 DOI: https://doi.org/10.26549/jxffcxysj.v3i14.5979

Research and Countermeasures on Cloud Security of Smart Campus

Jianbang Zhu

Anhui Business College of Vocational Technology, Wuhu, Anhui, 241003 China

Abstract

Nowadays, with the development of information age and the innovation of technology, people's production and life, mode of thinking and work concept have changed greatly. The informatization construction of colleges and universities should also seize the current opportunity, fully combine the advantages of cloud computing technology, strengthen the construction of smart campus network and enhance the integration of educational resources. Cloud computing technology is widely used, which brings great convenience to the campus and helps it create more benefits. However, cloud application faces many challenges and risks, such as security issues, which has become the focus of attention. This paper analyzes the cloud security problems of smart campus, and puts forward security protection and control measures.

Keywords

smart campus; cloud security requirements; cloud security issues

智慧校园云安全问题研究及对策

朱建帮

安徽商贸职业技术学院，中国·安徽 芜湖 241003

摘　要

现如今，随着信息化时代的悄然迈进以及技术手段的吐故纳新，人们的生产生活、思维方式以及工作理念都发生了巨大的改变。高校信息化建设也抓住当下机遇，充分结合云计算技术优势，强化高校智慧校园网络建设、增强教育资源的整合。云计算技术被广泛应用，给校园带来了很大便利，助力其创造更多的效益。然而，云运用方面面临着诸多挑战和风险，如安全问题。现结合智慧校园云安全问题，论文针对性地进行剖析，提出安全防护和控制措施。

关键词

智慧校园；云安全需求；云安全问题

1 引言

在高校智慧校园网中，云计算得到了快速发展及应用，其能快速提高工作效率、降低软件及硬件资源的投入，更好地为高校服务，但安全问题是不容忽视的首要问题。根据 CSA 发布的“十二大云安全威胁”报告显示，云环境下有着很多安全威胁，如数据泄露、身份验收以及凭证被盗、API 安全以及系统漏洞问题等，这些都威胁着云应用的安全性。所以云安全在高校中应用是一个非常重要的课题 [1]。

2 高校中云安全相关技术与安全需求

对于云计算服务类型来说，一般可分为三个层面，主要有 Iaas、Pass、Saas 三类，这三个层次组成了云计算技术层面的整体架构，高校中云安全技术简要介绍如下，见图 1。

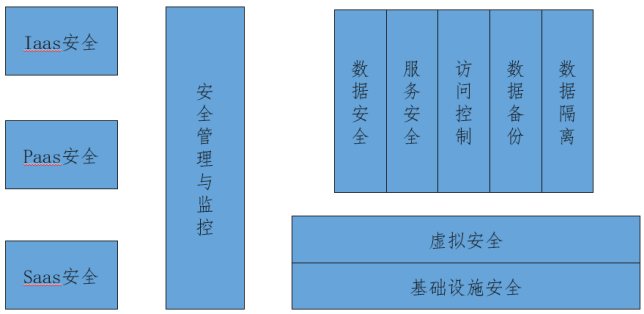

图 1 云计算技术层面的整体架构

2.1 云安全保障需求

云计算服务技术能实现信息以及服务资源的共享，与传统服务器安全防护有所差异，其边界防护、内部虚拟主机与内部虚拟化网络防护受到环境因素和其他因素的影响，面临

【项目名称】基于 MOOE 网络安全在线实验平台研究（项目编号：KJ2019A1008）。

 DOI: https://doi.org/10.26549/jxffcxysj.v3i14.5979

着各类安全问题。若想保障云环境的安全，要增强安全保障能力，如攻击行为感知能力以及网络行为预知能力，实现对重要业务以及数据的保护，防范黑客与不法人员的破坏。

2.2 数据安全需求

云计算主要利用网络资源提供服务，很多业务数据通过虚拟化技术手段，被存放在云端服务器位置。云计算技术具有分布式特点，在数据的利用方面，由于共同使用计算或者存储资源，使数据面临多重考验。在共享的环境下，加密技术对于数据的安全也没有办法，为了保证数据更好的安全，需要对数据进行隔离。若设置的安全隔离性能不完善，或者被非法用户攻击，极易造成数据安全问题，如访问机制不完善或者其他薄弱点的存在。在智慧校园的云平台中，数据的备份是特别需要的，数据放在哪里，哪里就有入侵的可能。如果一旦数据出现了丢失和攻击，可以及时对数据库进行还原，从而保障校园内部业务的正常使用 [2]。

