文章类型：论文|刊号（ISSN）：2972-4236(P) / 2972-4244(O)

人工智能技术在视频会议安全领域的应用

李明慧　李福霞
博鼎实华（北京）技术有限公司
DOI:10.12238/acair.v3i2.13554

[摘　要] 目前视频会议的安全问题成为亟需解决的关键问题,而人工智能技术为视频会议系统的安全保障提供了新的思路和方法。本文通过研究视频会议系统面临的安全威胁,并且在身份认证、数据加密传输、漏洞防范和内容与业务管理等方面,分析了人工智能用于视频会议系统安全保障的方法和措施,最后展望了人工智能在视频会议系统应用的趋势和带来的挑战。
[关键词] 人工智能；视频会议系统；安全
中图分类号：TP18　文献标识码：A

The Application of Artificial Intelligence Technology in the Field of Video Conferencing Security

Minghui Li　Fuxia Li
Potin(Beijing)Technology Co.,Ltd

[Abstract] At present, the security issue of video conferencing has become a key problem that urgently needs to be solved, and artificial intelligence technology provides new ideas and methods for the security guarantee of video conferencing systems. This article studies the security threats faced by video conferencing systems and analyzes the methods and measures of using artificial intelligence for security protection in areas such as identity authentication, data encryption transmission, vulnerability prevention, and content and business management. Finally, it looks forward to the trends and challenges brought by the application of artificial intelligence in video conferencing systems.
[Key words] Artificial Intelligence; Video Conferencing System; Security

引言

随着云计算、超高清和AI等技术的快速发展,视频会议行业呈现出前所未有的蓬勃发展和技术创新态势。据预测,2025年中国会议视频系统市场规模将达到304.1亿元,同比增长近25%。到2030年,这一数字将进一步攀升至488.1亿元。目前视频会议系统广泛用于办公协作、远程教育、远程医疗和应急指挥等场景,随着视频会议系统开放程度的提升以及部署网络环境的日趋复杂,视频会议系统的安全性成为亟需解决的关键问题。人工智能技术的发展为视频会议系统的安全保障提供了新的思路和方法。

1 视频会议系统安全概述

1.1视频会议系统

视频会议系统通常是指融合了多种通信技术,为异地用户提供多方、交互且实时的视音频通信和数据共享业务的通信系统。视频会议系统包括传统的基于硬件的视频会议系统和云视频会议系统。

传统的视频会议系统主要由用户终端、通信网络和多点控制单元(MCU)组成。用户终端由摄像头、麦克风、显示器、扬声器和编解码器等组成,负责采集视频和音频信号等数据编码发送,并将通过通信网络传输后收到的数据解码播放。通信网络可以是运营商公网、互联网、行业专网和企业内网等,承担数据传输的任务。多点控制单元用于实现信息和视音频数据的交换与处理。传统视频会议系统部署复杂,维护成本较高,适合对安全性要求高、在固定场所进行的专用、大型会议等。

云视频会议是一种基于云计算技术构建的视频会议解决方案,通过云计算中的虚拟化、分布式计算、弹性伸缩等技术手段,将视频会议系统的业务逻辑、信令交互与媒体流处理等过程在云端实现,支持会议室终端、PC、平板和智能手机等多种异构终端设备的接入,可以实现丰富的应用场景和跨平台协作。云视频会议系统具有低成本、高灵活性和强大的可扩展性,适合远程办公、在线教育、中小型企业协作等场景。

1.2视频会议系统的安全风险

1.2.1网络攻击威胁

网络攻击是视频会议系统面临的主要安全威胁之一,其中分布式拒绝服务(DDoS)攻击较为常见,并且DDoS攻击往往与其他类型的网络攻击相结合,形成混合攻击。攻击者通过向视频会

议服务器发送海量请求,使得服务器过载而无法响应正常用户的请求。另外中间人攻击也是一种常见的网络攻击手段,攻击者在通信过程中拦截、篡改或窃取数据。例如在视频会议中,攻击者可能拦截视频和音频数据,获取会议内容;或者篡改会议控制指令,干扰会议的正常进行。

1.2.2数据泄露风险

视频会议中涉及大量敏感数据,如企业的商业机密、个人的隐私信息等。视频会议的数据通过网络传输,如果未采用加密技术,攻击者可能通过网络监听工具截获传输中的数据信息。例如,在使用不安全的网络协议时,数据包可能在传输过程中被恶意用户截获并解码。另外如果视频会议平台或设备的存储系统存在漏洞,攻击者可能利用漏洞获取存储的会议记录、录制文件等敏感数据。

1.2.3未授权访问及身份冒用

如果会议链接或密码被泄露,未经授权的人员可能会加入会议并获取敏感信息;当视频会议系统使用简单的密码验证时,容易让攻击者通过暴力破解方式进入会议; 另外不法分子可能通过伪造身份信息,如利用技术手段注入预先录制的视频,伪装成合法参会者进入会议,或者通过深度伪造技术替换自己的面部图像、借助语音合成技术伪造他人的声音,冒用他人身份。

