基于零信任架构的线上培训安全平台研究*

秦文远，安　宁

（国务院国有资产监督管理委员会干部教育培训中心，北京　100053）

摘　要：新时代数智化技术的快速发展，使线上培训成为企业宣传企业精神、学习新技术的重要抓手。在线上教育培训应用广泛的背景下，以保障平台全流程支持培训业务开展为研究主线，依托现有零信任架构的理念，构建以可信终端环境感知、可信网络环境感知、可信代理、动态访问控制、信任评估、数据库细粒度访问控制六位一体的安全平台。通过实时感知环境状态，动态赋予用户最低权限，持续监督用户行为，让平台运行时达到持续验证、动态授权、全局防御的目标。平台在信任评估模块中引入自注意力机制，提高信任评估效率，保障培训平台安全运行，为培训组织单位构建信息安全堡垒。

关键词：线上培训；零信任安全架构；信任评估；数据库安全策略

中图分类号：TP309　　**文献标识码：**A　　**DOI：**10. 19358/j. issn. 2097 - 1788. 2025. 05. 002

引用格式：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.

Research on online training security system based on zero-trust architecture

Qin Wenyuan，An Ning

（SASAC Education and Training System，Beijing 100053，China）

Abstract：The rapid development of digital intelligence technology in the new era has made online training an important tool for enterprises to publicize their corporate spirit and learn new technologies. In this paper，against the background of the extensive application of online education and training，with the main research line of guaranteeing the platform′s full-process support for training business，relying on the concept of the existing zero-trust architecture，we construct a six-pronged security platform with trusted terminal environment awareness，trusted network environment awareness，trusted agent，dynamic access control，trust assessment，and fine-grained access control of the database. The platform senses the environment state in real time，dynamically grants users the lowest privilege，continuously monitors user behavior，and enables it to achieve the goals of continuous verification，dynamic authorization，and global defense during operation. The platform introduces the self-attention mechanism in the trust assessment module to improve the efficiency of trust assessment，ensure the safe operation of the training platform，and build an information security fortress for the training organizations.

Key words：online education and training；zero-trust security architecture；trust assessment；database security policy

0　引言

随着信息化技术的发展，线上培训方式以不限场地、沟通迅捷的优势被广泛应用，逐渐成为常态化培训模式。但线上培训涉及用户认证、数据传输、权限管理、内容保护等复杂业务逻辑，面临的网络威胁也逐渐增多。例如，远程用户、多终端接入导致传统网络边界模糊化，敏感课程内容、用户隐私数据易被窃取或滥用等安全问题时有发生，传统安全模型逐渐在线上培训领域暴露出局限性。

零信任架构对任何用户、网络均不信任，所有用户均需通过身份验证后才可获得最低权限，且平台动态监督用户行为，保障从终端到数据库的安全性。零信任架构的安全理念逐渐被用户认可，成为线上培训平台未来构筑安全防线的重要抓手，为线上培训提供更灵活的细粒度安全防护手段。

*基金项目：国务院国有资产监督管理委员会干部教育培训中心（中共中央党校国务院国有资产监督管理委员会分校）科研项目（25GZW0308）

1 背景介绍

1.1 线上培训平台现状

数智化技术的快速发展，为各企业带来全新的管理和经营理念。线上培训是高效传播企业文化、先进技术的方法，企业的培训需求正在逐年增加[1]。为满足大批量学员的培训需求，很多单位、机构普遍应用线上培训平台保障线上培训业务稳定运行[2]。在此过程中，培训机构通过端口映射或使用 VPN 建立远程网络通道，将业务系统开放至公网访问。但无论哪种方式，都会向互联网开放高敏感业务数据。另外，线上培训系统允许学员、讲师、管理员使用手机、电脑、平板等各类用户终端设备随时随地访问和调配资源，接入培训平台和网络的实体更加多样化[3]。硬件设备多样、用户权限繁杂、数据多层交叉是培训平台中实体多样性的重要原因。复杂多样的终端接入设备和不同身份权限混杂，使线上培训系统的防护设计复杂化，对网络安全防火墙的构建造成困难。