3 智慧校园云安全问题的分析

3.1 数据丢失与泄露

智慧校园云安全问题以数据安全为主要内容，是备受关注的重中之重。用户的数据统一存放在云服务器上，如果受到入侵就可以看到每个用户的信息，对于用户而言，如何保证这些数据不被别人恶意利用就成了一个非常大的问题，因此就需要技术部门的不断完善。数据资源为核心资源，若数据信息泄漏，则会造成重大损失，怎样有效存储数据，避免数据丢失或损坏；怎样避免数据被非法访问或者被无故篡改；怎样对应用进行数据隔离；怎样避免数据服务被阻塞等都是需要关注的。

3.2 网络攻击

基于云环境下，云计算平台的用户、信息资源的高度集中，比较容易成为黑客攻击的目标，因此由于服务造成的破坏性将会大大超过传统的企业网络应用环境。很多程序都是通过网络开展，如攻击者运用应用层 DDOS 攻击、SSRF 或者其他攻击方式，实现对用户的阻止，使其不能正常访问，造成资源浪费；再如，内存浪费等，拖慢服务器运行速度，造成资源消耗，最终造成损失。

3.3 技术漏洞

近年来，云技术虽然快速发展，但是共享平台组件和应用程序有着很多安全漏洞，致使技术应用面临较大的危险，甚至会造成系统瘫痪。除此之外，云计算资源具有虚拟化特征，对传统安全策略的应用有着很大的阻碍，增加了安全认证的难度，恶意代码以及病毒的传播增加了安全问题的发生几率。

4 校园云安全防范的策略

4.1 Iaas 云主机安全防护

4.1.1 云主机操作系统安全

云主机操作系统应着重满足以下安全配置要求：身份鉴别、访问控制、安全审计、入侵防范。参考等级保护基本要求并结合攻防实践，构建操作系统安全框架，见图 2。

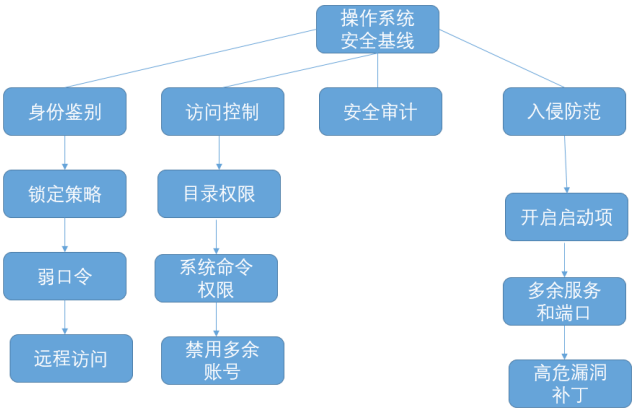

图 2 操作系统安全框架

4.1.2 云主机运行环境安全

云主机运行环境主要是指应用软件所依托的运行环境，这里针对 Web 应用服务器环境进行研究。Web 服务器采用 HTTP 协议提供 Web 信息浏览服务，功能扩展后可以支持脚本解析和业务逻辑处理，它是基于 Web 的应用软件不可缺少的运行环境。常见的 Web 应用服务器有 Apache、Tomcat、IIS、JBOSS、WebLogic 等。

Web 服务环境对 Web 应用安全影响非常大。可以从身份鉴别、访问控制、日志审计、信息泄漏以及入侵防范等方面加强 Web 服务运行环境安全。运行环境安全基线见图 3。

