基于人工智能和数据挖掘的零信任网络安全保障研究

刘章
湖南开放大学，湖南 长沙 410004

摘要：随着 5G、大数据、物联网等新兴技术的发展，传统的网络安全边界逐渐瓦解，企业面临的安全威胁愈加复杂。本文提出基于人工智能（AI）与数据挖掘技术的零信任网络安全保障模型，力求为现代网络提供更智能、更全面的安全防护。研究指出，AI 技术依托智能身份验证、动态访问控制、威胁情报分析等功能，做到了对用户行为的实时监控，识别异常并预测潜在威胁。数据挖掘技术进一步增强了风险评估与网络流量异常检测能力，使系统能够主动防御、及时响应。

关键词：人工智能；数据挖掘；零信任；网络安全保障

Research on Zero-Trust Network Security Assurance Based on Artificial Intelligence and Data Mining

Liu,Zhang

Hunan Open University, Changsha, Hunan, 410004, China

Abstract: With the development of emerging technologies such as 5G, big data, and the Internet of Things, traditional network security boundaries are gradually dissolving, and enterprises are facing increasingly complex security threats. This paper proposes a zero-trust network security assurance model based on artificial intelligence (AI) and data mining technologies, aiming to provide smarter and more comprehensive security protection for modern networks. The research indicates that AI technology relies on functions such as intelligent identity verification, dynamic access control, and threat intelligence analysis to achieve real-time monitoring of user behavior, identify anomalies, and predict potential threats. Data mining technology further enhances the capabilities of risk assessment and network traffic anomaly detection, enabling the system to actively defend and respond in a timely manner.

Keywords: AI; Data mining; Zero trust; Network security assurance

DOI: 10.62639/sspis25.20240103

近年来，随着 5G、大数据、物联网等新兴技术的快速发展，网络环境正变得日益复杂，传统基于网络边界的安全防护方式已难以应对日益多样化和隐蔽的网络攻击。根据《中华人民共和国网络安全法》及相关文件的精神，网络安全已上升为国家战略，要求企业和组织采取更加全面和智能的防护措施。在此背景下，零信任网络安全模型逐渐成为应对复杂安全威胁的关键。零信任打破了传统网络内外的信任假设，以“永不信任，始终验证”为核心理念，确保网络内外的每个访问请求都经过严格的身份验证和授权[1]。在全球网络安全领域，人工智能和数据挖掘技术的结合被广泛应用于增强网络防护能力。据 Gartner 的预测，到 2023 年将有 60% 的企业采用零信任策略；到 2025 年，至少 70% 的新增远程部署将使用零信任网络访问。AI 依托智能身份验证和动态访问控制等技术，实时监控用户行为并识别异常，数据挖掘技术则通过分析海量网络数据，帮助系统识别潜在威胁和预测攻击趋势[2]。这种智能化的安全防护体系为企业用户提供了更灵活、更强大的安全保障，特别是在面对复杂多变的网络威胁时，零信任结合 AI 与数据挖掘的模型能够主动应对，从而为企业的数字化转型保驾护航。

一、零信任的核心理念

零信任网络安全的核心思想是“不信任内外网中的任何用户和设备”。传统网络安全模型假设内部网络是可信的，然而，随着基于 IPv6 协议的新一代互联网络建设和数字化转型的不断深入，这种假设显然不再成立。零信任打破了这一界限，强调对每次访问请求都进行细致的验证，确保用户和设备的身份真实、行为合法，降低潜在的安全隐患。换句话说，它从根本上颠覆了过去对内部网络的“放任式信任”，以此来应对日益复杂的网络威胁。

二、人工智能在零信任中的应用

在零信任架构中，人工智能通过智能化的分析与学习，提升了安全系统的防护能力。AI 不仅

（稿件编号：IS-24-3-1026）

作者简介：刘章（1979-11），男，汉，籍贯：辽宁省北票市，研究生，高级工程师，研究方向：网络工程、网络安全技术、软件工程。

基金项目：中国高校产学研创新基金 - 新一代信息技术创新项目：“网络安全运营体系在智慧校园建设中的研究和应用”（基金号：2023IT163）。
湖南开放大学校级一般课题：“基于基线和态势感知的湖南电大网络安全防护体系研究”（基金号：XDK2019-C-5）。