1.2 线上培训平台安全风险

在新技术发展背景下，线上培训平台面临的身份冒用与隐私侵犯、黑客攻击与服务中断、数据泄露与钓鱼攻击等安全问题也逐渐发生变化。

在身份冒用和隐私侵犯方面，攻击者通过钓鱼邮件、暴力破解等方式窃取用户账号，冒充学员或讲师进行非法操作，达到篡改成绩、窃取课程内容的目的。而在新背景下，攻击者使用 AI 生成的虚假身份（如 Deepfake 视频）绕过指纹、人脸等生物或密码验证关卡，直接窃取数据库信息。

在黑客攻击与服务中断方面，攻击者通过分布式拒绝服务攻击（DDoS）瘫痪线上平台，导致课程中断、考试延误。而在新背景下攻击者往往通过结合物联网设备进行大规模的僵尸网络攻击，增加平台防御难度。

在钓鱼攻击和数据泄露方面，攻击者针对学员或讲师发送钓鱼邮件、虚假课程链接，诱导用户输入账号密码或下载恶意文件。在新背景下，攻击者使用 AI 通过模仿讲师语气、伪造课程通知生成高度仿真的钓鱼内容，用户点击后即会泄露账号信息。

日益多样、复杂的攻击手段也成为限制线上培训发展的羁绊，在线上教育培训被广泛应用的背景下，应该融入零信任理念，着力提升安全架构防护水平，从学员、设备、培训业务之间勾画出基于身份的细粒度虚拟边界，创建内外网一体的培训数字平台[4]。

1.3 零信任架构介绍

1.3.1 零信任架构研究现状

零信任概念自 2010 年提出以来，引起了国外政府机构、科技巨头的重视，部分国家陆续发布相关政策支持零信任技术的发展和应用[5]，如表 1 所示。

从表 1 可以看出，美国、加拿大、新加坡等国已陆续将零信任架构部署至政府办公领域。在政策影响下，谷歌、微软等科技巨头也接续开展大规模实践，例如谷歌的 BeyondCorp 项目首次将访问控制从网络边界转移到用户和设备身份[6]；微软结合零信任策略推出云身份验证和访问控制解决方案（Microsoft Entra ID）[7]。国外零信任架构起步早于国内，强调身份验证、动态访问控制与数据加密。

国内以政策驱动发展，发布一系列安全标准、参考架构、洞察报告等，持续开展网络安全项目建设，表 2 是近几年国内零信任理念发展情况。

表 1 国外零信任理念支持政策

名称	政策发布时间和组织	侧重点
《零信任网络安全当前趋势》	2019 年 4 月，美国技术委员会 - 工业咨询委员会	对政府机构采用零信任进行评估
《网络与安全战略》	2021 年 3 月，加拿大政府部门机构 - 共享服务部	采用零信任等新方法支撑政府办公
14028 号行政令	2021 年 5 月，美国总统拜登	发动联邦政府迁移上云使用零信任架构
《网络安全战略 2021》	2021 年 10 月，新加坡政府	要求相关机构实现从边界防护向零信任安全模式转变
《零信任成熟度模型》（第二版）	2023 年 4 月，网络安全和基础设施安全局	降低美国机构实施零信任的壁垒

表 2 国内零信任理念发展情况

名称	政策发布时间和组织	侧重点
等保 2.0	2019 年，全国网络安全标准化技术委员会	明确要求“动态访问控制”，推动零信任在关键行业的合规落地
《数据安全法》《个人信息保护法》	2021 年，全国人民代表大会常务委员会	强化数据分级与最小权限原则，与零信任理念高度契合
《零信任参考体系架构》	2022 年，信安标委（TC260）	发布零信任团体标准和参考体系架构
《零信任发展洞察报告》	2024 年，中国信通院	再次归纳和强调零信任架构在关键领域数据安全、数据安全防护效能等方面的应用

