

基于云端架构的无纸化会议数据安全性研究

魏连军 魏杰^(通讯作者)

杭州席媒信息有限公司 浙江杭州 310000

【摘要】伴随信息科技的革新,依托云端架构构建的无纸化会议系统,因具备高效便利特质而被广泛采用,但数据安全隐患成为阻碍其拓展应用的关键因素。本文全面探究云端架构下无纸化会议数据于存储、传输及访问过程遭遇的安全风险,考量数据加密、身份验证、权限管控等安全技术的实际成效,剖析安全管理策略的意义所在。经研究得出,技术手段与管理办法协同运用,能够显著增强数据安全性能,此项研究为确保无纸化会议数据安全、促进其在多领域的应用,提供了理论依据与实践指导。

【关键词】云端架构;无纸化会议;数据安全;加密技术;访问控制

Research on paperless conference data security based on cloud architecture

Wei Lianjun Wei Jie^(corresponding author)

Hangzhou Ximei Information Co., LTD Zhejiang Hangzhou 310000

【Abstract】 With the innovation of information technology, paperless meeting systems built on cloud architecture have been widely adopted due to their efficiency and convenience. However, data security risks have become a key factor hindering their broader application. This paper comprehensively explores the security risks encountered during the storage, transmission, and access of paperless meeting data under cloud architecture. It evaluates the practical effectiveness of security technologies such as data encryption, identity verification, and permission control, and analyzes the significance of security management strategies. The research concludes that the combined use of technical measures and management methods can significantly enhance data security performance. This study provides theoretical support and practical guidance for ensuring the security of paperless meeting data and promoting its application across various fields.

【Key words】 cloud architecture; paperless conference; data security; encryption technology; access control

引言

数字化办公浪潮席卷之下,依托云端架构的无纸化会议系统顺势出现,云计算技术作为支撑,让会议资料转变为电子形式,会议流程实现自动化运作,极大削减纸张使用量与会议开支,同时赋予会议更高效率与灵活度。但云端架构开放、分布的特性,致使数据脱离本地掌控,安全风险接踵而至,数据遭窃取、被篡改、受非法访问等状况,极易泄露企业或组织的商业秘密与隐私内容,进而引发严重经济损失,甚至危及声誉。深度钻研基于云端架构的无纸化会议数据安全问题,探寻切实可行的防护策略,对助力无纸化会议系统稳健前行、筑牢信息安全防线有着不可忽视的现实价值。

一、云端架构无纸化会议数据安全威胁分析

(一) 数据存储安全威胁

于云端架构无纸化会议系统内,数据寄存在云服务供应

商的服务器群组,所面临的安全威胁丰富多元,物理维度上,数据中心的环境要素干扰数据存储安全。诸如地震、洪水等自然灾害,电力供应突然中断,或是空调系统故障致使服务器温度过高,皆可能损毁数据存储设备,进而引发数据丢失。2021年就有某数据中心遭受雷击,致使多台存储服务器停止运行,部分存储其中的会议数据永久消失。

逻辑视角下,云存储系统软件层面的漏洞潜藏重大安全风险,操作系统的缓冲区溢出隐患、数据库管理系统的SQL注入漏洞,都易成为攻击者的突破口,恶意攻击者凭借精心编制的代码,可突破访问控制体系,获取服务器管理员权限,肆意对会议数据进行非法访问、篡改或删除操作。云存储多租户架构下,尽管理论上租户数据相互隔离,但一旦隔离机制存在缺陷,数据泄露便会发生,像某云服务供应商曾因虚拟化软件漏洞,致使不同租户的会议文档出现互访情况,酿成严重数据安全事件。云服务提供商内部管理问题同样不容小觑^[1]。员工违规操作、权限滥用都可能造成数据外泄,若内部人员私自将用户数据访问权限转交外部人员,或利用职

务便利盗取敏感会议数据用于商业牟利,都会给数据安全带来巨大威胁。

(二) 数据传输安全威胁

无纸化会议数据传输所处网络环境复杂,安全风险显著,无线网络场景下,数据传输遭遇窃听、中间人攻击等多重威胁,公共 Wi-Fi 网络中,攻击者构建钓鱼 Wi-Fi 热点,引诱参会者接入。一旦连接,攻击者借助 Wireshark 等嗅探工具,抓取传输中的会议数据,参会者会议期间的文字讨论信息、共享文档资料,皆可能被攻击者截获。