能够实时监控用户和设备的行为，还能够基于模式识别和异常检测来发现潜在威胁。

（一）智能身份验证

在零信任架构中，智能身份验证堪称核心环节之一，它运用了人工智能（AI）技术中的生物识别和机器学习手段，实现了多层次、多因素的身份验证。与传统的单一密码验证方式相比，AI 使得身份验证的过程更加全面、动态。具体来说，当用户尝试登录系统时，AI 不仅会验证用户输入的用户名和密码，还会从用户的操作习惯入手进行更为深入的背景验证[3]。比如，它能够监控用户的键盘输入模式、鼠标移动轨迹，甚至是设备的使用环境和位置等一系列行为特征。这些行为数据看似无关紧要，但在人工智能的分析下，它们能够形成用户的“数字指纹”，即一个独一无二的行为模式。正是基于这种分析，AI 才可以在不打扰用户的情况下“悄无声息”地判断其操作是否符合平时的使用习惯。假如某次登录过程中，系统检测到用户的行为与平时的特征有所偏离，比如键盘输入方式明显不同，或者登录地理位置异常，AI 便会立即触发更高级别的验证措施，如要求输入一次性验证码、进行生物特征验证（如指纹或人脸识别）等。这种动态且灵活的验证机制让安全保护如影随形，使得即使密码被盗，攻击者也难以轻易绕过验证。更重要的是，智能身份验证还大大减少了用户在不同安全场景下的重复输入与验证操作，简化了用户体验，而背后仍在运行的复杂验证过程，确保了每一步都严丝合缝，滴水不漏。正是因为这些智能技术的介入，零信任才能在不牺牲安全性的前提下，为用户提供流畅而安全的访问体验，避免了传统密码验证方法的种种弊端，特别是在面对日益复杂的网络攻击时，具备了更强的应对能力和防护效果。

（二）动态访问控制

在零信任架构中，动态访问控制是确保网络安全与访问灵活性的重要手段，它的核心在于利用人工智能对用户的历史行为和当前操作环境进行全面的实时分析，并据此动态调整访问权限。与传统的静态访问控制不同，动态访问控制并不依赖固定的权限配置，而是根据环境变化随时进行调整。具体来说，系统会实时监控用户的行为模式、操作设备、地理位置、网络环境等多种因素，甚至包括时间、设备类型、访问资源的敏感性等上下文信息[4]。如果系统检测到用户的行为突然与之前的习惯大相径庭，或者出现了潜在的安全风险，比如用户从低风险地区移动到高风险地区，系统就会立刻采取相应措施，比如要求用户进行额外的身份验证、调整访问权限，甚至是临时中断访问。这种机制的优势在于，它并不是一刀切地限制用户的操作，而是依据风险动态评估访问的合理性，既保证了用户在安全环境下可以顺畅工作，又能在发现潜在威胁时迅速采取行动，防止攻击者趁虚而入。这种基于情境的实时决策模式也使得企业能够灵活应对复杂多变的安全环境，不再局限于一成不变的权限设置，从而为网络安全带来了更多弹性和智慧。例如，当系统发现用户尝试从一台新的设备登录时，系统可以自动判断该设备是否曾被用户使用，并根据当前风险等级要求用户进行额外的验证步骤，避免未经授权的设备轻易进入系统。总的来说，动态访问控制使得零信任网络能够根据用户的实时状态和环境变化做出相应的安全反应，为用户提供灵活而强大的安全保障，同时也大大提高了防护的精确度和敏捷性。

