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

基于自主智能的云视频会议系统大数据隐私保护研究

李明慧　付学涛
博鼎实华（北京）技术有限公司
DOI:10.12238/acair.v3i2.13557

[摘　要] 随着云视频会议的广泛应用,会议产生的大量数据面临着安全威胁。基于此,本文通过研究分析大数据隐私保护技术和自主智能关键技术,建立两者结合的动态隐私保护模型方案,保障云视频会议系统的安全性,并对未来发展挑战与趋势进行展望。
[关键词] 云视频会议系统；大数据隐私保护；自主智能系统
中图分类号：C37　文献标识码：A

Research on Big Data Privacy Protection in Cloud Video Conferencing Systems Based on Autonomous Intelligence

Minghui Li　Xuetao Fu
Potin(Beijing)Technology Co.,Ltd

[Abstract] With the widespread application of cloud video conferencing, the large amount of data generated from meetings is facing security threats. By researching and analyzing big data privacy protection technologies and key technologies of autonomous intelligence, a dynamic privacy protection model that integrates both is established to ensure the security of cloud video conferencing systems. The future development challenges and trends are also looked forward to.
[Key words] Cloud Video Conferencing System; Big Data Privacy Protection; Autonomous Intelligent System

1 行业背景

目前云视频会议系统已经成为企业、教育机构、政府部门等众多组织实现远程高效沟通协作不可或缺的重要工具。根据市场调研机构Business Research Insights提供的数据,2023年全球云视频会议市场规模大约为81.3亿美元。据预测,到2032年,这个数字预计将飙升至202.1亿美元。云视频会议市场迎来了前所未有的发展机遇,会议产生的大数据的隐私保护也成为研究的关键课题。

1.1国内外研究现状

在国外,美国斯坦福大学的研究人员致力于开发基于自主智能算法的加密技术,能够依据会议数据的敏感度与使用场景,自动匹配最优加密策略,实现高效隐私保护。微软公司在其云视频会议产品中,引入自主智能的访问控制机制,通过持续学习和分析用户行为,实时动态调整访问权限,有效防范非法访问行为。

在国内,清华大学的学者提出一种基于区块链和自主智能系统的云视频会议隐私保护方案,利用区块链的不可篡改特性与自主智能系统的智能决策能力,保障数据的安全性与隐私性。华为、腾讯等企业也在不断探索创新,华为通过自主研发的智能安全引擎,对云视频会议数据进行实时监测与防护;腾讯则借助人工智能技术对会议内容进行智能识别与脱敏处理。尽管国内外在该领域已取得一定成果,但在技术融合的深度与广度、实际应用的普适性等方面仍存在提升空间,亟待进一步深入研究。

2 云视频会议系统概述

2.1系统架构与工作原理

云视频会议系统主要由用户终端、通信网络和云服务平台三大部分构成。用户终端包括专业的会议室终端、PC、平板和智能手机等。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,承担数据传输任务。云服务平台是系统的核心,主要负责会议管理、媒体处理分发、数据的存储与处理,涵盖会议管理模块、媒体处理模块、数据存储模块以及安全管理模块等。用户发起会议时,用户终端采集音视频信号,编码压缩后经网络传输至云平台。云服务平台根据会议需求对数据进行处理与分发,将多路音视频流进行混合处理后同步分发给参会者。会议过程中产生的文字聊天记录、文件等数据,也通过网络传输至平台进行统一存储与管理。会议结束后,部分数据将被保留,用于回放、归档或后续分析等。

2.2数据特点与隐私风险

云视频会议系统产生的数据具有体量庞大、类型多样、实时性强以及隐私敏感性高等特点。一场持续数小时的大型会议,

可能产生数GB甚至数TB的数据,涵盖结构化数据(如用户信息、会议信息)、半结构化数据(如会议纪要,聊天信息)和非结构化数据(如音视频、图片)。此外,会议过程需要实时传输和处理音视频数据,以保证流畅交互。

由于这些数据涉及用户个人隐私与商业机密,如身份信息、会议讨论的敏感业务内容等,云视频会议系统面临诸多安全风险。网络攻击是主要威胁之一,黑客通过DDoS攻击、中间人攻击、SQL注入攻击等手段,拦截、篡改或窃取会议数据。2023年,某知名云视频会议平台遭受大规模DDoS攻击,导致系统瘫痪数小时,期间大量用户数据面临泄露风险。恶意软件入侵也是常见问题,木马、病毒等可通过用户终端或云服务平台漏洞植入,窃取隐私信息。内部人员违规行为同样不容忽视,云服务平台管理员或企业内部有权限人员,可能因疏忽或恶意目的泄露用户数据。此外,数据共享与第三方合作过程中,若共享机制不完善,数据在传输和使用环节也可能被泄露和滥用。