2 人工智能技术及应用

2.1机器学习

机器学习通过设计和构建模型,让计算机从大量的数据中自动学习规律和模式,然后利用这些学到的知识来对新的数据进行预测、分类或决策。

在视频会议系统中,机器学习可以用于训练模型来识别已知的安全威胁。例如,通过收集大量的正常网络流量数据和恶意攻击流量数据作为训练集,训练一个分类模型。当网络流量进入视频会议系统时,模型可以根据学习到的模式判断该流量是否为恶意流量。

2.2深度学习

深度学习基于对数据进行表征学习的方法,通过构建具有很多层的神经网络,让计算机自动从大量数据中学习复杂的特征表示。

在视频会议系统中,深度学习在图像和语音处理方面具有显著优势。例如,在人脸识别用于身份认证时,深度学习神经网络可以学习人脸的各种特征,包括面部轮廓、五官比例等。通过对大量人脸图像的学习,模型能够准确识别出不同的人脸,从而实现参会人员的身份验证。

2.3自然语言处理

自然语言处理旨在使计算机能够读取、理解、生成和交互自然语言文本或语音,实现人机之间以自然语言进行有效的信息交流。

在视频会议系统中,自然语言处理可用于实时翻译功能,方便跨国交流。同时,自然语言处理还可用于会议内容分析,例如检测会议文本中是否存在敏感信息,如商业机密、隐私内容等。通过对大量文本数据的学习,模型可以识别出具有特定含义的词汇和语句,从而判断会议内容是否安全。

2.4计算机视觉

计算机视觉通过图像处理和深度学习技术,使计算机能够理解和解释视觉信息,并从图像或视频中提取有意义的信息,实现对目标物体的识别、跟踪和定位。

在视频会议系统中,通过图像处理和深度学习技术,实现对目标物体的识别、跟踪和定位,同时可以实现对视频内容的分析,例如基于目标检测模型实时识别视频中的异常区域(如AI换脸、伪造背景),结合画面时序一致性分析,阻断恶意伪造攻击。

2.5强化学习

强化学习通过试错让智能体学习如何在环境中做决策,适用于需要动态决策的场景。智能体通过与环境进行交互,根据环境反馈的奖励信号来学习最优的行为策略。

强化学习模型能够实时分析并提供智能建议,提升决策质量。在会议讨论过程中,AI智能助手能够实时对会议中的语音、文字等信息进行分析,挖掘其中的关键数据和潜在趋势,为参会者提供智能建议,辅助决策。例如根据数据模型预测出方案的市场反应,从而做出更加科学、合理的市场战略决策。

3 人工智能技术在视频会议安全领域的应用分析

3.1身份认证

视频会议系统身份认证的常用AI技术是人脸识别和声纹识别。人脸识别技术可以用于会议签到、培训点名等场景。声纹识别技术可以用于身份认证、智能语音跟踪等场景。但基于人脸和声纹的生物特征识别技术各自具有局限性,因此需要将不同生物特征模态结合后进行识别可以弥补单模态的不足之处,显著降低冒名欺骗的可能性。多模态生物识别技术是综合利用多种生物特征(如面部、声纹、虹膜、指纹、步态等)进行身份认证,关键技术是数据采集、特征提取和融合,模式识别和分类等,通过融合来自多个模态的生物特征数据来增强识别精度和鲁棒性,可实时验证用户生物特征的真实性,并依据环境光照、噪声强度动态调整认证阈值,有效提升识别的准确性,防止身份冒用问题。

3.2数据加密与传输安全

3.2.1加密算法优化和背景虚拟化

根据不同的应用和安全要求,人工智能可以实时分析数据流的特征,动态调整加密策略、加密算法的参数或切换不同的加密方法,也可以通过人工智能技术(如深度学习、神经网络等)来优化加密算法的设计,调整算法参数,平衡安全强度与计算开销,改进加密性能,确保数据安全的同时优化资源使用。

视频会议中,背景环境的摄入可能暴露私人空间或分散与会者注意力,从而影响会议效果。通过视频会议的虚拟背景功能,可以改变会议参与者所见的背景,提供了隐私保护的重要保障,让参会者在放松的环境下进行沟通。

3.2.2传输过程监控

人工智能技术可用于实时监控视频会议数据的传输过程。通

过建立正常数据传输的模型,利用机器学习算法对网络流量进行实时分析。当网络流量出现异常时,如流量突然大幅增加、数据传输速率异常波动等,系统能够及时发出警报。同时,人工智能还可以对网络流量的内容进行分析,检测是否存在数据被篡改的情况。通过对数据的校验和、哈希值等特征进行学习和比对,一旦发现数据特征与正常情况不符,即可判断数据可能被篡改,从而保障数据传输的完整性和安全性。在视频会议系统中,基于强化学习模型,通过算法分析流量特征,可以精准识别恶意流量提升异常行为检测效率。

