Computer Science and Application 计算机科学与应用, 2026, 16(6), 268-276
Published Online June 2026 in Hans. https://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2026.166226

Hans汉斯

零信任技术在高等院校中的应用研究进展

周　敏，陈伟杰，陈泽生*，冯李春，陈勇标，林川行

广州美术学院信息技术中心，广东　广州

收稿日期：2026年5月18日；录用日期：2026年6月22日；发布日期：2026年6月30日

摘　要

随着高等教育数字化转型的持续深化，云计算、移动办公与物联网技术的普及使得高校网络边界日趋模糊，传统基于物理边界的静态防护体系已难以适配开放多元的校园网络环境，更无法应对高频化、复杂化的网络攻击威胁，教育行业已成为全球网络攻击的重点受害领域，零信任安全范式为破解高校网络安全困境提供了核心解决方案。本文系统梳理了零信任技术的理论演进、核心原则与架构体系，结合高等院校的网络安全特性与场景化需求，全面解析了零信任技术在高校领域的全球应用进展、典型落地场景与国内外标杆实践案例，深入剖析了当前高校零信任建设的核心瓶颈与挑战。

关键词

零信任，高等院校，网络安全，访问控制，身份管理

Research Progress on the Application of Zero Trust Technology in Higher Education Institutions

Min Zhou, Weijie Chen, Zesheng Chen*, Lichun Feng, Yongbiao Chen, Chuanxing Lin

Information Technology Center, Guangzhou Academy of Fine Arts, Guangzhou Guangdong

Received: May 18, 2026; accepted: June 22, 2026; published: June 30, 2026

Abstract

With the continuous deepening of the digital transformation of higher education, the popularization of cloud computing, mobile office and Internet of Things technologies has made the network perimeter of universities increasingly blurred. The traditional static protection system based on physical

*通讯作者。

文章引用: 周敏, 陈伟杰, 陈泽生, 冯李春, 陈勇标, 林川行. 零信任技术在高等院校中的应用研究进展[J]. 计算机科学与应用, 2026, 16(6): 268-276. DOI: 10.12677/csa.2026.166226

perimeter can no longer adapt to the open and diversified campus network environment, let alone cope with the high-frequency and sophisticated cyber attack threats. As a result, the education sector has become a key victim of global cyber attacks, while the Zero Trust security paradigm provides a core solution to address the cybersecurity dilemma of colleges and universities. This paper systematically sorts out the theoretical evolution, core principles and architecture system of Zero Trust technology. Combined with the cybersecurity characteristics and scenario-based requirements of higher education institutions, it comprehensively analyzes the global application progress, typical implementation scenarios, and domestic and international benchmark practice cases of Zero Trust technology in the higher education field, and deeply dissects the core bottlenecks and challenges of current Zero Trust construction in colleges and universities.

Keywords

Zero Trust, Higher Education Institutions, Cybersecurity, Access Control, Identity Management

1. 引言

研究背景与意义

高等教育机构正处于数字化转型的关键时期，云计算、大数据、人工智能等新技术的广泛应用为教学、科研和管理带来了前所未有的便利，但同时也使高校面临着日益严峻的网络安全挑战。传统的基于网络边界的安全防护模式在面对无边界的网络环境时显得力不从心，零信任技术应运而生，成为解决高校网络安全困境的重要技术路径[1]。

零信任是一组不断演进的网络安全范式，它将网络防御的重心从静态的、基于网络的边界转移到了用户、设备和资源上。零信任架构使用零信任原则来规划企业基础设施和工作流，其核心特征是取消了传统基于用户的物理或网络位置而授予用户账户或者设备权限的隐式信任[2]。这一理念的提出，标志着网络安全防护思想的根本性转变。

从发展历程来看，零信任理念起源于 2003 年的耶利哥论坛上提出的一种“去边界化的网络安全架构”，主张去除内网的隐形信任[3]。Forrester Research 的分析师 John Kindervag 在 2010 年正式提出了零信任模型，其核心是对网络中的所有实体持续验证身份与权限，不因位置、历史行为或网络归属而默认信任[4]。Google 公布的 BeyondCorp 实践，首次将访问控制从网络边界转移到用户和设备身份[5]。2020 年，NIST 发布《零信任架构》(正式版)作为建立零信任架构的统一框架[2]，为零信任技术的标准化实施奠定了基础。表 1 详细描述了国内外知名机构关于零信任模型的描述及相关报告。