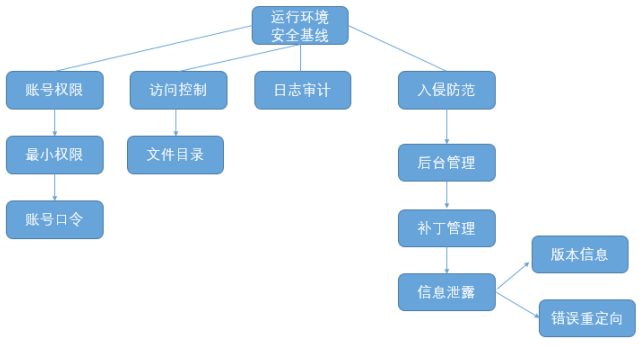

图 3 运行环境安全基线

 DOI: https://doi.org/10.26549/jxffcxysj.v3i14.5979

4.1.3 云主机应用系统安全基线

云主机运行环境部署好后，就可以开始部署应用系统。应用系统在上线前应进行安全评估和渗透测试，以尽早发现和修复应用软件安全漏洞。

4.2 采用物理安全技术

从云计算系统的应用实践来说，采取的安全防护措施要围绕环境安全进行，构建物理安全系统。实践中考虑温度和湿度等因素的影响，以保障云计算系统的应用安全，减少运行风险，实现安全运行。一般来说，云服务提供商会采取系列措施，保障运维环境的安全性，除了配置安全性较高的设备，包括温度控制器，还要配置支持不同环境的设备，如不间断电源或者其他设备，面对突变自然环境的影响。采取的设备维护措施，有助于保障设备处于长期稳定运行状态。实际应用中，要定期维护设备，记录设备运行存在的各类故障或者风险，为故障风险与处理提供依据。通过配置网络设备，提升云计算系统运行的整体性能。利用各类交换设备，配置具有冗余备份功能的网络设备以及网络链路等，辅助安全管理。实际应用中，当设备产生故障后，可以自动化恢复运行。利用企业网络的功能，如访问控制功能和安全检测功能等，保障云应用的安全。对于主机设备，通过多机负载模式实施安全防护，当主机产生故障，另外的主机还可以运行 [3]。

4.3 云安全数据库的安全

智慧校园云应用方面，要注重数据库的安全。中安威士根据多年数据安全的项目经验，总结出数据库面临的主要风险。

4.3.1 越权权限的滥用

数据库权限设置违反了“权限最小原则”在很多信息系统中比较普遍。如果这些超出的权限被滥用，则极易发生敏感数据泄漏事件。

4.3.2 合法权限滥用

系统中总是有一部分用户合法地拥有较大甚至是超级管理权限。如果这些权限被滥用，则极易发生严重后果。

4.3.3 权限盗用

由于商用数据库的用户认证方式主要为单一的口令方式，权限盗用容易发生，进而极易导致严重的数据泄漏事件。

4.3.4 数据库平台漏洞

数据库管理系统是个复杂的软件系统，从数据库厂家发布的补丁情况来看，数据库系统无一例外的具有严重的安全漏洞，如缓冲区注入漏洞或者认证、权限管理漏洞。这些漏洞极易被攻击者利用以窃取数据。

4.3.5 SQL 注入、缓冲区溢出风险

数据库本身不具备 SQL 注入攻击检测能力。通过 Web/APP 插入恶意语句，或者利用连接工具发动缓冲区溢出攻击，攻击者便有机会获得整个数据库的访问权限。

4.3.6 弱鉴权机制

商业数据库系统提供的基本的管理机制，主要是自主访问控制（DAC）和基于角色的访问控制（RBAC），并没有采用强制访问控制的方式（MAC），基于用户和数据的敏感级别来进行权限的鉴别，这容易使低密级用户访问到高密级的数据。

4.3.7 缺乏详尽审计

审计是每个数据库管理系统标配的安全特性，用于记录对数据的访问情况，从而形成对非法访问的威慑。而数据库自身的审计功能在可视化、智能化、入侵检测能力等方面能力较弱，通常无法满足实际的安全需求。

针对的数据库安全安全需求，为加强业务系统敏感信息的访问安全审计监控，防止数据库的高危操作，防止 SQL 攻击。中安威士给出基于数据库审计，数据库防火墙的综合数据安全解决方案，实现“可视”“可控”“合规”的需求，拟对存储敏感信息的数据库进行重点审计，核心数据库进行防火墙高危阻断。确保数据库访问合法合规，重点实现“数据库操作事后追溯取证”“数据库违规访问行为实时预警”“核心数据资产的防泄露、防篡改、防攻击”。