3.3安全漏洞检测与防范

3.3.1漏洞扫描与分析

传统的漏洞扫描技术存在误报率高、效率低、检测不全面等问题。与依赖已知漏洞库的传统工具不同,基于机器学习的系统能通过学习正常网络行为模式和常见漏洞特征建立模型,及时发现异常行为,通过分析海量数据发现安全漏洞。目前基于人工智能的漏洞扫描有多种方式,如大模型直接用于漏洞挖掘、大模型辅助模糊测试和大模型辅助静态分析等。与传统工具相比,人工智能漏洞扫描虽然具有一定的局限性,但通常更准确,能检测更多新漏洞。

3.3.2实时防护与预警

一旦人工智能检测到视频会议系统存在安全漏洞或遭受攻击,能够立即采取实时防护措施并发出预警。例如,当检测到系统受到SQL注入攻击时,系统可以自动阻断可疑的数据库查询请求,防止攻击者获取敏感数据。同时,向管理员发送预警信息,告知攻击类型、发生时间和可能的影响范围等详细信息。在预警方面,人工智能还可以通过对历史攻击数据的学习,预测可能发生的攻击类型和时间,提前做好防范准备。例如,根据以往的攻击记录,发现每周一上午网络攻击的发生率较高,系统可以在该时间段自动加强安全防护措施,提高系统的安全性。

3.4数据内容安全管理

3.4.1敏感信息检测

利用人工智能的自然语言处理技术,视频会议系统可以对会议内容进行实时敏感信息检测。首先,通过对大量包含敏感信息的文本数据进行学习,建立敏感信息识别模型。模型可以识别出诸如商业机密、个人身份证号码、银行卡号等敏感信息。在会议进行过程中,系统对语音转文字后的文本内容或会议聊天窗口中的文字内容进行实时分析。一旦检测到敏感信息,系统可以采取相应的措施,如对敏感信息进行模糊处理、提醒参会人员注意信息安全等。

3.4.2恶意内容过滤

人工智能还可以识别和过滤视频会议中的恶意内容,如广告、垃圾信息等。通过对大量正常会议内容和恶意内容的学习,建立分类模型。当会议中出现新的内容时,模型可以快速判断其是否为恶意内容。对于恶意内容,系统可以自动进行过滤,避免其干扰会议的正常进行。例如,在一些免费的视频会议平台中,经常会出现恶意广告的推送,影响用户体验。采用人工智能技术进行恶意内容过滤后,广告等恶意信息的出现频率大幅降低,提升了会议的质量和用户体验。

3.5业务安全

随着DeepSeek的横空出世,集成AI大模型成为视频会议的发展趋势之一。凭借语音识别、自然语言处理、强化学习等核心技术,规划设计覆盖会前、会中、会后全流程的智能化解决方案,并在会议流程中的各环节帮助实现视频会议的安全保障。例如智能会议通过一键创会,实现会议通知的批量发送和自动确认,召集参会人员；会议过程中支持快速上传文件,避免人为流程中的误操作;通过权限分级,给不同人员分配不同的操作权限,确保会议流程规范与数据安全;通过AI会议助手,用户不仅能够感知会议环境,通过自然语言指令完成各种会议操作,还可以进行故障排查分析等操作保障会议安全。

4 结束语

人工智能技术在视频会议中的安全应用促进了视频会议全流程的自动化和智能化,极大地提升了视频会议的效率和便捷性,也增强了用户体验。人工智能在安全领域的深入应用,可以在一定程度上解决传统视频会议的安全问题,但相应的也会带来新的问题,如AI本身需要大量的计算资源,能耗成本高。如何在保证安全性的同时,降低计算复杂度是研究的一个重要方向。未来,随着人工智能、大数据和边缘计算等技术的进步,人工智能和视频会议系统的结合会更加紧密,提供更有效的措施保障视频会议的安全,为社会发展和民生提供更安全、可靠的会议服务保障。

[参考文献]

[1]中研普华产业研究院,2025-2030年会议视频系统产业深度调研及未来发展现状趋势预测报告.

[2]东方隐侠安全团队-千里,DeepSeek(AI)如何赋能智能漏洞扫描与利用的思考,csdn,2025.

[3]曾程,黎静,赵高永,等.视频会议系统的安全防护体系及技术演进[J].保密科学技术,2022,(02):24-31.

作者简介：

李明慧(1975--),女,汉族,河北秦皇岛人,硕士,博鼎实华(北京)技术有限公司,高级工程师,研究方向：多媒体通信。

李福霞(1983--),女,汉族,山东龙口人,硕士,博鼎实华(北京)技术有限公司,工程师,研究方向：计算机通信。