教育云安全体系构建及应用研究

代娥[1] 龙辉[2] 郑小波[1*]

1. 四川公众项目咨询管理有限公司；2. 四川通信科研规划设计有限责任公司

摘 要：近年来，5G 网络大规模建设积极推动我国千行百业数字经济高质量发展。本研究介绍了教育云的应用现状，分析了教育云面临的安全风险，结合云安全技术的发展趋势提出教育云安全体系，通过某高校教育云网络安全典型案例进行了功能验证，为教育云网络安全提供数据支撑和安全策略参考。

关键词：教育云；安全风险分析；IaaS；PaaS；SaaS；安全体系研究

引言

随着信息技术的飞速发展，尤其是大数据、 云计算和人工智能等新兴技术的广泛应用，教育领域正经历着前所未有的变革[1]。教育云以动态调配、按需服务的模式面向教育机构、教师与学生提供所需的信息化教学、科学化管理等服务，是云计算技术在教育领域的深入应用,为传统教育教学和教务管理提供便利，促进传统教学和教务管理模式创新。随着教育云广泛应用，网络安全问题也日益突出，构建教育云安全体系需求日益迫切。

一、教育云安全风险分析

虚拟化作为云计算的关键技术，在提高云基础设施使用效率的同时，也带来了很多新问题。教育云应用程度越高、数据量越大所带来的网络安全风险就越高。云计算模式的成功依赖于强大可靠的虚拟化和分布式计算技术，其依赖于由计算、存储、网络等设备所构成的物理层。在云平台的物理安全中，主要包括自然风险、运行风险和人员风险等安全风险。在云计算信息系统中，常用的存储介质有硬盘、磁盘、磁带、打印纸、光盘等，使用这些存储介质来存储、交换数据，极大地方便了数据转移和交换，但也给云信息系统带来了很大的安全风险。在教育云系统部署与运营期间应该告知学生如何保护私人信息以及使用平台需遵循的法律义务。为防范网络漏洞遭受恶意攻击需做好平台的基础网络安全防护工作。持有合法用户账户的教师可能存在蓄意破坏造成教学责任事件；合法账户未妥善保管导致账户泄密，被他人非法登录进入教育云平台数据库加载恶意信息或篡改教学内容。在教育云平台中只允许合法的协议和许可的服务进行登录访问和数据传输，可能面临网络入侵、恶意攻击等行为。恶意 SQL 攻击风险。攻击者利用系统漏洞，构建项目提供程序条件，直接在商业数据库系统后端读取和写入未经授权的数据,并绕过或欺骗站点用户身份验证。攻击者可以在进入商业数据库系统后伪造、下载和分发恶意信息，严重影响正常操作系统正常运行。

二、教育云安全体系构建

云计算信息系统设备安全应该考虑设备安置、供电、设备维护及处置等方面的安全控制。必须从技术与管理两个层面入手加以解决：①从技术层面来看，解决好基础架构是 保障安全的关键要素。安全的基础架构一方面要基于教 育云的自身规划与建设重点，按需配置，在体系构建的过 程中，要重点关注开放性与动态可重构；另一方面要合理 把握，按需部署，确保教育云的安全，要从动态可重构、 实时监控和自动化部署等方面解决资源存在的问题。②从管理层面来看，机制体制、运行维护、人才队伍等 都是确保教育云安全的关键要素[2]。基于教育云安全风险，教育云安全需要在传统信息系统安全措施的基础上，充分利用云计算平台的特点，采用先进的信息安全技术来提高云计算平台的安全性。本研究建议根据云计算平台和物理资源的边界将其分为基础设施层、平台组件层与应用接入层，以构建教育云的安全体系，如图 1 所示。通过对每层分别进行安全事件处理策略以及安全日志的严格管理进行教育云平台安全防护与信息安全管理。

（一）基础设施层

基础设施层安全防护措施主要涉及物理设备安全、网络安全及虚拟化安全。物理设备的安全与地理、物理、环境的安全紧密相关[3]。对云计算平台所

作者简介：代娥（1984—），女，本科，经济师，研究方向为数字经济、政府采购招标。
龙辉（1985—），男，本科，工程师，研究方向为 5G智慧行业应用及信息安全。
通讯作者：郑小波（1985—），男，本科，工程师，研究方向为 5G行业应用及网络安全。