高等院校作为知识创新和人才培养的重要基地，其网络安全具有特殊的重要性。一方面，高校存储着大量敏感数据，包括学生个人信息、科研成果、财务信息等；另一方面，高校网络环境具有开放性、多样性和复杂性的特点，师生、研究人员、访客等不同群体需要从各种设备和位置访问校内资源。这些特点使得高校成为网络攻击者的重点目标，数据显示，97%的教育机构经历过钓鱼攻击，勒索软件攻击影响了超过 8000 所学校[11]。

高等教育数字化转型带来的安全挑战已成为全球高校的共性痛点，零信任技术作为破解传统边界防护失效问题的核心范式，其在高校场景的应用已进入规模化落地的关键阶段。为此，本文梳理零信任技

术在高等院校中的应用研究进展，分析技术发展趋势，总结实施经验，为高校网络安全建设提供理论指导和实践参考。

Table 1. Descriptions and reports on the zero trust model from prestigious domestic and international institutions
表 1. 国内外知名机构关于零信任模型的描述及报告

零信任相关模型或报告名称	发布机构	年份
零信任成熟度模型 2.0 [6]	美国网络安全与基础设施安全局	2023
零信任和可信身份管理[7]	美国国家安全电信咨询委员会	2022
拥抱零信任安全模型[8]	美国国家安全局	2021
网络安全先进技术与应用发展系列报告——零信任技术[9]	中国信息通信研究院安全研究所，奇安信科技集团股份有限公司	2020
零信任发展研究报告[1]	中国信息通信研究院云计算与大数据研究所	2023
零信任发展洞察报告[10]	中国通信标准化协会云计算标准和开源推进委员会，中国信息通信研究院云计算与大数据研究所	2024

2. 零信任技术基础理论

2.1. 零信任核心概念与原则

零信任的核心原则是“永不信任，始终验证”，这一原则彻底颠覆了传统网络安全的基本假设。零信任架构基于三个核心支柱：明确验证、最小权限访问和假设已被攻破[12]。明确验证要求基于所有可用数据点(如用户身份、位置、设备健康状况、服务或工作负载、数据分类和异常情况)进行持续的身份验证和授权。这意味着无论是内部用户还是外部用户，每次访问请求都必须经过严格的验证流程，不能因为其位于内网就给予信任。最小权限访问是通过即时和刚好足够的访问、基于风险的自适应策略和数据保护来限制用户访问，以帮助保护数据。这一原则确保用户只能访问其完成任务所必需的资源，最大限度地减少了攻击面。假设已被攻破通过按网络、用户、设备和应用意识分割访问来最小化泄露的爆炸半径并防止横向移动。这一原则要求安全架构设计必须考虑到即使攻击者已经渗透到网络内部的情况，通过微分段等技术限制攻击者的横向移动能力。

2.2. 零信任架构设计理念

零信任架构的设计理念体现了从边界防护向身份为中心的安全模型的根本性转变。传统的网络安全模型基于“城堡与护城河”的理念，认为只要保护好网络边界，内部就是安全的。然而，随着云计算、移动设备和物联网的普及，这种静态的边界防护模型已经无法适应新的安全需求[13]。

零信任架构采用控制平面和数据平面分离的设计理念[14]。控制平面用于各种基础设施组件维护和配置资产、判断、授予或拒绝资源访问，以及执行建立资源之间通信路径所需的任何操作；数据平面用于软件组件之间的实际通信。这种分离设计提高了系统的灵活性和可扩展性，使得安全策略的制定和执行可以独立进行。零信任架构包含多个关键技术组件，这些组件协同工作，实现“永不信任，始终验证”的安全目标。图 1 描述了零信任技术体系框架。