国内以政策驱动网络安全建设发展，零信任架构标准初步成型。紧跟政策导向，国内科技公司也逐步推出自主产权产品，如华为聚焦身份治理与软件定义边界（SDP）技术，推出华为 HiSec 零信任架构[8]；腾讯基于多因素身份认证、终端防护和动态访问控制，推出腾讯 iOA 零信任解决方案[9]。除此以外，零信任架构在政务云（如广东“数字政府”）、金融（如中国银联）、能源（如国家电网）等领域广泛试点，呈现新的发展形势。国内零信任政策强调在政务、金融、能源等关键领域实现核心技术自主化和跨平台兼容性。

1.3.2 零信任架构的优势

在身份冒用和隐私侵犯方面，零信任架构强化身份验证，通过自适应身份认证在高风险操作时触发额外验证，使用身份联邦与单点登录确保用户服务遵循严格的认证策略，这些手段使攻击者无法通过单一验证因素或绕过验证关卡访问平台数据。

在黑客攻击与服务中断方面，零信任架构拒绝匿名流量流入，强制所有请求必须携带有效令牌，通过身份驱动的访问控制，可以阻断僵尸网络的洪泛攻击[10]。其次，零信任架构要求精细化网络分段，对关键业务隔离成为独立的微服务单元，通过零信任代理控制访问，如遇个别段服务遭受黑客攻击，其他单元仍可正常运行。

在钓鱼攻击和数据泄露方面，零信任架构限制合作伙伴或供应商的访问权限范围与有效期，避免供应链钓鱼攻击波及核心系统，除此以外，零信任架构通过设备健康性强制验证、浏览器与证书绑定等方式实时掌握终端动态，阻止攻击者伪装服务端。

2 基于零信任架构的线上培训安全平台设计

2.1 设计目标

零信任架构的核心是“持续验证、动态授权、全局防御”[11]，基于零信任架构的线上培训安全平台（以下简称“平台”）围绕数据、身份、设备、网络和业务场景等方面的安全防护展开，主要聚焦以下关键方向：

（1）在身份冒用和隐私侵犯方面，支持身份与设备的精细化验证，确保用户（学员、讲师、管理员）和设备的身份合法性，杜绝身份冒用或非法接入。

（2）在黑客攻击与服务中断方面，实现动态最小权限访问控制，按需授予用户最小权限，防止横向移动和越权访问，确保培训内容（课件、考试、学员信息等）在存储、传输和使用中的安全。

（3）在钓鱼攻击和数据泄露方面，可以快速识别异常行为（如暴力破解、数据爬取）并自动阻断攻击，尽量使用户减少钓鱼攻击的风险。

2.2 总体架构

零信任安全平台基于用户终端、网络、服务器、数据库四部分设计，用户终端承担可信终端环境感知的任务，而网络部分负责感知网络环境和代理情况，服务器端将会进行信任评估和动态访问控制，最后由数据库细粒度访问控制策略把关数据存储过程。图 1 是总体架构图。

本文定义 UR = < T, I, A, D > 表示用户请求，其中 T 是 Terminal，表示终端环境信息；I 是 Internet，表示网络环境信息；A 是 Agents，表示代理信息；D 是 Database，表示数据库评估信息。安全性评估的主要算法如下：