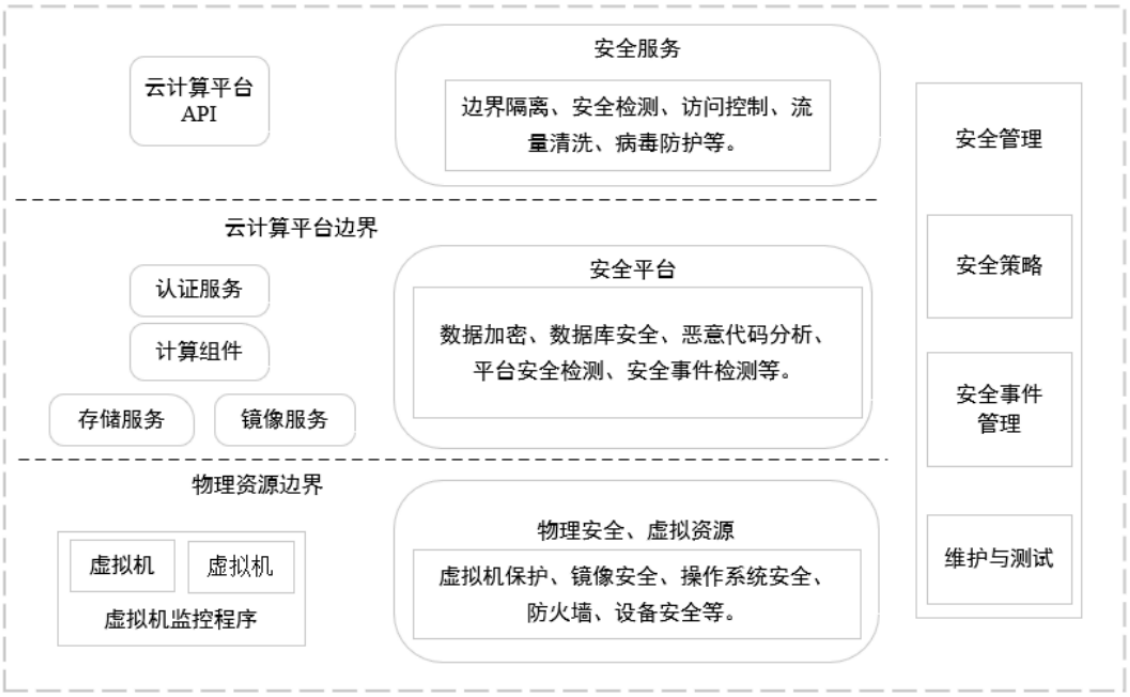

图 1　教育云安全体系架构

处物理环境的保护包括防火、防水、防静电、防雷击等。在网络安全的各个方面，我们需要使用 IPS、防护墙和其他身份验证、授权和访问控制方法，传播身份认证以检测网络攻击，并及时发出自动警报。为了防止 DoS 攻击并防止攻击者控制的大量资源，流量控制系统将流量数据流式传输到云平台。传播恶意数字保护系统，防止物理计算机系统渗透，从而确保物理计算机系统和管理程序的安全。教育平台云中物理设备或虚拟设备之间的通信可以识别恶意流量监控和针对计算机黑客的数字保护。它还可以阻止云中物理设备或虚拟设备之间的通信，通过教育平台识别恶意流量监控并保护免受计算机黑客攻击。它还可以防止虚拟机水平或垂直攻击其他虚拟机，虚拟安全可以防止物理机入侵虚拟机，从而确保良好的系统性能。

（二）平台组件层

平台组件层安全防护措施是确保教育云全生命周期的各种操作和数据处理过程的安全[3]。其中，认证授权过程涉及加密算法的应用和密钥管理，可采用公钥基础设施（Public Key Infrastructure， PKI）或通用唯一识别码（Universally Unique Identifier， UUID）等方式进行授权认证。存储服务涉及数据的产生、传输、存储、使用、迁移、销毁、备份和恢复的全生命周期，对数据进行分类分级、标识、加密、审计及销毁等数据安全管理工作。容灾备份使用物理分离，通过在同一城市或其他地方建立和维护备份存储系统，确保系统和数据免受灾难性事件的影响。