数据传输加密机制若有缺陷,同样会衍生安全问题。采用陈旧或强度欠佳的加密算法,像 DES 算法,其 56 位密钥长度在当代计算能力下,能借暴力破解手段在较短时间内被攻破。即便数据传输时经过加密处理,攻击者依旧有机会获取明文内容,传输协议存在的安全漏洞,同样干扰数据传输安全性。HTTP 协议因缺失加密与身份认证功能,数据传输期间容易遭到篡改,攻击者可修改 HTTP 请求头信息,于会议文档下载链接中植入恶意链接,参会者一旦点击,便可能感染恶意软件,致使设备被操控,进而威胁会议数据安全。数据传输两端,终端设备安全状态同样关键,参会者使用的移动设备若存在未修复的系统漏洞,或安装恶意应用,这些设备便可能成为数据泄露的源头。恶意应用可于后台盗取会议数据,并通过网络传输给攻击者。

二、保障云端架构无纸化会议数据安全的技术措施

(一) 数据加密技术应用

数据加密技术于云端架构无纸化会议安全保障环节起着举足轻重的作用。在数据存储加密层面,AES 算法凭借其卓越的高效性与安全性,成为静态数据加密的常见优选方案,其支持 128 位、192 位和 256 位等多元密钥长度,能够有力抵御各类已知的密码分析攻击^[2]。以企业级无纸化会议系统为例,对存储的会议文档实施 AES - 256 位加密策略后,即便存储设备遭受物理窃取,攻击者若无解密密钥,依靠现有的计算能力,破解密钥所需时间将远远超过数据的有效使用周期,而非对称加密算法 RSA,在密钥交换和数字签名场景中具备不可替代的优势。无纸化会议系统实际运行过程中,RSA 算法可用于对称加密算法密钥的安全分发工作,服务器生成一对 RSA 密钥,即公钥和私钥,将公钥发送至客户端,客户端使用公钥对 AES 密钥进行加密处理,再把加密后的密钥回传服务器,服务器通过私钥解密从而获取 AES 密钥,即便密钥在传输过程中被截获,攻击者因没有私钥,也无法成功解密获取真实密钥。

在数据传输加密领域,SSL/TLS 协议构建起安全可靠的数据传输通道,其握手过程复杂且有序,客户端先发 ClientHello 消息,内含支持的 SSL/TLS 版本、加密算法列表等关键信息,服务器收到后以 ServerHello 消息回应,确定采用的协议版本与加密算法,并发送证书供客户端验证身份。客户端完成证书核验,生成预主密钥并用服务器公钥加密发送,服务器凭借私钥解密获取预主密钥,双方据此计算出会话密钥,后续数据传输均依赖此密钥加密,以此保障数据传输保密性与完整性。密钥管理系统(KMS)全方位保障加密密钥全生命周期安全,其涵盖密钥生成、存储、分发、更新和销毁等功能,生成时用符合密码学标准的随机数算法确保随机性,存储借助硬件安全模块(HSM)加密存放,分发采用安全协议保证准确送达,定期更新降低破解风险,不再使用时及时销毁,消除密钥泄露隐患。

(二) 身份认证与访问控制技术

身份认证技术作为守护无纸化会议系统安全访问的首要屏障,多因素认证机制凭借不同类型认证要素的组合,大幅增强认证的可靠性,生物特征认证因其独特性与稳定性,在多因素认证体系中占据重要地位^[3]。指纹识别技术依据指纹纹路特性实施身份核验,光学指纹传感器通过拍摄指纹影像,运用图像处理算法提取指纹特征点;电容式指纹传感器借助电容感应原理,获取指纹三维信息,人脸识别技术借助摄像头采集人脸图像,运用深度学习算法提取面部轮廓、眼睛、鼻子等关键部位特征点,再与预存人脸模板比对完成身份认证。动态令牌认证基于时间同步或事件同步机制,每隔固定时长或每次操作时生成独一无二的动态密码,时间同步令牌依据当前时刻与特定算法生成密码,事件同步令牌则根据用户操作事件(如按键次数)生成密码,生物特征认证、动态令牌与传统用户名/密码相互配合,可有力抵御身份冒用行为。

基于角色的访问控制(RBAC)模型为无纸化会议系统带来灵活高效的访问管控模式,会议场景下会议主持人被赋予创建会议、邀请成员、把控流程、管理资料等权限;参会人员仅具备查阅资料、参与研讨、提交反馈等基础权限;管理员则掌握系统配置、用户管理、数据备份恢复等高级权限。系统依据用户所分配角色,自动赋予对应权限,规避权限分配无序状况,RBAC 模型支持角色层级关系,可设定父角色与子角色,子角色继承父角色部分或全部权限,让权限管理更趋简便。最小权限原则的贯彻,使得用户在完成的任务时仅拥有必要权限,如普通参会者会议结束后,自动丧失会议资料访问权,有效降低数据遭非法访问与泄漏风险。