算法 1 线上培训安全平台总体评估算法

Input：UR

Return：SR which means system response

0 Put UR. T，UR. I，UR. A，UR. D into T/I/A/D，

1 Define S = U. matrix；

2 Define Temp = Temporary Variant；

3 Temp = Terminal Assessment（UR. T）；

4 S = Matrix Append（S，Temp）；

5 Temp = Internet Assessment（UR. I）；

6 S = Matrix Append（S，Temp）；

7 Temp = Agents Assessment（UR. A）；

8 S = Matrix Append（S，Temp）；

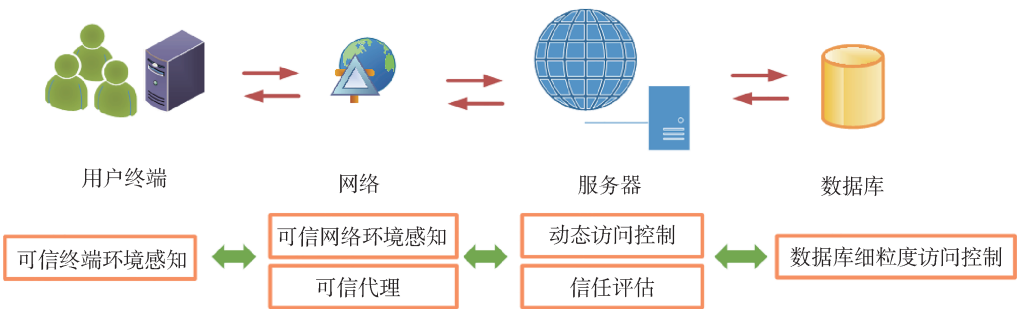

图 1 总体架构图

9 Temp = Trust Assessment (S);

10 Database Assessment (UR. D);

11 S = Matrix Append (Temp, UR. D);

12 SR = Dynamic Control (S);

13 return SR.

在上述代码中，每个模块负责本位的数据校验，但并不独立运行，会在生成评估信息之后协同传递控制信息，最后汇总到信任评估中心，由动态访问控制中心全方面控制，确保数据流通全方位监管。

2.3 详细设计

图 2 是平台详细架构图。该图从用户终端、服务器、数据库三端展示零信任架构安全平台的详细设计内容以及实现过程。

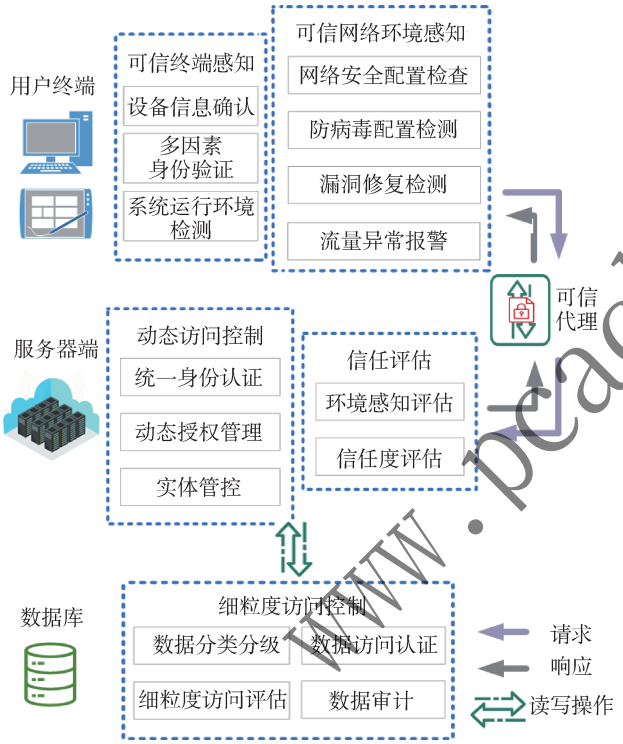

图 2 平台详细设计图

可信终端环境感知主要作用是识别终端安全属性、终端用户身份，感知终端异常行为；网络环境感知确定学员端网络环境的安全性，确保对流量使用异常现象实时监测到位；可信代理通过拦截来自终端的访问请求，判定这些请求是否为数据抓取、网络爬虫等威胁；动态访问控制根据访问安全策略、访问请求上下文属性、信任等级，认证和动态授予所有访问请求的权限，是信任评估结果的执行者；在数据库端采用细粒度访问控制策略，对数据存储精细校验，把关数据存储过程。

2.3.1 可信终端环境感知

可信终端环境感知是零信任安全平台重要的环境感知组件，终端感知信息是信任评估模块的主要风险评估输入[11]。可信终端感知包括设备信息确认、多因素身份验证、系统运行环境检测三部分内容，保障终端设备、使用者身份和系统运行环境可信。

设备信息确认：通过设备标识、密钥沙箱、白盒加密等技术，建立设备唯一标识，防止终端硬件身份被篡改或盗用，确保终端的可信性、不变性、可用性和唯一性。

多因素身份验证：利用人体生物特征，通过人工智能算法提取、分析关键信息并保存，建立授权人、代理人、游客为一体的身份验证特征库。在使用终端设备时，通过物理传感器感知专人专用、代理人使用、多人围观等场景，并匹配生物特性，保证使用者身份可行。

