基于人工智能的云计算通信网络安全传输控制技术

刘天庚　刘明林
河北方维网络技术有限公司　河北　石家庄　050000

摘　要：本文围绕基于人工智能的云计算通信网络安全传输控制技术展开。首先阐述其在风险防控精准性、响应时效性、传输可靠性及自动化管理等方面的重要性。接着介绍核心技术架构，包括数据采集、智能分析、传输控制三层。随后说明关键技术应用，如基于机器学习的攻击识别预警等。最后指出该技术应用中存在模型训练数据质量不足、技术兼容性差、实时性有待提升等问题，并给出相应解决思路。

关键词：人工智能；云计算；通信网络；安全传输控制；数据防护

引言：在数字化高速发展的当下，云计算通信网络已成为信息传输的关键基础设施，但复杂多变的网络环境使其面临诸多安全挑战。传统安全传输控制技术在应对不断演变的网络攻击时，逐渐显露出风险防控不精准、响应不及时、传输可靠性欠佳等问题。在此背景下，基于人工智能的云计算通信网络安全传输控制技术应运而生。它凭借在风险防控、响应时效、传输可靠及自动化管理等方面的显著优势，成为保障云计算通信网络安全的关键力量。本文将深入探讨其重要性、核心技术架构、关键应用及常见问题与解决思路。

1　基于人工智能的云计算通信网络安全传输控制技术的重要性

在当今数字化浪潮汹涌澎湃的时代，网络环境变得极为复杂且多变。基于人工智能的云计算通信网络安全传输控制技术，在这样的背景下展现出不可替代的重要性，主要体现在风险防控精准性、响应时效性、传输可靠性以及自动化管理等多个核心维度。（1）在风险防控精准性方面，传统安全传输控制技术主要依靠预先设定的固定规则进行匹配。然而，网络攻击手段层出不穷且持续演变，特别是那些未知攻击类型，传统技术面对它们时极易出现漏判情况。而人工智能技术借助先进的机器学习算法，能够对海量的网络传输数据进行深度剖析与细致挖掘。通过持续不断的学习和训练，它可以精准区分正常数据传输模式与异常攻击特征。不仅能对已知攻击实施精准拦截，还能凭借对数据规律的把握，对潜在未知攻击提前发出预警，极大地提升了风险防控的精准程度，为云计算通信网络构建起一道坚实的防线。（2）从响应时效性来讲，网络攻击往往具有突发性和快速传播的特点。传统技术由于规则更新存在滞后性，在面对突然出现的攻击时，难以及时做出应对，导致处置不及时，使得攻击造成的损失不断扩大。而人工智能技术可实现对网络传输状态的实时监测以及对数据的动态分析。一旦检测到异常传输行为，能立即触发响应机制，迅速完成攻击的识别、定位和处置，有效缩短攻击响应时间，将攻击造成的损失控制在最小范围内。（3）在传输可靠性上，人工智能技术能够依据实时感知到的网络状况，自适应调节传输参数、优化传输路径，增强数据传输的稳定性与效率。同时，其具备强大的数据加密与解密能力，能为数据传输提供全方位的隐私保护，保障数据在云计算通信网络中安全流转。此外，该技术减少了传统安全控制对人工干预的依赖，提升了安全传输控制的自动化水平与管理效率，让云计算通信网络的安全运行更加智能、高效[1]。

2　基于人工智能的云计算通信网络安全传输控制核心技术架构

2.1 数据采集层

数据采集层在基于人工智能的云计算通信网络安全传输控制核心技术架构中处于基础性地位，其核心使命是达成对云计算通信网络传输数据的多维度、全场景感知与精准采集。（1）该层借助分布式采集节点展开部署，这些节点广泛覆盖网络接入点、传输链路以及云节点等关键部位，以此保证数据采集的全面性。采集的数据类型丰富，包含传输数据内容、传输协议的各类参数、网络带宽的实时占用情况、节点的运行状态以及数据传输的延迟等关键信息。（2）为保障采集数据的完整性和时效性，一方面采用实时数据采集技术，另一方面结合边缘计算对采集的数据进行初步过滤与预处理，去除无效和冗余信息，减轻后续分析的负担。此外，通过建立数据采集同步机制，确保各节点采集数据在时间上保持一致，为后续基于人工智能的智能分析提供精准可靠的数据基础。