身份安全基础设施是零信任架构的核心基石与底层支撑，为整个体系提供标准化的身份治理、密码学安全与资源管理能力，是实现“以身份为中心”安全模型的核心前提，包含身份管理、认证管理、基础安全、资源管理和公钥基础设施共五大核心子模块。身份管理承担全量实体的身份全生命周期治理职能，覆盖高校场景下各类人员的统一身份建模、身份同步与生命周期管控，实现“一个实体、一个身份、全

域可溯”。认证管理提供多维度、自适应的身份核验能力，为每一次访问请求提供可靠的身份真实性校验。基础安全为整个零信任体系提供基础安全基线与合规能力，包括终端安全基线校验、密码策略管控、安全审计日志标准化、合规规则配置等。资源管理针对防护目标进行全量资产梳理与标准化管理，为精细化访问控制提供资产依据。公钥基础设施为全架构提供密码学安全支撑，保障零信任体系内所有通信与操作的不可伪造、不可篡改。

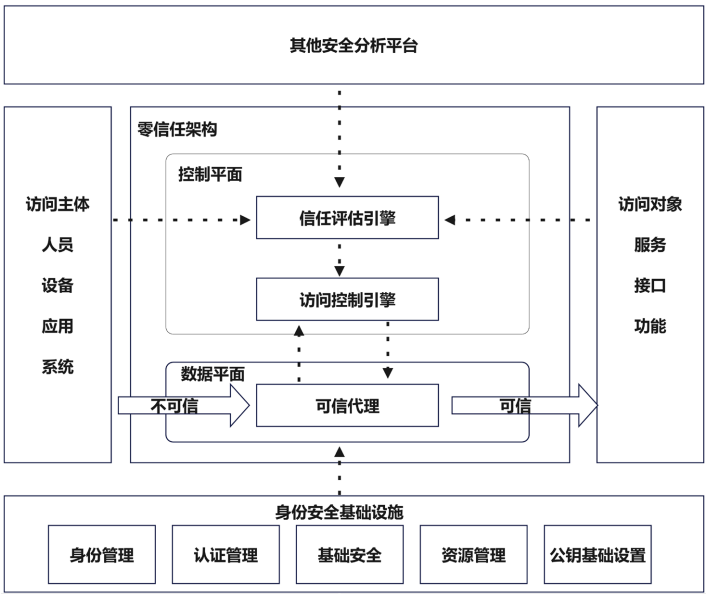

Figure 1. Zero trust technology architecture framework [15]
图 1. 零信任技术体系框架[15]

控制平面是零信任架构的中枢决策大脑，承担信任评估、权限判定、策略下发的核心职能，是实现“持续验证、动态授权”的核心，包含信任评估引擎和访问控制引擎。信任评估引擎汇聚三大维度的核心数据：一是访问主体(人员、设备、应用、系统)的身份属性、设备健康状态、历史访问行为等基础数据；二是访问对象的敏感等级、合规要求、防护级别等资源属性数据；三是第三方安全分析平台同步的全局威胁情报、异常行为告警、攻击特征库等外部数据。信任评估引擎基于多维度特征构建动态信任评估模型，对每一次访问请求进行实时、全生命周期的信任度量化计算，表 2 是部分信任评估计算方法。访问控制引擎是零信任权限管控的决策执行单元，承接信任评估引擎的输出结果，完成最终的访问决策与策略下发。该引擎严格遵循最小权限原则，融合基于角色的访问控制(RBAC)、基于属性的访问控制(ABAC)模型，结合预设的安全策略，为本次访问请求生成精准的访问控制决策

数据平面是零信任架构的策略执行层，核心组件为可信代理，是访问主体与访问对象之间唯一的通信通道，承接控制平面下发的访问控制策略，承担访问流量的转发、加密、管控与审计职能。仅放行经控制平面完整验证、明确授权的访问流量，对所有未授权的访问请求完全阻断；同时通过代理模式隐藏访问对象的真实网络地址与服务端口，使外部攻击者无法通过扫描发现目标资产，大幅缩小校园网络的攻击面。

其他安全分析平台是零信任架构的能力拓展模块，也是动态信任评估的重要数据来源，可无缝对接用户与实体行为分析(UEBA)、终端检测与响应(EDR)、安全信息与事件管理(SIEM)、威胁情报平台等第三方安全系统，为信任评估引擎提供全局威胁情报、异常行为告警、终端失陷检测、攻击事件溯源等补

