深度学习等算法，构建威胁识别模型、态势评估模型，威胁识别准确率超95%。态势可视化模块采用云原生可视化技术，通过仪表盘、热力图等形式直观展示信息。应急响应模块与研判模块联动，自动触发应急处置流程，实现威胁快速响应。

3 云计算技术在体系中的关键应用优化

3.1 弹性计算技术的应用优化

弹性计算技术在高校网络安全态势感知体系中的应用优化，核心在于实现算力资源与态势感知需求的动态精准匹配。针对高校态势感知数据处理存在明显时段性波动的特点，优化弹性算力调度策略，基于历史数据构建算力需求预测模型，结合校园网络运行规律提前调度算力资源。采用容器化技术（如Docker、Kubernetes）封装态势感知分析任务，实现计算资源的细粒度调度，单任务资源分配精度达0.1核CPU、128MB内存。优化弹性计算的伸缩触发机制，设定多维度触发阈值（如CPU利用率80%、内存占用率75%、数据处理延迟500ms），当监测到某一阈值超标时自动触发算力扩容，3分钟内完成节点添加；当资源利用率低于30%时自动缩容。针对复杂分析任务，采用分布式弹性计算架构，将任务拆分至多个云节点并行处理，使APT攻击研判时间从2小时缩短至30分钟，提升效率与准确性。

3.2 分布式存储技术的应用优化

针对高校态势感知海量多源数据的存储需求，对分布式存储技术的应用进行多维度优化。在存储架构优化方面，采用混合存储架构，结合对象存储、块存储、文件存储的优势分类存储数据，具体适配如下表所示。在数据可靠性优化方面，采用多副本备份与纠删码技术相结合的方式，为核心数据配置3个副本存储于不同云节点，同时利用纠删码技术将数据按N+M比例编码，即使2个节点故障也可恢复数据，数据可靠性达99.999%。在访问效率优化方面，构建分布式缓存机制，将高频访问的数据缓存至边缘节点，数据访问延迟从100ms降至20ms以内。优化数据生命周期管理策略[3]。对数据分级管理，自动将超过6个月未访问的历史数据迁移至低成本存储节

点，降低存储成本30%。

表1 分布式存储架构数据分类适配表

存储类型	适配数据类型	核心优势	应用场景
对象存储	非结构化数据（流量日志、视频日志）	单桶容量达PB级，扩展成本低	海量历史日志长期存储
块存储	结构化数据（设备状态、威胁告警）	IOPS达10万级，读写速度快	实时态势分析数据存储
文件存储	半结构化数据（分析报告、配置文件）	支持多节点共享，访问便捷	跨部门协同研判数据共享

3.3 云原生安全技术的融合应用

为提升基于云计算的高校态势感知体系自身的安全性，强化云原生安全技术的融合应用。将容器安全技术深度融合于体系架构，在容器镜像构建阶段进行安全扫描，扫描覆盖率达100%，过滤包含恶意代码、漏洞的镜像；在容器运行阶段实时监测容器行为，每秒采集10条行为日志，防范容器逃逸、权限滥用等安全威胁。采用微服务安全架构，将态势感知体系的核心功能拆分为8个微服务模块，每个模块部署独立的安全防护策略，通过API网关对微服务间的通信进行加密与身份认证，通信加密强度达AES-256级。融合云安全访问代理（CASB）技术，对高校访问云端态势感知资源的行为进行集中管控，实现身份认证、权限校验、行为审计等功能，非法访问拦截率达99%。集成云安全态势感知技术，实时监测云端基础设施的安全状态，漏洞发现时间缩短至24小时内，与高校自身态势感知体系形成协同防护。

3.4 大数据分析技术的协同应用

优化大数据分析技术与云计算技术的协同应用，提升高校态势感知的数据处理与威胁研判能力。在数据协同处理方面，依托云计算的分布式算力优势，优化大数据分析的并行处理架构，采用Spark、Hadoop等框架将海量数据拆分至多个云节点并行处理，数据处理吞吐量达10GB/分钟，解决传统分析技术难以处理海量数据的问题[4]。在算法协同优化方面，将机器学习、深度学习等算法与云计算的弹性算力相结合，利用云端算力支撑算法模型的训练与迭代，模型训练时间从72小时缩短至12小时，构建高精度的威胁识别、态势评估模型，异常流量识别准确率达96%。在数据协同关联方面，优化多源数据关联分析算法，实现校园网络内不同来源数据的深度关联分析，挖掘数据间的潜在关联，识别隐藏的复杂攻击行为。构建大数据分析结果的反馈机制，将研判结果实时反馈至云计算资源调度模块，实现深度协同。

结束语

云计算技术凭借在算力、成本、扩展性等多方面的适配优势，为高校网络安全态势感知带来全新变革，有效解决了传统模式面临的算力不足、成本高昂、扩展困难等难题。通过适配性分析、体系架构搭建以及关键应用优化等举措，显著提升了高校网络安全态势感知能力。展望未来，网络安全形势依旧复杂多变，需持续深化云计算技术与态势感知的融合，紧跟技术发展趋势，不断优化完善体系，为高校各项活动的顺利开展筑牢坚实的网络安全防线。

参考文献

[1]王佳君.基于"云计算"虚拟化技术高校计算机网络安全实训实验室构建分析[J].信息技术与信息化,2021(11):222-224.

[2]杨华.基于云计算技术的计算机实验室网络安全研究[J].信息记录材料，2025，26(10):157-159.

[3]吴凌,吴雨辰.基于云技术的高校计算机实验室网络安全隐患与防护策略研究[J].无线互联科技,2022,19(8):104-105.

[4]刘勇.基于云计算和虚拟化的网络安全实验教学平台建设研究[J].对外经贸,2024(7):89-92.