云通讯在远程协作场景中的安全传输技术创新

陈玉琪

杭州三体科技股份有限公司，浙江杭州，310000；

摘要：随着云计算和移动互联网技术的快速发展，云通讯已成为支撑远程协作系统的关键基础设施。远程办公、在线医疗、虚拟教育等场景对高可靠、低延迟、强安全的通信需求不断提升，尤其在数据传输环节中，对加密性、完整性和抗攻击能力提出了更高标准。本文从云通讯在远程协作场景中的典型应用出发，分析现有传输面临的核心安全挑战，进一步探讨在协议加密、动态认证、数据隔离、边缘安全等方面的技术创新，提出多层次、可扩展的安全传输解决方案，旨在为云通讯平台建设提供系统性的安全设计参考。

关键词：云通讯；远程协作；安全传输；加密认证；数据防护；边缘计算

DOI：10.64216/3080-1508.25.03.041

引言

数字化转型浪潮推动着组织间协作模式的根本变革，远程办公、异地协作、跨网作业等新型工作方式日益普及。作为支撑这些模式的关键技术，云通讯通过音视频传输、即时消息、共享文档、远程控制等多维交互功能，为构建无边界的实时协作空间提供了基础保障。与此同时，数据在网络中高频流动、终端类型多样、环境异构化等特征也加剧了信息泄露、内容篡改、身份伪装、拒绝服务等安全风险，成为阻碍远程协作进一步普及的技术瓶颈。传统网络安全体系难以直接适应云通讯的高并发、低延迟、敏捷部署特性，亟需从体系架构、协议机制、加密算法、认证方式等层面进行重塑创新。本文从多维场景需求出发，深入剖析云通讯传输过程中存在的核心风险与隐患，进一步提出基于动态密钥协商、信道隔离、多因子身份识别、可信边缘节点等技术的综合解决策略，构建面向未来协作生态的云通讯安全防护体系。

1 远程协作场景下云通讯系统的应用特点与安全诉求

1.1 多终端异构接入带来的安全通道挑战

在远程协作环境中，用户可能通过手机、平板、笔记本、桌面终端甚至智能穿戴设备接入同一通讯系统。这些终端所处网络环境差异极大，包括企业专网、家庭 Wi-Fi、4G/5G 公网、物联网边缘网络等，存在 NAT 穿透困难、网络质量不稳定、系统安全策略不统一等问题。云通讯系统需对接入终端进行统一认证和资源授权，确保每一类设备在传输层、应用层的通讯行为合法可信。而多终端异构接入也意味着攻击面随之扩大，如流量劫持、中间人攻击、会话注入等风险愈加频繁。因此，保障通信链路中数据的机密性、完整性和可验证性，构建终端到云端之间的可信传输机制，是设计安全传输系统的首要前提。

1.2 多角色协同交互催生动态权限控制需求

远程协作场景往往涉及不同角色间的频繁信息交换，如管理者、操作者、访客、外部协作方等。这些角色权限的边界可能随着会议进展、项目阶段或文档状态实时变化，从而产生动态授权、权限转移、访问审计等一系列复杂管理需求。例如，某远程设计协作平台中，设计者可随时调用云端图纸进行修改，而审查人员只能在规定时间内查看部分内容，这种精细化控制无法依赖传统静态 ACL（访问控制列表）实现。云通讯平台必须引入基于策略的访问控制（PBAC）模型，结合上下文感知技术，动态生成安全策略并实时应用于通讯会话中。同时，传输过程中还需记录审计链，确保通信数据可回溯、不可篡改，满足安全合规要求。

1.3 高并发低延迟传输对加密算法性能提出新挑战

远程办公、在线教育等典型场景常常伴随音视频实时传输、高频互动和突发并发访问，对通讯系统的延迟容忍度极低。尤其在音视频通话、屏幕共享、在线白板等功能中，任何微小的延迟都会严重影响用户体验。这就对安全传输中的加密解密算法提出了高性能要求。传统的对称加密（如 AES）虽具备高速性，但密钥协商难以支持大规模会话；非对称加密（如 RSA）安全性高但计算成本大；哈希签名与完整性校验机制也需在安全与速度之间权衡。因此，构建适应高并发场景的轻量化加密框架，采用算法混合、多通道异步处理、并发压缩传输等方式，成为提升安全性与体验感的核心课题。