充数据，实现零信任架构与高校现有安全体系的深度集成、能力互补，进一步提升动态信任评估的精准度与攻击检测的时效性。

Table 2. Trust score calculation methods in partial literature
表 2. 部分文献信任评分计算方法

参考	公式	描述
[16]	$FC_t = \sum_{flowcount=1}^{n} (b_s + b_d)$	假设访问源在时刻 t 发起对访问对象的访问动作。时刻 t 的访问可信指数设置为 FC_t，n 表示访问动作发起的总数，b_s 表示为访问源的环境动态熵值，b_d 表示为访问源到访问对象之间的网络威胁指数。
[17]	$DTV = \sum W_a \cdot S_a$	将用于信任评估的属性的集合用 A 表示。对于属性 $a \in A$，若访问主体具备该属性，则其状态值 S_a 为 1，否则为 0。由管理员根据实际需要设定每个要素所对应的权重 W_a，每次访问时的直接信任评分为 DTV。
[15]	$T = w_1F_1 + w_2F_2 + \cdots + w_nF_n$	F_i 表示第 i 个特征(如登录频率、地理位置、设备类型等)，w_i 是对应的权重。信任评分 T 用于动态调整访问权限。

3. 高等院校网络安全需求分析

高等教育机构的网络安全形势日趋严峻，面临着来自多个维度的安全威胁。根据最新统计数据，教育部门在 2025 年第二季度平均每周面临 4388 次网络攻击，同比增长 31% [18]。这一数据充分说明了高校网络安全防护的紧迫性。

3.1. 高校网络安全需求

与政务、金融等强监管、高封闭性的行业不同，高等院校的网络空间承载着学术交流开放共享的核心需求，其网络环境兼具用户群体多元、网络架构开放、敏感数据集中、合规要求严格的多重特征，这也使得高校的网络安全需求无法直接套用通用行业的标准化建设框架，呈现出鲜明的行业专属属性。

首先是大规模、多样化的用户群体带来的精细化身份治理需求。高校网络环境包含学生、教职员工、研究人员、供应商、访客等不同群体，每个群体都有不同的安全意识和访问需求。这种多样性增加了身份管理和访问控制的复杂性，需要建立精细化的身份治理体系。

其次是开放的网络架构带来的攻击面管控需求。高校网络通常具有开放性特征，包括开放的 Wi-Fi、公共实验室、访客访问网络，以及用于研究、学生组织和行政单位的多个子网。这种开放性虽然有利于学术交流和资源共享，但也增加了网络攻击的入口点。

此外，高校存在敏感数据的管理需求。高校存储着大量敏感数据，包括学生记录、财务信息、健康数据、知识产权和研究数据集。这些数据不仅数量庞大，而且价值较高，容易成为网络犯罪分子的目标。

在教育领域，高校有严格的合规要求。高校需要遵守各种数据保护法规，包括网络安全法、个人信息保护法等，业务系统需要按照合规需求完成网络安全等级保护测评和备案。这些法规对数据的收集、处理、存储和共享都有严格的要求。

3.2. 高校现有安全架构的局限性

传统的高校网络安全架构基于边界防护理念，存在明显的局限性。首先，静态的网络边界已经模糊。随着云计算、移动设备和物联网的普及，高校的网络边界变得越来越模糊，传统的防火墙和 VPN 等边界防护措施已经无法有效应对无边界的安全威胁。其次，内网安全风险被忽视。传统安全模型假设内网是可信的，但实际上，许多安全事件源于内部威胁或已突破边界的外部攻击者。高校网络的开放性和复杂

性使得内部威胁的防范更加困难。此外，身份管理粗放，传统的身份认证系统通常只进行一次认证，无法应对动态变化的安全需求。高校的多角色、多场景访问需求要求更加精细和动态的身份管理机制。传统网络安全架构也缺乏持续监控能力。传统安全架构往往是被动的，只有在发生安全事件后才能发现问题。高校需要的是主动的、持续的安全监控和预警能力，能够及时发现和应对安全威胁。表 3 详细描述了传统的高校网络安全架构存在的问题以及具体表现场景，同时给出了技术/架构缺陷归因。