该方案概括来讲，就是把数据关进笼子，让数据的访问在阳光下进行，分为两个递进层次：第一是把数据关进笼子，通过数据库防火墙产品，基于自动学习和规则配置，生成细粒度的访问控制规则，阻断异常的查询和访问，防止敏感数据泄漏；第二是阻断异常的和违规的数据修改和删除操作，防止敏感数据被非法篡改，让数据的访问在阳光下进行。通过数据库审计产品，对数据的分布、性能、访问和活动情况进行全方位的监控和记录，做到哪个用户、在什么时间、访问了哪些数据库中的什么语句，便于事后审计和追查，及时

 DOI: https://doi.org/10.26549/jxffcxysj.v3i14.5979

发现数据的异常活动情况和风险，产生报警，输出可视化的报表，便于分析。

4.4 采用云安全监控作用

为了确保智慧校园云平台能快速、准确、安全而稳定的运行，监控系统是必不可少的，实施安全监控和审计措施，能获得较好的安全防护效果。采用监控手段，如日志监控，实现对相关事件的监控，防范与控制系统运行的安全。再如，利用性能监控，通过网络监控，促使云计算平台处于安全状态运行。采取审计措施，运用日志收集以及数据库审计等方式，采集相关数据信息，并且进行分析，为安全防护提供依据和参考，保障网络安全运行。目前 CMS（Cloud Monitoring Service）云监控服务是盛大云计算推出的一款针对云计算用户的监控服务。通过和云计算平台的整合，针对网络、系统、应用等内容提供可用性、用户体验和安全性方面的监控服务。保障云计算用户的业务稳定安全运行。当服务器发送故障时，及时给网站管理人员发送邮件和短信报警。第一时间了解网站状态，将故障时间降低到最小。同时，也提供其他服务，如追踪用户访问网站的速度、协助用户判断故障原因等。

4.5 云平台访问控制

智慧校园云平台云安全防护，采取访问控制措施，能获得不错的成效，具体措施如下。

4.5.1 网络安全访问控制

在云平台与用户之间，通过路由控制措施，搭建安全访问路径，增强网络安全。例如，采用限制管理终端访问网络设备措施或者采取安全访问控制措施等，实现对云应用的安全防护。

4.5.2 采取边界防护措施

明确边界防护与综合防护的边界，合理划分系统区域，增强访问控制，合理配置访问控制资源，结合运用防火墙措施或者其他设备控制措施，搭建完善的边界防护系统。当然访问控制系统有一个比较困难的点，那就是细粒度的权限控制。这一点在访问控制模型中你找不到答案，里面只在比较宏观的层面讨论了人和权限的关系。但细粒度的权限控制需求在实际的业务场景中又切实存在着。

例如，一个企业有若干台虚拟机，有一些虚拟机用作 webserver，而有一些虚拟机用作数据库，还有一些作为中间件服务器，Zookeeper 等，使用这些虚拟机的人各不相同，所以他们能看到并操作的虚拟机也应该得到严格的监管，否则可能会引起安全事故。访问控制的难点还包括身份的多样性、如何实现动态的授权体系。总而言之，云环境下的访问控制系统面临的挑战很多。

5 结语

综上所述，智慧校园云安全问题的有效防范，保障应用的安全性。论文结合常见的安全问题，总结了安全防护措施。在实践中，运用物理安全技术、云平台访问控制等，打造安全性能较好的防护系统，保障云应用的安全性。

参考文献

[1] 何华丽 . 智慧校园建设的无线网络安全问题分析 [J]. 数字通信世界 ,2018(06):221.

[2] 罗定福 , 李厦龙 , 吴权轩 . 无线智慧校园建设研究 [J]. 现代信息科技 ,2018(10):61-63+66.

[3] 孙利国 . 智慧校园建设中无线网络安全问题 [J]. 电子技术与软件工程 ,2018(02):212.