3 数据隐私保护技术

3.1加密技术

加密技术是大数据隐私保护的核心和基础手段。对称加密算法如高级加密标准(AES),具有高效的加密和解密速度,广泛应用于音视频数据的实时加密传输。非对称加密算法如RSA,常用于身份认证和密钥交换环节。在用户登录云视频会议系统时,可采用单向或双向数字证书用于身份验证,确保合法用户进入会议,并通过RSA算法进行密钥交换,为后续对称加密通信建立安全密钥通道。目前商密算法SM2、SM3、SM4也已经广泛应用于云视频会议系统。

同态加密作为新兴加密技术,允许在加密数据上直接进行计算,无需解密原始数据。在对会议记录进行统计分析时,利用同态加密技术,云服务平台可直接对密文数据计算,得出统计结果,而无需接触原始明文数据,从而大幅提高了数据隐私保护能力。

3.2数据匿名化与脱敏技术

数据匿名化通过去除或替换数据中能直接或间接识别个体的信息,使数据无法与特定个人关联。在云视频会议系统中,可采用假名化技术,将用户真实身份信息替换为随机生成的标识符。在会议记录中,将用户真实姓名替换为唯一ID,并对IP地址、设备指纹等可能识别身份的信息处理,显著降低数据泄露和隐私泄露的风险。

数据脱敏技术对敏感信息进行变形和模糊处理,将敏感数据转换成无法还原的形式。对于会议中的敏感文字内容,如商业机密、个人身份证号码等,采用字符替换、截断、屏蔽等方式脱敏。将身份证号码部分数字替换为星号,既保留数据的必要特征以供业务流程使用,又能有效保护个人隐私。差分隐私通过在数据中添加适量噪声,使攻击者难以从数据分析结果推断个体信息,保障数据可用性的同时强化隐私保护。

3.3访问控制技术

访问控制技术通过限制用户对数据的访问权限,确保只有授权人员能获取和操作相关数据。在云视频会议系统中,基于角色的访问控制(RBAC)是常用方式。根据用户在组织中的角色,如管理员、普通参会者、嘉宾等,分配不同权限。

目前属性基加密(ABE)技术也逐渐应用于云视频会议系统访问控制。ABE根据用户属性,如部门、职位、会议参与级别等,对数据加密和权限控制。只有具有相应属性的用户才能解密和访问数据。某企业核心商业会议数据,只有特定部门高级管理人员能访问,通过ABE技术可基于这些人员部门和职位属性进行加密与权限设置。自主访问控制(DAC)赋予用户对自己创建的数据一定访问控制权,用户可自主决定将数据共享给其他用户,但DAC存在安全风险,若用户账号被盗用,攻击者可能利用权限访问和泄露数据。因此,实际应用中,常常将多种访问控制技术结合,提高访问控制安全性和灵活性。

4 自主智能系统关键技术

4.1机器学习技术

机器学习是构建自主智能系统的核心技术之一。在云视频会议系统大数据隐私保护中,监督学习通过收集和标注大量正常数据和隐私威胁数据样本,训练分类模型,以实现对新输入数据中潜在隐私风险的准确识别。无监督学习用于发现数据中的异常行为,在网络流量数据中,识别与正常流量模式差异较大的流量,可能预示着网络攻击行为,从而实现早期预警。以DDoS攻击为例,系统通过识别特定时间段内突增的异常流量,结合数据传输行为变化,即可及时判断并发出攻击预警。

4.2深度学习技术

深度学习在图像识别和语音处理领域具有显著优势,广泛应用于云视频会议的安全保障中。在云视频会议中,利用深度学习的人脸识别技术进行参会人员身份认证,确保只有授权用户能够进入会议,有效防止身份冒用导致隐私泄露。语音识别技术对会议中的语音内容实时分析,自动识别并标记敏感信息。如通过语音识别技术,实时监测会议语音,若识别到涉及商业机密的关键词,及时提醒或启动保密措施机制。此外,深度学习还可用于增强数据加密算法的优化加密算法,提高数据加密和解密效率与安全性。通过生成对抗网络(GAN)等模型形成更复杂且难以破解的加密密钥,有效提升通信过程中的数据保密能力。

4.3自然语言处理技术

自然语言处理(NLP)技术在云视频会议系统的隐私保护中具有广泛应用价值。首先,通过会议内容的文本转写和情感分析,可对会议中涉及的敏感内容进行智能识别。例如,系统可实时将会议语音转换为文本并进行语义分析,识别包含政治、商业或个人隐私等敏感词汇,并对相关内容进行脱敏处理或触发预警机制。NLP结合命名实体识别(NER)技术,能够从会议文本中自动提取人名、公司名、地名、账户信息等敏感实体,并进行标注与加密。在涉及多语种会议时,多语言处理技术可确保对不同语种的内容实现统一隐私防护标准。NLP还可用于自动生成会议纪要,既提升效率,又减少人工干预,降低人为泄露隐私的风险。