Table 3. Problems, descriptions, scenarios and root cause analysis of traditional cybersecurity architectures
表 3. 传统网络安全架构的问题、描述、场景和归因

局限性维度	核心问题描述	具体表现场景	技术/架构缺陷归因
边界防护失效	静态边界架构被打破，防护范围失控	大量师生、科研设备通过居家网络、公共WiFi 接入校园；云端教务系统、SaaS 科研平台脱离传统防火墙管控；物联网设备大量接入，未被传统边界防护覆盖。	原有的 IP 地址层边界随云计算、移动办公及 IoT 普及变得日趋模糊，传统防火墙/VPN 无法构建有效的防护屏障，导致外部攻击可轻易穿透外围防线。
内网信任风险	基于“内网可信”的假设存在重大安全隐患	校内宿舍、公共机房设备被劫持后横向渗透全校园网；内部员工误操作或恶意泄露敏感数据；攻击者突破边界后利用内网信任关系进行横向移动。	信任假设错误：高校网络具有高度开放性和复杂性，内网并非绝对安全，传统架构无法防范内部人员误操作、恶意攻击或已沦陷终端的深层渗透。
身份管控滞后	身份认证静态、粗放，无法适配多元身份体系	单一密码认证易被破解，且一旦认证通过，便长期授权；缺乏基于设备、位置、行为的动态身份验证机制。	认证机制低效：传统身份管理仅支持单因子认证，且缺乏对访问上下文的实时校验，无法应对高校复杂的多角色、多场景访问需求及身份盗用风险。
被动防御滞后	缺乏持续、主动的安全监控与响应能力	仅在攻击发生后或通过安全设备日志被动溯源，无法实时预警；缺乏对全网流量和用户行为的持续分析与异常检测 安全响应周期长，无法快速阻断攻击蔓延。	防御模式被动：传统架构多为事后响应，缺乏主动的、持续的监控与预测能力，难以应对日益隐蔽和快速演变的高级持续性威胁。

4. 零信任技术在高校的应用进展

4.1. 高校零信任技术整体发展趋势

近年来，零信任技术在高等教育领域呈现出快速发展的态势。根据最新市场研究报告，47%的大学和39%的制造企业正在向零信任过渡，特别是为了保护知识产权和数字学习系统[19]。这一数据表明，零信任技术已经从概念验证阶段进入了规模化部署阶段。然而，教育行业的零信任成熟度仍然偏低。调研显示，仅 26%的教育机构评估其零信任成熟度为高级或最优，38%处于初始阶段，18%根本没有开始零信任建设[20]。这说明虽然零信任技术受到了广泛关注，但在实际部署和成熟度方面仍有很大的提升空间。

从技术采用趋势来看，80%的高等教育组织已制定零信任策略，但真正大规模实施的数量急剧下降[21]。这一现象反映了零信任技术在高校实施过程中面临的挑战，包括技术复杂性、成本、人员培训等问题。

根据法国网络安全权威杂志 Global Security Magazine 发布的调查显示，97%的企业表示已实施零信任举措或计划在未来 12~18 个月内实施，而 2018 年这一比例仅为 16%，在四年间增长了 500%以上[22]。尽管上述调研数据以企业为核心统计对象，但高校作为承载海量师生敏感信息、持续面临高强度网络攻击威胁的关键社会组织，加快落地零信任安全架构已是保障校园网络安全的必然选择，更是行业安全升级的大势所趋。

4.2. 零信任在高校的具体应用场景

作为支撑高校数字化校园平稳运行的核心安全范式，零信任技术的落地应用始终与高等院校的业务场景深度绑定。区别于通用行业的标准化部署模式，高校开放办学的属性、多元复杂的业务体系，决定了零信任技术的应用需精准适配不同场景的专属安全需求，其落地场景已覆盖教学科研、行政运维、校园服务等高校运行的全维度。