2.2 智能分析层

智能分析层作为整个基于人工智能的云计算通信网络安全传输控制技术架构的核心部分，承担着对传输数据进行深度剖析、精准识别攻击模式以及科学评估网络传输状态的关键任务。（1）在攻击识别环节，运用机器学习与深度学习算法构建专门的攻击识别模型。借助对大量历史攻击数据的训练，模型能够精准捕捉恶意代码注入、DDoS攻击、数据窃取等常见攻击模式的典型特征。同时，采用无监督学习算法对未知传输行为展开异常检测，有效发现潜在的未知攻击风险。（2）在传输状态评估方面，通过对传输延迟、带宽利用率、数据丢包率等关键参数进行细致分析，构建网络传输状态评估模型，实时、准确地判断网络传输的稳定性与安全性，为后续制定合理的传输控制策略提供坚实的数据支撑。此外，该层还需具备模型自适应优化能力，通过不断学习新的传输数据和攻击特征，持续提升分析精度与识别效率。

2.3 传输控制层

传输控制层在基于人工智能的云计算通信网络安全传输控制技术架构中，依据智能分析层输出的精准分析结果，达成对云计算通信网络传输过程的自适应调控与优化。其核心功能丰富且关键。在传输路径优化上，依据网络传输状态评估结果，运用强化学习算法，实时、动态地规划出最优传输路径，有效避开网络中的拥堵链路以及潜在安全风险区域，显著提升数据传输的效率与安全性。在传输参数调节方面，能根据实时的带宽占用状况以及数据传输的具体需求，自适应地调整传输速率、数据包大小等关键参数，确保整个传输过程稳定可靠。面对智能分析层识别出的各类攻击风险，传输控制层会自动触发与之匹配的拦截策略，及时阻断恶意攻击行为，并采用基于人工智能的动态加密技术，根据数据重要程度自适应选用加密算法与密钥长度，实现数据传输的精准加密保护[2]。

3 基于人工智能的云计算通信网络安全传输控制关键技术应用

3.1 基于机器学习的攻击识别与预警技术

基于机器学习的攻击识别与预警技术，在基于人工智能的云计算通信网络安全传输控制领域，是达成风险精准防控的关键核心技术之一。（1）此技术首先会广泛收集海量的网络传输数据样本，这些样本涵盖正常传输数据以及各类已知攻击数据。利用这些样本对机器学习模型展开训练，让模型深入学习并精准掌握不同攻击模式的特征规律。在实际应用场景中，模型会实时接收来自数据采集层的传输数据，经过特征提取和模式匹配等操作，迅速识别出数据传输过程中存在的恶意攻击行为，并依据攻击的严重程度生成对应等级的预警信息。（2）为进一步提升模型的泛化能力和识别精度，可采用集成学习算法，将多种单一机器学习模型的优势有机融合，有效降低攻击漏判和误判的概率。此外，还需建立模型动态更新机制，持续纳入新的攻击样本数据，确保模型能够及时适应不断变化和演进的攻击手段。

3.2 基于强化学习的传输路径与参数优化技术

基于强化学习的传输路径与参数优化技术，为云计算通信网络传输过程的自适应优化提供了有效手段。（1）该技术把网络传输过程巧妙地建模为强化学习中智能体与环境交互的过程，将提升传输效率、降低安全风险设定为奖励目标。智能体在这个虚拟环境中持续进行探索与学习，不断试错并积累经验，最终获取最优的传输路径选择策略和参数调节策略。（2）在传输路径优化方面，智能体能够实时、精准地感知网络各链路的带宽、延迟、安全状态等关键环境信息，依据这些信息动态地选择最优传输路径，避开拥堵或存在安全隐患的链路。在传输参数调节上，它能根据数据传输的类型以及网络当前的负载情况，自适应地调节传输速率、重传机制等重要参数。凭借强化学习所具备的自适应能力，该技术可以快速响应网络拓扑结构的变化以及负载的波动，切实保障数据传输的稳定性与安全性。

3.3 基于深度学习的动态数据加密传输技术

基于深度学习的动态数据加密传输技术为云计算通信网络中的数据传输隐私保护提供了极为高效的解决方案。（1）此技术借助深度学习算法，深入挖掘传输数据的内在特征，依据数据的重要程度和敏感级别，自动且精准地划分加密等级，并为其匹配适宜的加密算法与密钥管理策略。（2）针对高敏感数据，会采用高强度的加密算法，利用深度学习模型生成动态密钥，并定期更新密钥，以此大幅提升加密的安全性，防止数据被非法窃取或篡改。而对于普通数据，则选用轻量化的加密算法，在确保数据安全的前提下，有效降低数据传输与解密过程中产生的延迟，提升传输效率。此外，该技术还能运用深度学习算法实时监测加密数据的传输状态，一旦发现存在加密破解风险，便会迅速动态调整加密策略，从而实现对数据传输全流程的动态、全面且可靠的安全防护[3]。