2 安全传输体系的核心技术创新路径

2.1 多层级加密机制构建纵深防护架构

云通讯平台在远程协作时会遇到很多安全威胁，这些安全问题有好多方面而且变得很复杂的情况。攻击者会在各个层面发起攻击比如窃听或者篡改数据这些操作所以只用一种加密方法或者固定密钥的话，现在根本挡不住那些越来越厉害的攻击方式。为了解决这个问题必须搞多层次的加密体系来进行全面保护，这已经成为技术发展的重点方向。整个体系应该包括信号层、传输层还有应用数据层这些部分，搞成每层之间互相支持的结构。在信号控制层主要用 TLS1.3 协议，这个协议有个特点就是能保证就算密钥泄漏了之前的通信也不会被破解，这样就能防止被人偷听。在传输层的话用的是 SRTP 协议，专门给语音视频加密的，搭配 DTLS 协议一起使用时能在传输过程中每个数据包都加密和确认身份，这样就能防止中间人攻击

应用层安全方面变得非常重要，特别是在多人共享文件、白板协作、远程控制这些高敏感操作时候，最好使用 E2EE 方式加密策略，这种就是在用户自己设备上进行加密解密，不需要通过服务器来中转，从根本上避免云平台或者其他数据处理节点非法获取内容。为了加强系统的稳定性，还应该设计根据时间或者操作行为触发密钥定期动态更新的方式，再加上每个会话单独用不同的密钥和临时令牌的机制，这样就算某个密钥被泄漏了，也不会让其他会话内容的安全性受影响，这样就形成了能够自我恢复和抵抗攻击的整体的加密防护结构。

2.2 基于可信身份的多因子动态认证体系

身份安全总是云通讯防护系统的首要防线，尤其是在远程协作时候，攻击者可能会假冒登录、横向移动或者权限升级等手段入侵系统。传统的固定密码为主的认证方式已经不太适合现在通信环境的安全要求。所以建立基于可信身份的多因素动态验证系统变成了实现零信任架构的关键重点。这个系统结合了密码、生物识别（比如指纹人脸虹膜）、一次性验证短信、设备特征码、地理位置核对等验证方法，让用户身份验证从一次认证变成了多重认证混合，大大加强了防伪装的水平。再加上行为分析的技术，可以动态评估风险和身份匹配，比如用户打字速度、鼠标移动轨迹这些数据生成用户行为模型，用 AI 算法发现异常行为时，就会启动二次验证或者直接阻止操作

在高敏感度业务场合中，也可以通过 TPM 模块、TEE 可信执行环境这样的硬件信任根基，实现对设备层的可信度评价和身份验证的绑定，这样能让通信行为来源真实可靠而且可以被控制。另外区块链分布式身份管理（DID）技术现在变成了可信身份生态里创新型的解决方案。用链上注册加上链下授权这样的组合办法，可以做到用户身份的去中心化的托管和多平台的信任机制，让用户在不同的云通讯系统拥有可以迁移的数字身份，不需要依赖中心化的平台进行控制，这样既提升了身份管理的安全级别，又让用户对自己的数据主权能有更多掌控

2.3 数据分段隔离与边缘智能安全协同机制

在远距离协作的时候，通讯的内容有很多不同的类型，比如实时的语音和视频，还有文字消息、图片、附加文件、共享代码、远程桌面图像这些形式，怎么把这些内容安全地传送，是保证平台正常运行和用户隐私不被泄露的重点问题。以前的老方法经常用统一的通道来传输所有数据，结果要是这个通道被攻击或者有漏洞的话，所有数据都可能被泄露。现在数据分段隔离技术给出了更细致的安全防护办法。把不同类型、不同重要程度的数据在逻辑上分开不同的通道，比如说把音频流、视频流、控制信号、文件传输各自单独处理和加密，这样就算某个通道出问题，也不会影响到整个系统。再加上流量追踪机制，系统可以对每个数据包的整个生命周期进行管理，从发送开始到传输、暂时存储再到接收，每个环节都加入了验证和日志追踪功能，这样就保证了数据的完整性和可以被追溯检查

为了让处理效率更高，系统可以在边缘侧装一些轻量化的节点设备，这样在用户网络边缘就能做数据的加密打包、权限管理、风险排查这些工作，避免所有流量都传回中心服务器造成卡顿。另外这些边缘节点还能用本地的人工智能模型，对像是重复发送数据、请求太频繁、流向不正常这些情况，直接在本地就能识别并发出警报，及时堵住可能的攻击路线。然后还能加些内容感知方面的安全策略，把重要数据做内容识别、脱敏处理掉、再给它们加上数字水印什么的，万一泄漏了还能通过水印找到是哪边漏的，这样整个数据的保护流程就有闭环了