例如，对于智慧校园数据中心安全，通过模拟平台和相关测试实例，利用持续的身份识别、行为分析和业务流量识别等技术，结合校园网中的业务需要，对基于零信任架构安全体系的高校智慧校园数据中心进行实测。结果表明，基于零信任架构思想设计的网络安全体系能根据环境策略的变化而使用多因子认证，实现持续的动态验证，降低资源访问的安全风险[23]。在 API 数据安全架构方面，构建基于零信任的 API 数据安全架构，高校能够降低内部数据泄露的风险，提升整体安全防御能力。这种架构特别适用于需要对外提供数据服务的高校，如在线教育平台、科研数据共享平台等[24]。在网络安全运维方面，针对高校网络运维面临的日益严峻的安全挑战，张震提出了零信任 API 网关解决方案。该方案基于 APISIX 架构，遵循零信任原则，强调身份认证和持续信任评估，通过微服务架构，构建了一个全面的安全防护体系[25]。

5. 高校零信任技术应用案例分析

5.1. 高校零信任实践

随着零信任架构在高等教育领域的应用逐步深化，国内知名高校已率先开展零信任技术的落地实践，通过结合自身业务场景与安全需求，探索出适配高校开放办学环境的零信任建设路径，形成了一批具有行业示范意义的成功案例。

清华大学构建了高校零信任安全接入体系，实现远程接入能力的升级，完成了新一代高校零信任安全架构的转型。该方案基于零信任架构，实现统一身份认证管理，持续对访问校内业务系统的终端状态、访问行为、网络流量进行实时监测，为高校提供全方位防护[26]。清华大学零信任的动态信任评估，包括身份可信、终端可信、行为可信 3 个核心能力。

厦门大学作为国家“双一流”建设高校，基于 SASE 架构打造了零信任统一接入平台。该平台依托全球 2800 多个加速节点，为全校师生提供安全、高速的接入服务。目前，零信任平台已为校内超 7.3 万教职工提供校外安全接入服务，上线应用 400 多个，最大并发设备数超过 1000 台，实现全域终端支持。该平台的成功实施有效解决了海外师生访问国内系统延迟高、研究生远程操作实验室设备卡顿、VPN 频繁掉线等问题[27]。厦门大学与清华大学所使用的零信任安全厂商相同，因此，对于身份可信、终端可信、行为可信构成了零信任动态信任评估。

河南科技大学采用 aTrust 构建了可信访问、简化运维、智能权限的零信任安全架构。该架构以身份为中心，通过实施最小权限访问、动态的访问控制和持续的信任评估，更大限度地缩小业务暴露面，为师生访问业务提供了“端到端”的全流程保护。aTrust 零信任核心理念是以身份为中心，基于不同访问用户的身份，最小化授权访问权限。河南科技大学的实践表明，零信任技术不仅提升了网络安全性，还简化了运维管理，提高了工作效率[28]。

西安电子科技大学同样采用 aTrust 在零信任系统建设方面也取得了重要进展。该校的零信任系统对接了校内统一身份认证平台，支持二次认证机制。新设备首次登录零信任系统需完成二次验证，确保了设备接入的安全性[29]。这种与现有身份系统的无缝集成，既保护了投资，又提升了安全防护能力。

5.2. 高校零信任技术实施经验总结

当前零信任技术在高等教育领域的应用，已逐步从概念验证走向规模化落地，国内外高校的先行探索，为行业积累了宝贵的一手实践经验。结合前文梳理的标杆案例建设路径、落地成效与共性特征，可提炼出高校零信任建设的核心成功经验。

制定清晰的实施策略。成功的高校都制定了明确的零信任实施路线图，包括短期目标和长期愿景。例如，先从身份认证和访问控制入手，逐步扩展到网络分段和数据保护。这种渐进式的实施策略既降低了风险，又能够快速看到效果。

注重技术选型和集成。高校在选择零信任技术时，充分考虑了与现有系统的兼容性。例如，清华大学、西安电子科技大学等都选择了与现有身份认证系统集成的方案，避免了大规模的系统改造。同时，许多高校选择了模块化的零信任解决方案，可以根据需求逐步部署。