（三）应用接入层

应用接入层将访问层应用于安全保护措施需要用户身份验证，部署严格的访问控制和权利管理政策，以消除访客并有效监控安全区内外的通信。通过检测异常流量分析系统，进行流量分析和过滤。Web 应用防火墙根据预设的安全规则检查流量，并对流量 统计分析，实时监控云平台流量的地域分布，应用组成分布，变化趋势，并生成统计表[3] 安全区域是指需要云服务提供商进行保护的业务场所和包含被保护信息处理设施的物理区域。管理云计算平台、云计算服务、云数据、云设备、运行维护和检测。信息安全管理通过提供安全政策、管理和评估安全事件和安全杂志来确保活动的连续性。云平台管理器可以专门用于安全管理、组织和管理员，以确保云系统教育平台的正常运行。

三、教育云安全应用案例

以我国某大学教育云为例，从案例概述、需求分析、方案设计、部署实施及案例效果等方面详细分析天池实验云计算平台在教学信息系统安全合规建设场景中的典型应用，对本研究提出的教育云安全体系有效性进行功能验证。

（一） 案例概述

某大学采用阿里云技术架构建设了一套云计算平

台，目前该云计算平台已经建设完成并投入使用，主要为大学内部的各个院系及其他院校提供云资源服务，支撑教学信息系统及教务系统等，构建大学自己的教育云，打造教育行业的云生态圈。但在教育云规划建设初期，没有充分考虑安全建设，尤其是云上的安全建设。为了解决教学业务系统存在的安全隐患，防止教学信息数据泄露，某大学计划建立和完善云安全建设，全面打造云生态圈的服务能力。

（二）需求分析

我国某大学教育云需要满足教育云上的教学业务系统自身安全防护、云上教务系统的安全合规要求、云安全资源统一管理及按需分配、云租户（院系自身系统）安全自主管理与自助服务。

（三）方案设计

采用天池超融合一体机云安全解决方案帮助我国某大学在云机房搭建一套私有化的云安全资源池。云安全资源池提供的安全能力包括：综合漏洞扫描、下一代云防火墙、云 Web 应用防火墙、网页防篡改、云堡垒机、云数据库审计、EDR 及云综合日志审计等。人员保障措施包括详细了解具有云基础设施平台访问权限的内部人员信息，坚持人员安全管理的原则，进行合理职责分配，执行人员安全培训等有效措施，加强人员的安全保障；在对安全相关工作进行部署时，每项工作都必须有 2 人或多人在场，避免误处理。信息安全管理人员不应长期担任与信息安全运行有关的职位，从而保持信息管理安全管理岗位的竞争力和流动性。

本方案为教育云上的租户提供安全服务能力，实现云安全能力服务化。云上的租户可以根据自己业务需求登录天池云安全管理平台自助申请云安全服务，保障云上业务系统安全。

（四）部署实施

本方案某大学教育云部署结构如图 2 所示。中天池超融合一体机采用旁路部署的方式与某大学教育云计算平台的核心交换机互连，通过策略路由的方式对云计算平台的进出流量进行牵引，结合云安全资源池中的安全能力对进出流量进行清洗和防护。从物理主机、主机操作系统、虚拟机操作系统、Hypervisor 及其应用程序等从不同层面有针对性地制定相应的安全措施，以保障云平台虚拟化的安全。在云计算环境下对物理设施及环境进行安全保护主要是对环境考虑、访问控制、监测、人员识别、非法行为检测进行多方面保护。

（五）案例效果

我国某大学教育云计算平台的建设及应用完善了云计算平台自身的安全能力，构建了统一的安全资源池，形成了云安全运营管理中心，对云计算平台本身进行了安全加固。精简 Hypervisor 代码，优化代码质量，减少代码中存在的漏洞，并简化 Hypervisor 功能。为虚拟机提供良好的隔离性，防止恶意虚拟机利用