系统运行环境检测：终端通过定时上报进程、服务、注册表、外设、应用软件的状态，平台全方位感知终端的基础安全环境、运行安全环境，发现已有和潜在的风险，并上报至业务访问控制单元处理，保证培训业务的可信访问。

2.3.2 可信网络环境感知

可信网络环境感知包括网络安全配置检查、防病毒配置检测、漏洞修复检测、流量异常报警等[12]。

网络安全配置检查：主要检查防火墙配置、路由器和交换机安全、网络分段信息，允许通过必要的端口、协议拒绝未经明确的流量访问，并限制敏感区域的访问，隔离出不同安全级别的网络。

防病毒配置检测：在该步中，平台确认服务器、工作站等设备防病毒软件的安装情况和运行状态，确认无异常退出或禁用行为，并对病毒库和防毒引擎进行版本检测，确保已更新至最新版本。

漏洞修复检测：检查系统是否已修复常规漏洞，是否有定期检查漏洞的防护软件，漏洞扫描和修复软件是否处于开启状态，并保持持续监控状态保证无异常退出的情况发生。

流量异常报警：建立流量消耗异常检测机制，一旦出现流量异常，平台检查安全配置和数据库访问情况，自动排查原因，并将其报送至控制中心，由控制中心处理异常情况。如遇软件漏洞如 SQL 注入、跨站脚本攻击(XSS)等，平台将迅速主动防御，避免被黑客利用。

2.3.3 可信代理

可信代理是动态访问控制的策略执行点，也是保证业务访问的第一关。零信任安全平台中通常使用零信任网关代理所有流量，以达到检测服务器的性能、类型、

匿名级别、物理位置、支持协议、响应时间等信息的目的[13]。可信代理使用流量加密（例如 TLS/国密算法）加密数据，提高数据安全性。通过可信代理，可以筛选有效的 IP 地址，封禁频繁使用的不合法代理 IP 地址，提高数据访问的效率，避免因失效代理 IP 恶意访问导致的数据泄露或因此产生法律问题。

2.3.4 信任评估

信任评估模块通过采集外部平台分析结果和各类实体动作行为日志信息，并综合分析信任程度，支撑动态访问控制过程[14]。本文引用 Self-attention 机制思想[15]，将矩阵相乘表示相关特征的算法引入信任评估模块，创建信任评估算法，用以快速评估和判定请求的可信环境。

本文定义 UM = < T. S，I. S，A. S，D. S > 表示信任评估矩阵，T. S、I. S、A. S、D. S 分别表示终端环境信息、网络环境、代理、数据库的可信度属性向量；SA 为安全度评估矩阵。信任评估算法如下：

算法 2 信任评估算法

Input：T. S，I. S，A. S，D. S

Return：SS which means Security Assessment Matrix

0 len = Length［T. S，I. S，A. S，D. S］

1 Define SA = Zero［len，len］

2 Define OM = Unit Matix［len，len］

3 For each r in［T. S，I. S，A. S，D. S］

4 SA. Append（r）

5 SA = MultiplyMatrix（SA，SA）

6 If SA. Match（OM）：

7 Return SS = 1；

8 Else：

9 Return 0；

信任评估模块接收包含终端、网络、代理环境等信任评估参数及用户提交参数的请求，并计算信任度，得出响应结果。表 3 为用户请求示例。

表 3 用户请求示例

名称	路径	参数
添加讲师	GET：/api/teacher/addTeacher	｛“terminal”：［0，1，0］，“internet”：［0，1，1］，“agents”：［1，1，1］，“key1”：value1，“key2”：value2 …｝
删除课程	POST：/api/course/delCourse	｛“terminal”：［1，1，1］，“internet”：［1，1，1］，“agents”：［1，1，1］，“key1”：value1，“key2”：value2 …｝

信任评估模块接收用户请求参数后，以特征向量的形式整合计算。特征向量设置如下：

$$f_m = [x_1, x_2, x_3, \cdots, x_n],\ x_n \in \{0, 1\} \tag{1}$$

其中，f_m 为特征向量类型，m 表示特征向量类型个数。例如：可信终端环境、可信网络环境均为一类特征向量。而 x_n 为特征向量值，取值范围为 0 和 1，表示一类特征中特征的评估结果，其中 n 为所有评估向量中最大的维度数，不足 n 维度的向量用 1 补齐。例如［0，1，1］表示设备信息确认有误、多因素身份验证通过、系统运行环境可行。