（三）威胁情报分析

在零信任架构下，威胁情报分析是确保网络安全的关键一环，而人工智能的引入让这一过程更加高效、智能。AI 技术在机器学习模型的帮助下，可实时分析网络流量，并利用数据挖掘技术从海量数据中迅速筛选出异常流量模式和潜在的恶意行为。AI 会持续监控网络中的各种通信和活动，分析其中是否存在流量突然激增、数据包的分布异常等状况，或者某一设备开始向未授权的地址发送大量请求等。凭借对历史数据的学习，AI 能够从正常网络行为中“嗅探”出那些隐藏的威胁，这些威胁往往不是一开始就暴露出来，而是以微小的异常信号逐步显现。正如经验丰富的侦探能够基于细节判断潜在危险一样，AI 同样可以根据细微的网络波动识别出潜在攻击[5]。当系统检测到潜在威胁时，它可以立即自动采取措施，比如阻断可疑通信、隔离相关设备，或者提醒管理员进行进一步调查，及时阻止攻击者的进一步渗透，还能有效减少威胁扩散的风险。在零信任环境中，威胁情报分析的实时性和智能化尤其重要，因为网络边界已经不再明确，攻击者可能隐藏在内部网络或外部环境的任何地方。不断挖掘、分析流量中的潜在威胁，使企业能够在早期就发现问题，避免网络攻击造成更大的损失。此外，AI 的学习能力还让它能够随着时间推移，逐步优化对威胁的识别和应对策略，不断提升网络的防护能力。这种灵活、快速的威胁响应机制，正是零信任体系中确保安全的一大核心优势。

三、数据挖掘技术在零信任中的应用

数据挖掘是一种从海量数据中提取有价值信息的技术，结合零信任架构，可以进一步增强网络安全保障能力，在对历史数据进行挖掘、分析的过程中，数据挖掘技术可以发现隐藏的安全威胁，并预测未来的风险。

（一）行为分析与模式识别

在零信任架构中，行为分析与模式识别是实现持续验证和动态防护的重要技术手段。通过数据挖掘技术，系统能够对每个用户的日常行为进行建模，逐步形成其独特的行为“画像”。这种“画像”并不仅仅是单纯的身份标识，而是综合了用户的登录时间、访问频率、所用设备、访问资源的类型以及具体操作习惯等多维度的信息。每一次的登录操作、系统访问、文件下载，甚至鼠标点击和键盘输入的节奏，都在无形中为系统提供了关于用户行为的关键信息。对这些行为数

据进行持续学习，系统能够划定一个“正常行为范围”，也就是用户的标准行为模式。一旦某次登录或操作显著偏离这一模式，例如用户在非常规时间登录、从不常用设备访问敏感数据、或者突然出现异常频繁的资源访问请求，系统就会立即触发预警机制，甚至要求进一步的身份验证[6]。这样的行为分析不仅仅是简单的“对比差异”，而是基于用户长期行为的细致观察，结合实时的环境判断，来决定当前操作的可信度。正是因为这种技术能够在不打扰用户正常操作的前提下进行细致的背景分析，它让网络的安全性大幅提升，同时用户体验也不会因频繁的验证而受到干扰。零信任模型正是利用了这种实时的行为识别，才有效防范了内部威胁和已获得初步访问权限的外部攻击者，因为即便是被盗用的合法账户，操作习惯和行为模式也是很难完全复制的。这一层基于行为的智能防护，成为了零信任体系中动态安全的有力补充，使得系统能够更主动、更敏锐地感知潜在威胁，并及时作出应对，真正实现“始终验证，永不信任”的理念。