三、云端架构无纸化会议数据安全策略

（一）安全管理制度建设

健全完备的安全管理制度构成无纸化会议数据安全的坚实保障，数据分类分级制度则是安全管理体系的核心基石，按照会议数据的敏感特性与重要程度，可细致划分为绝密级、机密级、秘密级以及公开级。绝密级数据囊括企业核心商业机密、重大战略决策等关键信息，对其存储与传输环节必须采用最高规格的加密手段，同时将访问权限严格限定于少数核心关键人员；机密级数据涵盖企业重要业务数据、客户敏感信息等内容，在加密处理和访问控制方面的要求仅次于绝密级；秘密级数据包含一般性业务资讯、内部会议资料等，适用常规化的安全防护举措；公开级数据则面向全体人员开放访问权限^[4]。用户权限管理制度清晰界定各岗位人员的数据访问权限，于系统初始化进程中，根据不同岗位的工作职责与业务需求，为用户精准分配相应的初始权限，在后续管理过程中，定期对用户权限实施审核，当员工出现岗位调动或职责变更时，即刻对其权限进行更新调整。员工从业务部门转岗至财务部门的情况，需及时撤销其原有的业务数据访问权限，并重新赋予契合财务工作需要的权限，构建严谨的权限变更审批流程，任何权限的新增、修改或删除操作均须经过严格的审批程序，以此确保权限管理工作的规范性与严谨性。

数据备份恢复策略关乎数据可用性保障，全量备份与增量备份协同运用，全量备份按固定周期（像每周）对全部会议数据完整备份，增量备份于两次全量备份间隙，仅针对变动数据备份，以此提升备份效率，备份数据存放于异地数据中心，避免本地数据中心遭遇灾难时备份数据受损。同时制定详尽恢复预案，清晰界定数据丢失或损毁状况下的恢复流程及责任划分，并定期开展恢复演练，确保数据灾难发生时能迅速精准恢复数据，安全事件应急响应机制对突发安全事件应对至关重要。借助部署入侵检测系统、日志分析工具等构建安全事件监测体系，实时把控系统安全态势，及时察觉异常动向，确立安全事件报告规程，一旦发现安全事件，涉

事人员即刻向上汇报，详实记录事件发生时间、现象、影响范围等信息，明确不同类型安全事件（诸如数据泄露、系统入侵）处理步骤，制定相应处置方案，涵盖切断网络连接、隔离感染设备、修复系统漏洞等操作。事后复盘分析安全事件，总结经验教训，持续优化安全防护举措。

（二）人员安全意识培训与管理

在数据安全管理体系中，人员因素起着决定性作用，故而强化人员安全意识培训与管理成为重中之重，面向所有使用无纸化会议系统的人员，需定期开设安全意识培训课程。培训内容广泛涉及多个重要领域，其中包括数据安全基础理论知识，例如数据泄露带来的严重后果、常见的网络攻击手段；安全操作标准规范，像设定符合要求的强密码（长度不低于8位，并组合字母、数字与特殊字符）、规避利用公共网络处理敏感数据、按时对设备系统及应用程序进行更新升级；还有应急处置方法技巧，如在察觉数据泄露情况时如何迅速上报、怎样妥善保护现场相关证据等内容。

系统管理员等关键岗位人员接受网络安全攻防、漏洞处理、设备管理等专业安全技术培训，模拟真实攻击场景，组织渗透测试演练，助其掌握应对威胁技能，了解攻击思路，强化系统防护^[5]。建立人员安全行为考核机制，将数据安全融入员工绩效考核。对遵规、发现报告隐患员工给予物质奖金奖品、精神表彰晋升奖励；对违规行为依情节严重程度，予以警告罚款、调离岗位等处罚，激励员工遵守数据安全制度，营造全员护数据安全氛围。

结语

云端架构无纸化会议系统提升会议效率，数据安全却不容小觑。数据存储传输存在诸多安全威胁，影响保密性、完整性与可用性。应用数据加密、身份认证、访问控制等安全技术，搭配健全安全管理制度与人员安全培训，可构建全方位数据安全防护体系。云计算、密码学技术发展，新安全威胁与手段不断涌现，需持续关注并优化安全防护策略，为无纸化会议系统应用发展筑牢数据安全根基。

参考文献

- [1]张静.物联网技术在高校无纸化会议系统的应用实践研究[J].中国宽带, 2024, 20(08): 151-153.
- [2]樊国庆, 张海平.无纸化会议系统建设策略研究[J].通信与信息技术, 2022, (01): 76-80.
- [3]刘奕.5G网络技术对提升4G网络性能的研究[J].数码世界, 2020, (04): 24.
- [4]夏保昆.基于平板电脑的新型无纸化会议系统的设计与应用研究[J].信息与电脑(理论版), 2018, (18): 150-151.
- [5]钱俊凤, 付璠, 陆岫昶.无纸化会议系统建设及应用实例[J].贵州电力技术, 2017, 20(03): 61-63+78.