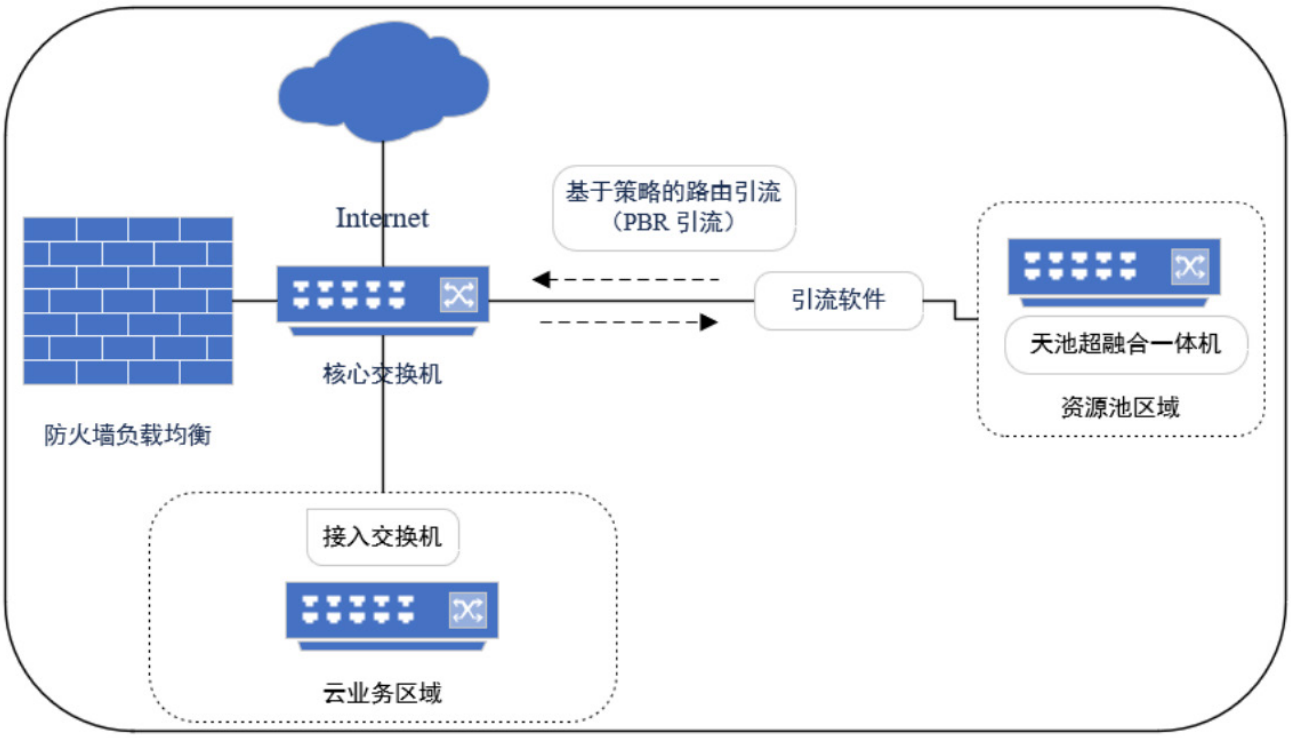

图 2　某大学教育云部署结构

Hypervisor 的漏洞威胁其他虚拟机。增强虚拟机中 I/O 操作的安全性，I/O 操作虚拟机需要与外部设备进行交互，Hypervisor 需要对其进行模拟。如果模拟操作出现问题，则会影响整个平台上的所有虚拟机。

提供多元的安全服务，解决云上业务系统安全问题，实现云安全资源动态分配和按需使用，实现云安全统一管理，打造了云安全增值服务。

四、结语

未来，云计算应用作为教育机构实现教育数字化、智能化的有效途径将持续受到大力推崇。在我国财政部门对教育信息化大力支持下，预计 2020—2025 年云计算在教育行业应用营收规模有望以 22% 左右的增长率快速增长，前瞻预计到 2025 年市场规模有望达到 285 亿元。着力构建教育云安全体系是推动教育云服务标准建设和规范教育云发展的重要路径。实现教育云之间资源动态调配和按需使用，是对我国教育云建设和广泛应用提出的必然要求，积极推动数据经济赋能教育领域高质量发展。

参考文献：

[1] 梁冰峰，张瑶．学分银行框架下大数据与财务管理专业课程建设路径 [J]. 山西青年，2025(16):166-168.

[2] 王磊，门海，张涛．黑龙江省教育云的建设与应用 [J]. 现代教育技术，2019,29(2):107-112.

[3] 陈平，双锴，皇甫大鹏．基于 STRIDE 威胁模型的教育云安全风险评估研究 [J]. 中国教育信息化，2017(5):15-19.