（二）风险评估与预测

在零信任架构中，风险评估与预测是构建强大安全体系的关键一环，而数据挖掘技术的引入为这一过程提供了强大的技术支持。系统可以对大量历史数据和攻击事件进行深入分析，从中识别出潜在的高风险区域和易受攻击的环节，并预测未来可能发生的安全威胁。它的工作原理类似于防疫中的流行病学分析：在研究过往发病案例和传播途径的过程中，可提前判断出疫情的高发地带，部署防控措施。具体到网络安全领域，系统会利用数据挖掘技术，搜集并分析网络中的异常数据流、未授权访问尝试、恶意软件活动等信息，构建出一套关于威胁行为的“数据库”。这些数据能够帮助系统识别出常见的攻击模式，还可发现不易察觉的、潜伏期较长的复杂攻击手段。比如，当某一段时间内企业的网络流量突然激增或出现异常数据包传输时，系统能够迅速意识到可能正在酝酿的网络攻击，并提前触发相应的安全策略，如加固防火墙、限制高风险访问或要求用户进行额外的身份验证。零信任架构依靠这种基于历史数据的动态预测，更加主动地应了对各种潜在威胁，不再依赖“事后响应”，而是将安全防护前置化，做到防患于未然。这种风险评估与预测的优势在于，它能够提高企业的整体安全防御水平，减少突发性网络攻击带来的损失，特别是在面对复杂的多层次攻击时，零信任可以基于风险预判行为帮助企业提前做好布局，灵活调整防护措施，更有效地降低攻击的成功率。正是这种前瞻性和主动防御的能力，使零信任体系在现代网络安全领域中占据了重要位置。

（三）网络流量分析与异常检测

在零信任架构中，网络流量分析与异常检测是确保网络安全的关键环节之一，数据挖掘技术则为这一过程提供了强有力的支持，系统在数据挖掘技术的支持下，实时监控、分析着网络中的每一个数据包，深入挖掘数据流量的类型、大小、传输频率等特征，从而识别出隐藏在正常流量背后的异常行为。比如，DDoS 攻击通常伴随着流量的突然激增，而恶意软件的活动则可能体现在某些端口的频繁小数据包传输上。系统可以对这些流量模式进行分析，及时发现不符合常规的网络活动，并判断背后存在的潜在威胁。实际上，这种异常检测并不仅仅是简单的流量对比，而是基于大量历史数据和正常流量特征的复杂建模。例如，某企业的网络中某类数据包的传输频率一贯较低，但如果某天这类数据包突然密集出现，系统会立刻判断该行为可能是潜在的网络威胁，并发出预警或自动采取防御措施。更重要的是，零信任体系下的网络流量分析并非依赖预设的“正常流量规则”，而是利用机器学习和数据挖掘技术不断自我学习和更新，能够根据不同企业的网络特点动态调整安全策略。这意味着，系统不再只是被动地等待攻击发生，而是通过对异常流量的快速反应，主动出击，保护企业的关键资产免受攻击。举例来说，当系统检测到某一服务器的流量模式与以往明显不同，可能意味着攻击者正在进行数据渗透，系统可以迅速采取隔离措施，限制该服务器的访问权限，从而阻止攻击进一步扩展。正是因为有了这种基于流量分析的异常检测机制，零信任架构得以在复杂多变的网络环境中保持高度的敏捷性和防护能力，维持网络的可控状态，企业可以更从容地应对各种潜在网络威胁。

四、结语

在当前复杂多变的网络安全环境中，零信任模型为企业提供了一种全新的安全理念与架构，结合人工智能和数据挖掘技术，零信任网络安全保障体系得以进一步增强，实现了对用户行为的实时监控和分析，还能够预判潜在的安全风险，有效防止网络攻击的发生。随着 5G、物联网和大数据的不断发展，零信任与 AI 的结合将为未来的网络安全体系带来更多可能性，为企业的数字化转型保驾护航。

参考文献：

[1] 桂旭东，付明远．基于零信任理念的广播电视网络安全架构设计与应用 [J]．广播与电视技术，2024，51（09）：111-116.
[2] 王一芃，代娇，兰柳，马家骥．零信任技术在铁路信息网络安全场景的应用构想 [J]．交通工程，2024，24（07）：36-43.
[3] 侯琳琳．零信任架构的水利数字孪生物联网安全防护技术应用 [J]．河南水利与南水北调，2024，53（07）：100-101.
[4] 冯燕飞．基于零信任架构的 MFA 多因素统一身份认证平台的运用 [J]．网络安全技术与应用，2024，（01）：22-23.
[5] 张宜力．基于零信任的广电网络安全防护体系应用研究 [J]．广播电视网络，2023，30（11）：91-93.
[6] 王锋．零信任理念在公安视频网络安全防护体系建设中的启发与设计 [J]．中国安防，2023，（11）：13-17.