在信任评估环节加入 Self-attention 机制，目的是快速统计用户在评估过程中遇到的问题，并减少遍历和判定次数，直接使用数乘运算得到信任度评估结果。式（2）是特征向量计算公式：

$$\text{OneMatrix}(\boldsymbol{Q}, \boldsymbol{K}) = \text{softmax}\left(\frac{\boldsymbol{Q}\boldsymbol{K}^{\mathrm{T}}}{\sqrt{d}}\right) \tag{2}$$

其中，$\boldsymbol{Q}$、$\boldsymbol{K}$ 是特征向量矩阵，$\boldsymbol{Q} = [f_1, f_2, f_3, \cdots, f_m]$，$\boldsymbol{K} = [f_1, f_2, f_3, \cdots, f_m]^{\mathrm{T}}$，$\boldsymbol{Q}$、$\boldsymbol{K}$ 相乘后可以得出自注意力矩阵，若自注意力矩阵为全 1 矩阵，则表示各信任评估环节均通过，若为含有结果不为 1 的矩阵，则表示其中的信任评估不通过，此项访问不予通过。通过自注意力机制可以经过一次矩阵运算就得出各环节评判结果，而不需进行循环遍历，从而减少运算次数，提高系统运行效率。

2.3.5 动态访问控制

该控制模块一般设定为强制认证模式，严格控制动态信任访问请求。其主要基于授权服务、身份认证、信任评估模块指令等基础模块与信任代理联动[16]。

在身份认证方面，零信任架构并非传统的静态、单因子身份认证方式，而是演变为强制性、动态性的认证策略；在授权服务方面，零信任架构由基于静态规则判定权限，变为基于角色、安全策略、信任等级、评估结果的动态权限调整；实体指任何请求访问资源的对象，平台汇总来自用户、设备、应用服务、网络流量等所有实体的评估结果，根据结果控制实体的权限、请求、读写等操作。通过动态访问控制，可以动态控制用户行为，实现全方位管控。

2.3.6 数据库细粒度访问控制

细粒度访问控制策略是数据从服务器端至数据库端往来的重要控制策略，主要包括数据分类分级、访问认证、细粒度访问评估、审计四个部分[17]。数据分类分级主要是将相关培训数据按照类别和安全等级划分，划分完成后认证用户的身份信息，并在细粒度评估策略中心评估数据信息，数据合规后执行入库操作，最后反馈访问结果。细粒度访问控制策略由数据库执行，但受平台控制。审计是为管理员设置的功能模块，方便后期对数

据进行数据监督和查漏。通过数据库细粒度访问控制，可以把控数据库读写操作，防止 SQL 注入攻击、数据泄露等。

2.4 部署方案

零信任架构的部署需围绕身份、设备、网络、数据和应用五大核心要素，结合线上培训场景特点（如高并发、多终端接入、敏感数据保护），分阶段实现动态验证与最小权限控制[18]。以下是具体部署步骤与技术实现：

（1）实现身份与设备可信化

①实现身份统一管理。部署身份识别与访问管理（Identity and Access Management，IAM）系统，集成学员、讲师、管理员身份，支持多因素认证（Multi Factor Authentication，MFA），例如短信 + 生物识别等。学员首次登录需绑定手机号 + 人脸识别，讲师账号需硬件令牌认证。

②终端环境感知。安装轻量级终端代理，强制检测设备健康状态。例如检查操作系统版本、杀毒软件、磁盘加密状态，标记越狱手机、未打补丁的台式机为“高风险设备”，设置高风险设备仅允许访问公开课件，禁止进入考试系统等。