重视用户体验设计。零信任技术的成功实施离不开良好的用户体验。高校在部署零信任系统时，特别注重简化用户的操作流程。例如，通过单点登录、智能认证等技术，使用户在享受安全保护的同时，不会感到操作复杂。厦门大学的实践表明，良好的用户体验是零信任系统成功的关键因素之一。

建立完善的运维体系。零信任系统的有效运行需要专业的运维团队和完善的管理制度。高校普遍建立了专门的零信任运维团队，负责系统监控、策略调整、事件响应等工作。同时，制定了详细的操作规程和应急预案，确保系统能够稳定运行。

加强安全意识培训。技术措施只是零信任架构的一部分，人的因素同样重要。高校通过各种形式的培训和宣传，提高师生的安全意识，使其理解和配合零信任系统的实施。例如，定期举办安全讲座、发布安全提示、开展应急演练等。

6. 结论

本研究系统综述了近年来零信任技术在高等院校中的应用研究进展，得出系列核心结论，零信任技术正成为高校网络安全建设的核心选择，面对日趋严峻的网络安全威胁，传统边界防护模型已无法适配高校多元场景的安全需求，该技术以“永不信任，始终验证”为核心原则，通过身份认证、微分段、持续监控等技术组件为高校构建全方位安全防护体系。当前高校零信任技术应用虽呈快速发展态势，但整体成熟度仍有较大提升空间，尽管 80%的高等教育组织已制定零信任建设策略，仅 26%的教育机构评估自身零信任成熟度达高级或最优水平，该技术在高校的应用仍处于发展阶段，需在技术、管理、人员等多维度持续优化；清华大学、厦门大学等知名高校的落地实践，已形成涵盖清晰策略规划、合理技术选型、兼顾用户体验设计、完善运维体系与持续安全培训的宝贵经验。针对高校零信任技术的应用，建议高校结合自身实际制定分阶段、分层次的实施策略，优先覆盖核心业务系统并兼顾存量系统兼容性。在守住安全底线的同时优化用户访问体验，稳步推进零信任架构落地。

基金项目

中国高校产学研创新基金(2024MU039)；广州美术学院体制机制改革项目(20231125-029)。

参考文献

[1] 中国信通院 CAICT. 中国信通院发布《零信任发展研究报告(2023 年)》 [R/OL]. 2023-08-28. https://mp.weixin.qq.com/s/xdNw_Xb2obUu6E1nhB1sSg, 2025-11-19.

[2] 美国国家标准与技术研究院, 美国商务部. 《NIST 零信任架构(正式版)》 [R/OL]. https://mp.weixin.qq.com/s/5oQgaoBxKU9FYeWIvg9P0Q, 2026-04-10.

[3] 张嘉伟, 蒋亚丽, 王进. 基于 UEBA 的零信任安全体系架构设计与实现[J]. 信息安全与通信保密, 2024(11): 71-84.

[4] 赵敏, 瞿康健. 零信任架构及其技术应用研究综述[J/OL]. 信息网络安全: 1-18. https://link.cnki.net/urlid/31.1859.TN.20260319.1852.002, 2026-06-17.

[5] 秦文远, 安宁. 基于零信任架构的线上培训安全平台研究[J]. 网络安全与数据治理, 2025, 44(5): 10-16.

[6] (2023) Zero Trust Maturity Model Version 2.0. Cybersecurity and Infrastructure Security Agency, Cybersecurity Division. https://www.cisa.gov/zero-trust-maturity-model

[7] NSTAC (2022) Zero Trust and Trusted Identity Management. https://www.cisa.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20Zero%20Trust%20and%20Trusted%20Identity%20Management%20%2810-17-22%29.pdf

[8] National Security Agency (2021) Embracing a Zero Trust Security Model. National Security Agency. https://cloudsecurityalliance.org/zt/resources/embracing-a-zero-trust-security-model

[9] 中国信息通信研究院, 奇安信科技集团股份有限公司. 网络安全先进技术与应用发展系列报告——零信任技术[R/OL]. https://pdf.dfcfw.com/pdf/H3_AP202008141398426442_1.pdf, 2026-05-07.