5 大数据隐私保护与自主智能系统的结合应用

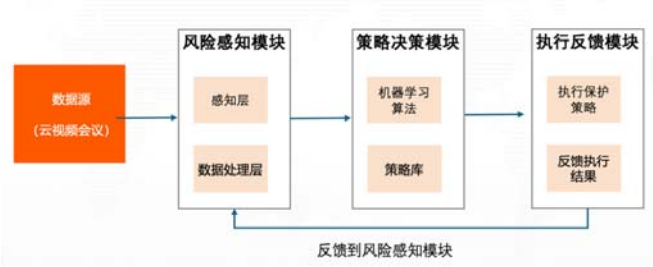
5.1动态隐私保护模型

为了提升对云视频会议系统的数据隐私保护能力，文章提出并构建了一种基于自主智能系统构建动态隐私保护模型，该模型主要包括风险感知模块、策略决策模块和执行反馈模块。

(1)风险感知模块通过自主智能系统的感知层和数据处理层，实时收集和分析云视频会议系统中的各类数据，识别潜在隐私风险，并对风险量化评估，如确定风险等级、影响范围等。

(2)策略决策模块根据风险感知模块提供的风险信息，利用机器学习算法和预定义的策略库，制定相应隐私保护策略。策略库包含针对不同类型风险的多种保护策略，如加密算法选择、访问权限调整方案等。系统根据风险具体情况，从策略库中选择最优策略或组合策略。

(3)执行反馈模块负责执行策略决策模块制定的隐私保护策略，并将执行结果反馈给风险感知模块和策略决策模块。风险感知模块根据反馈结果，评估策略执行效果，若隐私风险未有效控制，策略决策模块重新调整策略，形成闭环的动态隐私保护机制。



图一 动态隐私保护模型

5.2动态隐私保护模型在不同领域的应用

动态隐私保护模型可以用于金融、医疗、政企、交通等不同业务领域，在会议、会诊、办公协作等方面动态调整并执行隐私保护策略，保证云视频会议系统的安全。

在金融行业云视频会议中，涉及大量敏感财务数据、客户信息等。自主智能系统实时监测会议数据传输，利用加密技术对敏感数据实时加密。当检测到异常数据访问行为，如非授权人员试图访问高敏感度财务报表数据时，系统自动提升访问权限验证级别，采用多因素认证方式，同时对该数据进行更高级别加密处理，防止数据泄露。

医疗领域远程会诊视频会议中，患者病历、病情诊断等隐私信息至关重要。自主智能系统通过自然语言处理技术对会诊中的语音和文字内容分析，识别敏感医疗信息。一旦发现信息可能被不当泄露风险，如聊天记录中出现患者个人敏感病情描述且发送给未授权人员，系统立即对相关信息脱敏处理，并向会诊医生发出隐私风险提醒，保障患者隐私安全。

企业商业机密讨论会议中，自主智能系统根据参会人员角色和行为，动态调整访问权限。如发现某参会人员频繁尝试访问超出其权限的机密数据，系统及时限制其访问，并记录相关行为，以便后续审计。同时，利用加密技术对会议中的机密数据全程加密，确保数据在传输和存储过程中的安全性。

6 结束语

随着云视频会议系统的广泛普及，如何在提升用户体验的同时保障数据隐私安全，已成为业界重要课题。本文从系统架构、数据特征出发，系统梳理了面临的隐私风险，并提出了以自主智能系统为核心的多维度技术融合策略。通过加密、脱敏、访问控制等基础手段，结合机器学习、深度学习、自然语言处理等智能技术，构建更加智能化、灵活化的数据保护体系。未来，随着联邦学习、边缘计算等技术的进一步成熟，云视频会议系统将朝着“安全智能协同”的方向持续演进，推动隐私保护技术在更大范围内的落地应用。

[参考文献]

[1]冯登国.大数据安全与隐私保护[M].北京:清华大学出版社,2018.

[2]何强.大数据环境下的隐私保护与访问控制模型研究[J].信息与电脑,2025,37(04):26-28.

[3]廖芳,李雪松,杨力,等.大数据应用中的数据安全保障技术研究[J].中国新通信,2025,27(03):34-36.

[4]Samarth K.Patil,etc.Integrating Artificial Intelligence and Encryption in Web Real-Time Communication: A Smart Video Conferencing Platform With Real-Time Transcription and Translation[J],Cureus Journal Of Computer Science,2025(4).

[5]云视频会议市场报告概述.https://www.businessresearchinsights.com/zh/market-reports/cloud-video-conferencing-market-100473. Business Research Insights,2025.

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。

付学涛(1975--),女,汉族,北京人,本科,博鼎实华(北京)技术有限公司,工程师,研究方向：密码通信。