（2）实现动态网络与访问控制

①部署零信任网关。在培训平台入口部署 ZTNA 网关，隐藏后端服务（如直播服务器、考试系统），所有请求经网关验证身份与设备状态后，动态路由至目标服务。

②实现微隔离与 SDP。划分细粒度安全域，例如直播区允许高带宽访问，但限制 IP 地理范围（如仅限国内）；考试区仅允许已认证设备在考试时间段内访问，禁止录屏、截屏；管理后台仅限管理员通过 VPN + 硬件令牌访问。

③动态权限策略。实现基于角色的访问控制，例如学员可观看直播、下载课件（低敏感度），讲师可上传课件、发布考试（中敏感度）。另外应实现基于上下文的动态调整，管理员可配置系统、导出学员数据（高敏感度，需审批流程）。学员在非考试时段访问考试系统时，自动拒绝并告警。

（3）数据全生命周期保护

①数据分类与加密。自动化识别敏感数据并分类标记，例如识别学员身份证号、考试答案等；自动进行动态脱敏，对低权限用户仅显示身份证号后四位。

②防泄露与溯源。添加动态水印，并记录所有数据访问行为日志追踪，如在课件和考试界面叠加学员 ID + 时间戳水印，防止拍照泄露。

（4）持续增强用户安全意识

①开展网络安全意识普及活动，增强培训平台用户网络安全意识。

②通过模拟钓鱼演练等方式增强用户安全意识，可以定期向员工发送模拟钓鱼邮件，并实时反馈风险等。

3 基于零信任架构的线上培训安全平台的应用

3.1 应用场景

本文提出的零信任安全平台主要应用于线上培训场景。例如：平台的动态身份验证、最小权限访问等特点，适用于涉及敏感资料（如战略文档、技术资料、客户数据等），需防止内部或外部泄露的企业内部培训；平台的多因素使用身份验证适用于需防止替考、作弊或成绩篡改的考试与认证系统；平台的可信终端感知适用于学员通过手机或平板接入，设备可能处于公共 Wi-Fi 等不安全环境的移动端学习场景等。在开发培训平台时，可以根据平台理念，设置相应安全策略，构建整体安全平台，保障运行安全。

3.2 未来发展方向

线上培训和网络安全平台建设应协同规划、齐头并进。对培训机构来说，线上培训平台的开发和网络安全系统建设密不可分，网络安全是前提，系统开发是重点。零信任安全防护策略灵活多样，应对能力强，但这也意味着安全策略建设方式多种多样，需要同步投入人力物力来建设零信任安全平台，部署零信任策略方法，应对不可预知的安全风险。

在培训领域，新型 IT 环境面临的安全挑战和网络威胁是持续存在的，推动零信任安全策略和产品更新迭代应当常态化。目前培训平台与新兴防护策略的兼容是升级换代的主要困难，应提前规划软硬件升级和安全防护工具更迭，同步零信任安全防护措施，不断抬高网络安全层级，构建网络安全生态环境。

4 结束语

零信任架构重新评估和审视传统边界安全架构思想，默认不信任任何网络、设备和用户，要求对用户操作、使用设备、数据资产进行细粒度控制和动态调整，是网络安全威胁的重要隔离带和防火墙。基于零信任架构的线上培训安全平台首次将零信任理念应用至培训业务场景，确保严格审查用户操作行为，让不规范、存在隐患的请求被有效、准确拦截，保证学员和培训机构的数据资产安全。另外，平台中首次融合自注意力机制思想，创建信任度计算算法，快速计算用户行为信任度，提高运行效率。基于零信任架构的线上培训平台是在科技进步情况下提出的应对和抑制未知威胁的安全机制，对提高线上培训平台安全防护水平具有重要意义。