3 安全传输体系的工程实践与系统部署策略

3.1 构建统一安全架构支撑多场景远程协作应用

随着云计算通信技术在各个行业加快渗透到各个行业，远程协同系统不只是普通办公环境用了，而是被大量用在医疗、教育、政府、金融、工业这些高需求场

合。每种应用场景对应不同风险类型和安全标准要求，所以系统搭建时候急需建立统一灵活的安全架构体系。在这个体系里最好用集中式安全控制引擎作为核心，统一管理秘钥的生存周期、认证方式的策略、数据访问权限和异常行为的响应规则，通过策略配置驱动多个模块一起工作。系统需要有处理多租户安全策略的隔离能力，保证不同业务部门或组织之间的数据和规则互不影响。另外在安全策略管理这块应该采用声明式建模方法，就是可以用图形化界面或者 DSL 语言来定义发布策略，这样能提高系统的维护性和不同团队协作的效率。

比如针对医疗远程会诊平台，可以制定'禁止会议后的内容长期保存、不许不同机构间互相传病历'这样规则；教育类平台的话，应该规定'用户必须是实名认证学生并且要打开摄像头才能参加课堂讨论'。通过策略引擎灵活匹配各种需求，这样能大幅提升系统安全性和合规性保障效果，避免出现安全架构不统一和反应速度慢的情况。

3.2 安全协议标准的选型与定制化组合策略

在建立云通信系统的过程中，需要考虑处理各种通信任务和数据流的类型，比如文字信息、语音对话、文件传输、屏幕共享以及控制指令这些，传输协议怎么选择和搭配会很大程度影响系统安全性和运行效率。主流的几种安全协议例如 TLS、DTLS 还有 SRTP 以及 QUIC 和 WebRTC 各自有不同的特点，实际使用时要根据不同应用场景来组合配置。比如说如果是在对实时性比较看重的音视频应用里，可以选择用基于 UDP 的 QUIC 协议结合 SRTP 的应用，这样既能降低传输延时又能保证数据加密强度；当遇到传输大文件或者网络带宽有限的情况的话，最好是用 TLS1.3 版本协议再加上断点续传功能再加上把文件切块压缩的办法，这样就能节省传输资源。要是碰到涉及保密数据或者需要符合严格监管要求的环境，可以考虑在现有标准协议基础上自己再加一层安全防护模块或者专门定制的协议架构，这样能更好防止数据被破解也方便安全验证。系统还应该自带扩展协议的支持和切换功能，这样不管遇到不同系统版本或者不同品牌的网络设备时，可以自己切换到适配的模式，防止因为协议不兼容造成通讯中断或者出现安全问题。另外还可以增加协议运行状态的可视化监测界面，把正在使用的协议、密钥协商的情况以及传输延迟这些参数实时显示出来，方便做安全检查的时候快速发现问题。

3.3 持续演进的安全运营机制与攻击防御体系

云通讯平台在运行时会碰上不停变化的安全问题，比如有 DDoS 攻击、重放攻击、劫持数据、爬数据、乱用权限这些情况。为了系统能长期安全，需要搞一套能够实时监控、自动防护、快速反应还能不断升级的安全管理措施。最好是让公司成立专门的安全中心（SOC），装上入侵检测系统（IDS）、处理安全事件的系统（SIEM）和像蜜罐那样的诱捕装置，这样就能全天候发现攻击然后及时拦住。安全中心要用人工智能搞用户行为模型，用机器学习算法把用户过去的行为数据训练一下，才能提早发现不对劲的操作然后精准处理。处理流程要分成好几层，从自动封号、断开连接、改设置再到让真人来检查，整个环节都要连起来形成闭环。为了让系统能对付新出现的攻击手法，还要经常搞安全演习、系统压力测试和让红队来攻击测试，这样才能知道系统在极端情况下稳不稳定。另外平台可以弄个安全黑匣子，把每次通讯时的加密解密记录、登录验证和异常操作日志全都存下来，这样后面查账和交报告时候方便，也能给建立可信的通讯环境打好基础。

4 结语

远程协作的持续深化使得云通讯在社会生产生活中的重要性日益凸显，而传输安全正成为制约其大规模普及的核心瓶颈之一。本文通过分析多终端异构接入、高并发交互、多角色协同等现实需求，构建了涵盖多层加密、多因子认证、边缘协同与分段隔离等维度的技术创新路径，并提出了从协议优化到安全运营的全栈部署策略。未来，云通讯的安全传输体系还将进一步融合隐私计算、量子加密、零信任体系等前沿技术，构建更开放、更灵活、更可信的通信防护架构，为数字时代的高效协作提供坚实保障。

参考文献

[1]余虹.云计算背景下通信网络安全传输控制技术的研究[J].信息与电脑，2023.

[2]宋东辉.基于云计算通信网络安全传输控制技术研究[J].长江信息通信，2021.

[3]杨有霞.基于云计算的通信网络安全传输控制技术探究[J].通讯世界，2023，30（4）：48-50.

[4]林皓.一种全新的即时通信路由方法和路由器:中国，CN106533894B[P]2018-04-03.

[5]罗进,党艳平.即时通讯中消息分组管控的方法：中国，CN106027381B[P]2019-0403.