4 基于人工智能的云计算通信网络安全传输控制技术应用的常见问题与解决思路

4.1 模型训练数据质量不足问题及解决思路

在基于人工智能的云计算通信网络安全传输控制技术应用中，模型训练数据质量不足是较为突出的问题。其

具体表现为数据样本存在不完整情况，部分关键信息缺失；标签标注不准确，与实际数据特征不符；数据分布不均衡，某些类别样本数量过多，而另一些则过少。这些问题会直接致使人工智能模型的识别精度降低，泛化能力变弱，无法在实际应用中准确、稳定地发挥作用。

为解决这些问题，要构建完善的数据采集与预处理体系。一方面，扩大数据采集范围，从更多渠道、更广泛场景收集数据，保证数据样本的多样性与完整性。另一方面，运用数据清洗技术去除异常数据，通过建立数据标注校验机制，提高标签的准确性。还可采用数据增强技术对稀缺样本进行扩充，调节数据分布的均衡性。此外，建立数据质量评估指标体系，定期对训练数据质量进行量化评估，确保输入模型的数据达到训练要求，从而提升模型性能。

4.2 技术兼容性差问题及解决思路

在基于人工智能的云计算通信网络安全传输控制技术实际应用中，技术兼容性差是一个亟待解决的问题。其具体表现为该安全传输控制技术与现有的云计算通信网络架构、硬件设备以及传输协议等存在不匹配的情况，这使得技术难以顺利集成并投入应用，影响整体安全传输控制效果的发挥。

为解决这一问题，在技术研发阶段就需高度重视兼容性设计。研发人员要充分调研现有网络架构和各类硬件设备的特性，采用模块化、标准化的技术架构，增强技术对不同环境的适配能力。同时，开发通用接口与适配插件，以此实现与不同网络设备、传输协议的无缝对接，降低集成难度。此外，在技术应用之前，要开展全面且充分的兼容性测试，详细记录测试过程中出现的兼容性问题，并针对这些问题进行有针对性的优化和改进，确保该技术能够平稳、高效地集成到现有的网络体系当中。

4.3 实时性有待提升问题及解决思路

在基于人工智能的云计算通信网络安全传输控制技术应用中，实时性不足是一个突出问题。这主要是因为人工智能模型计算复杂度颇高，且数据传输与分析环节存在较大延迟，使得该技术难以契合云计算通信网络高速数据传输时对实时控制的要求。

为解决此问题，首先要对人工智能模型结构进行优化，采用轻量化模型设计理念，精简模型计算流程，去除不必要的冗余计算，从而有效降低模型推理延迟。其次，可借助边缘计算技术，把部分智能分析与控制功能合理部署在边缘节点。如此一来，数据无需长距离传输到云端，减少了传输延迟，能在本地快速完成分析与控制操作。此外，还需优化数据传输与处理流程，运用并行计算技术，让多个计算任务同时开展，大幅提升数据处理效率，确保该技术可以迅速响应网络传输状态的动态变化以及各类攻击行为，满足实时控制需求[4]。

结束语

综上所述，基于人工智能的云计算通信网络安全传输控制技术意义重大，其核心技术架构涵盖数据采集、智能分析与传输控制层，关键技术包含攻击识别预警、传输路径参数优化及动态数据加密传输等。尽管在应用中面临模型训练数据质量不足、技术兼容性差、实时性有待提升等常见问题，但通过构建完善的数据体系、强化兼容性设计、优化模型与数据处理流程等针对性解决思路，可有效应对挑战。随着技术的持续发展与创新，该技术必将在保障云计算通信网络安全传输方面发挥更为关键的作用，推动云计算通信网络向更安全、高效、智能的方向稳步迈进。

参考文献

[1]郭黎明.计算机通信技术中网络远程控制研究[J].通信电源技术,2023,40(2):131-133.

[2]陈功,陶晓霞,刘丹妮.虚拟现实技术在计算机网络通信中的应用[J].中国宽带,2023,19(12):88-90.

[3]宗燕,颜实.计算机网络通信工程中的数据加密技术及实践研究[J].软件,2023,44(10):176-178.

[4]赵笛杉.大数据时代计算机远程网络通信技术创新研究[J].科技视界,2023(35):74-76.