参考文献

[1] 陈铭媚. 新时代企业人员培训中的问题与对策 [J]. 品牌

研究，2024（1）：217－219.
[2] 刘鹏远. 数字化驱动，让培训更智能 [J]. 人力资源，2025（3）：80－81.
[3] 韩佼男，张万莉，王春秀，等. 智慧培训平台赋能企业培训管理数字化转型 [J]. 中国管理信息化，2024，27（22）：144－146.
[4] 马春梅. 在线教育平台信息安全防护策略——以 XX 公共培训服务平台为例 [J]. 青岛远洋船员职业学院学报，2023，44（2）：74－76.
[5] 王若晗，向继，管长御，等. 零信任架构的回望与未来发展研究 [J]. 信息安全研究，2024，10（10）：896－902.
[6] WARD R，BEYER B. BeyondCorp：a new approach to enterprise security [J]. the Magazine of USENIX & SAGE，2014，39：6－11.
[7] 诸葛程晨，王群，刘家银，等. 零信任网络综述 [J]. 计算机工程与应用，2022，58（22）：12－29.
[8] 薛人瑞，吴华佳. Hisec 零信任安全解决方案 [C]// 2021 年国家网络安全宣传周“网络安全产业发展论坛”论文集，2021：119－123.
[9] 蔡东赟. 腾讯 iOA 零信任安全技术实践 [J]. 信息安全与通信保密，2020（S1）：98－102.
[10] 李治宇. 基于零信任策略在网络攻防演练中的实践研究 [J]. 信息产业报道，2024（1）：60－62.
[11] 罗栗，黎臻，陈洋. 零信任网络架构与实现技术的研究与思考 [J]. 通信技术，2023，56（4）：509－514.
[12] 莫爵君，陈哲，春增军，等. 基于企业现有安全架构的零信任架构可行性研究 [C]//2023 电力行业信息化年会，2023：226－232.
[13] 徐言海. 零信任安全体系的设计与实现 [J]. 集成电路应用，2024，41（2）：329－331.
[14] 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]. 鄂州大学学报，2024，31（1）：99－101.
[15] VASWANI A，SHAZEER N，PARMAR N，et al. Attention is all you need [J]. arXiv：1706. 03762，2017.
[16] 孙振中. 零信任和 SDP 技术框架在新华社移动办公中的应用研究 [C]//中国新闻技术工作者联合会 2024 年学术年会论文集，2024：232－236.
[17] 安宁，许文静，刘珠慧，等. 基于零信任模型的细粒度数据库安全控制方法 [J]. 电子技术应用，2024，50（10）：63－68.
[18] 吕忠亭，朱丹妮，雷世斌，等. 基于零信任体系的数字身份安全平台设计与研究 [J]. 微型电脑应用，2024，40（2）：45－49.

（收稿日期：2025－03－14）

作者简介：

秦文远（1998－），男，硕士，助教，主要研究方向：软件工程、数据安全、深度学习、计算生物学。

安宁（1990－），男，硕士，高级工程师，高级经济师，主要研究方向：软件工程、云计算、人工智能、大数据、信息安全、数字教育等。

（上接第 9 页）

[14] RAHMAN M M，CHAYAN M M H，MEHRIN K，et al. explainable deep learning for cyber attack detection in electric vehicle charging stations [C]//Proceedings of the 11th International Conference on Networking，Systems，and Security，2024：1－7.
[15] BUDDI E D，GHORBANI A A，DADKHAH S，et al. Enhancing ev charging station security using a multi-dimensional dataset：CICEVSE2024 [C]//IFIP Annual Conference on Data and Applications Security and Privacy. Cham：Springer Nature Switzerland，2024：171－190.
[16] BENFARHAT I，GOH V T，SIOW C L，et al. Temporal convolutional network approach to secure open charge point protocol（OCPP）in electric vehicle charging [J]. IEEE Access，2025，13：15272－15289.
[17] SHEN T，DING L，SUN J，et al. Edge computing for IoT security：integrating machine learning with key agreement [C]//2023 3rd International Conference on Consumer Electronics and Computer Engineering（ICCECE）. IEEE，2023：474－483.
[18] ABDULKAREEM S A，FOH C H，CARREZ F，et al. A lightweight SEL for attack detection in IoT/IIoT networks [J]. Journal of Network and Computer Applications，2024，230：103980.

（收稿日期：2025－04－07）

作者简介：

姚沁怡（1999－），女，硕士研究生，主要研究方向：网络安全、工业大数据。

龙莆均（1987－），通信作者，男，博士，讲师，主要研究方向：最优化方法。E-mail：longpujun@ gmail. com。

陈世伦（1998－），男，硕士研究生，主要研究方向：图像处理。

版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视作该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付的稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部