[10] 云计算与大数据研究所. 《零信任发展洞察报告(2024)》正式发布! [R/OL]. https://mp.weixin.qq.com/s/KApA0efglDE2P0cw75Ldbg, 2025-11-19.

[11] SentinelOne (2026) Cybersecurity in Higher Education: Risks, Best Practices & Frameworks. SentinelOne. https://www.sentinelone.com/cybersecurity-101/cybersecurity/cybersecurity-in-higher-education/

[12] Microsoft Security (2026) What Is Zero Trust Architecture? https://www.microsoft.com/en-us/security/business/security-101/what-is-zero-trust-architecture

[13] Kerman, A., Souppaya, M., Scarfone, K., *et al*. (2022) Implementing a Zero Trust Architecture: 1800-35E. National Institute of Standards and Technology.

[14] 张文柱, 石亚坤, 高杜梅. 边云协同下的计算卸载与资源分配策略[J]. 计算机工程与科学, 2026, 48(3): 398-410. https://kns.cnki.net/KCMS/detail/detail.aspx?dbcode=CJFQ&dbname=CJFDAUTO&filename=JSJK202603003

[15] 曾宇. 基于零信任架构的信息化系统数据访问控制与安全隔离技术[J]. 电子元器件与信息技术, 2025, 9(3): 163-166.

[16] 张宇南, 洪超, 杨祎巍, 等. 基于零信任网络安全的身份验证与授权的新型架构研究[J]. 网络安全技术与应用, 2025(7): 19-23.

[17] 金志刚, 林亮成, 陈旭阳. 行为异常检测技术在零信任访问控制中的应用[J]. 信息安全研究, 2024, 10(10): 921-927.

[18] Rohann@Checkpoint.Com (2025) Global Cyber Attacks Surge 21% in Q2 2025—Europe Experiences the Highest Increase of All Regions. https://blog.checkpoint.com/research/global-cyber-attacks-surge-21-in-q2-2025-europe-experiences-the-highest-increase-of-all-regions/

[19] (2026) Zero-Trust Security Market Size, Share, Growth, and Industry Analysis. https://www.industryresearch.biz/market-reports/zero-trust-security-market-108775

[20] Viano, A. (2026) Why Are Universities Slow to Adopt Zero Trust? https://edtechmagazine.com/higher/article/2024/07/why-are-universities-slow-adopt-zero-trust

[21] Chris Liou, N. (2025) Network Security in Higher Ed: The Importance of Zero Trust. https://www.ecampusnews.com/cybersecurity/2025/07/16/network-security-in-higher-ed-the-importance-of-zero-trust/

[22] OKTA (2026) Etude okta: Le zéro trust à l'agenda des conseils d'administration, son adoption ayant augmenté de 500%. https://www.globalsecuritymag.fr/Etude-Okta-Le-Zero-Trust-a-l,20220919,130010.html

[23] 贾万祥, 张平华. 零信任架构下的智慧校园安全性实测技术[J/OL]. 鄂州大学学报, 2024, 31(1): 99-101, 112.

[24] 殷浩翔. 面向智慧视听的省级平台网络安全防护体系研究与应用——以"视听四川"平台为例[J]. 广播电视信息, 2026, 33(3): 79-82.

[25] 张震. 零信任 API 网关在高校网络运维中的应用[J]. 无线互联科技, 2024, 21(23): 69-72, 93.

[26] 网宿科技 x 清华大学|构建高校零信任安全接入体系[EB/OL]. 2022-10-13. https://www.wangsu.com/news/content/news/3112, 2026-04-13.

[27] 厦门大学 x 网宿 SASE: 重塑百年学府安全边界[EB/OL]. 2025-09-11. https://www.wangsu.com/news/content/productupdates/4009, 2026-04-07.

[28] 河南科技大学: 零信任助力降本增效护安全, 满足数字化转型安全建设需求[EB/OL]. 2022-12-07. https://www.sangfor.com.cn/case/1670231025432, 2026-04-13.

[29] 校园远程访问体验与安全双重升级[EB/OL]. 2026-03-31. https://xxzx.xidian.edu.cn/info/1396/4183.htm, 2026-04-15.