

视联网应用中用户隐私保护与数据安全挑战

周开役¹ 徐伟炎² (通讯作者)

1. 中国电信股份有限公司慈溪分公司 浙江宁波 315000;

2. 中国电信股份有限公司宁波分公司 浙江宁波 315000

【摘要】视联网技术驱动视频内容朝多模态交互转变,使得用户隐私及数据安全遭遇重大考验,本研究搭建“数据采集—传输处理—应用生态”三维架构,挖掘出多模态数据融合引发的隐私泄露危机、实时交互过程的数据滥用风险,以及跨域协同治理的困局。对智能摄像头、视频会议等应用场景深入探究可知,传统加密手段在实时性上存在短板,现行合规框架难以适应动态的数据流转,通过研究,针对性地提出多模态隐私强化技术、数据全周期治理模式与跨域协同安全架构等应对策略,并对联邦学习等技术在敏感信息防护中的成效加以验证。研究成果显示,构建技术、管理、生态相互协同的全方位防护体系十分必要,这将为数字视频产业的发展提供理论指引与实践方向。

【关键词】视联网;用户隐私保护;数据安全;多模态数据;隐私计算

User privacy protection and data security challenges in Internet of Things applications

Zhou Kaiyi¹ Xu Weiyan² (Corresponding author)

1.China Telecom Co., LTD. Cixi Branch Zhejiang Ningbo 315000;

2.China Telecom Co., LTD.Ningbo Branch Zhejiang Ningbo 315000

【Abstract】The Internet of Vision technology is driving video content towards multimodal interaction, posing significant challenges to user privacy and data security. This study constructs a three-dimensional framework of "data collection—transmission processing—application ecosystem" to uncover the privacy leakage risks caused by multimodal data fusion, the risk of data abuse during real-time interactions, and the difficulties in cross-domain collaborative governance. In-depth investigations into application scenarios such as smart cameras and video conferencing reveal that traditional encryption methods fall short in real-time performance, and current compliance frameworks struggle to adapt to dynamic data flows. Through research, targeted strategies are proposed, including multimodal privacy enhancement technologies, full-cycle data governance models, and cross-domain collaborative security architectures. The effectiveness of federated learning and other techniques in protecting sensitive information is also verified. The research findings indicate that it is essential to build a comprehensive protection system that integrates technology, management, and ecosystem collaboration, which will provide theoretical guidance and practical direction for the development of the digital video industry.

【Key words】visual Internet; user privacy protection; data security; multimodal data; privacy computing

引言

5G、人工智能与边缘计算的融合应用,促使视联网由传统视频传输网络转型为涵盖短视频、直播等场景的交互生态系统,每日超 200 亿 GB 数据于此产生,其中不乏用户面部特征等敏感信息,致使隐私泄露及数据攻击风险显著攀升。2023 年国家网信办公布案例里,视联网相关应用占比高达 37%,生物特征滥用等深层次问题随之暴露,鉴于视联网数据具备多模态融合特性,加之实时性要求严苛、交互场景繁杂,传统单模态加密技术与访问控制模型已难以满足安全需求,构建适配的安全防护体系迫在眉睫。本文对核心挑战展开剖析并提出应对策略,期望为视联网应用合规发展提供借鉴。

一、视联网应用中的隐私与安全核心挑战

(一) 多模态数据采集的隐私泄漏风险

视联网终端设备智能化进程推进,使得数据采集范畴不断拓宽,摄像头、麦克风、传感器协同运作,实现“视觉—听觉—环境”多维度信息整合。于智能安防领域,高清摄像头借助步态识别技术可精准定位个体身份,环境传感器采集的 WiFi MAC 地址、蓝牙信号强度等数据,能够与用户家庭住址、日常活动轨迹等隐私信息相关联。曾有社区智能监控系统被披露,其通过视频分析手段推测居民健康状况,例如依据步态异常识别帕金森病患者,这种未经许可的生物特征采集行为引发广泛隐私争议。

在短视频直播场景里,用户生成内容(UGC)的自动标

鉴化操作暗藏隐私暴露风险，平台借助人脸关键点检测、语音情感剖析、文本语义识别等技术，给视频内容添上诸如“颜值评分”“情绪标签”“地域特征”这类元数据，这些数据在用户毫无察觉时就被用于精准营销。2024 年，某直播平台因过度采集用户微表情数据用于广告推送，受到监管部门处罚，这凸显出多模态数据处理中落实“最小必要”原则的艰难。视频会议系统常用的屏幕共享功能，在用户误操作时，极有可能泄露包含敏感信息的文档内容。曾有某金融机构，因员工共享屏幕，致使客户账户信息泄露，这也暴露出终端数据管控在技术层面存在盲区。

（二）实时数据传输与处理的安全威胁

视联网业务具备实时交互特性，对数据传输的低延迟、高可靠性要求颇高，而传统加密技术的计算开销成为制约其发展的瓶颈。以端到端加密（E2EE）用于 4K 视频传输为例，编解码延迟会增加 30%，致使视频卡顿率上升 15%，无奈之下部分平台只好采用“中心服务器解密转发”模式，又滋生数据存储安全隐患。2023 年某视频会议平台因服务器密钥泄露，致使 10 万场会议内容遭窃取，集中式解密架构存在的单点故障风险由此暴露无遗。

边缘计算与云计算协同架构致使数据流路径变得复杂^[1]。智能交通场景中路侧摄像头捕获车牌图像，经边缘节点车牌辨识后，脱敏流量数据上传云端，若边缘节点脱敏算法存有瑕疵，诸如车牌区域模糊处理欠佳，个人身份信息仍有泄露可能。某城市智慧交通系统因边缘节点数据净化未达标准，黑客借由恢复算法复原 10 万条车辆行驶轨迹，暴露边缘计算场景下轻量化安全技术实现层面的不足。视频内容 AI 智能处理涵盖美颜滤镜、内容审核等流程，多次涉及用户数据加工，某短视频平台 AI 美颜算法被揭将用户面部特征传输至境外服务器，违背数据本地化存储规范。

二、现有技术体系的适配性缺口

（一）传统安全技术的场景化失效

于数据加密范畴，对称加密算法（像 AES）难以兼顾视联网实时特性与安全诉求，非对称加密（例如 RSA）因计算复杂度，使移动端设备功耗攀升超 20%，严重限制其在手机直播、AR 交互等场景应用。隐私计算领域的联邦学习技术虽可达成“数据静止模型迁移”，但在视频数据分布式训练进程中，梯度信息泄露隐患犹存。2024 年有研究团队借逆向工程手段，从联邦学习梯度数据里复原出 12% 原始视频像素，充分表明当前技术在多模态数据防护方面存在局限性。

访问控制机制于动态交互情境下遭遇权限管理难题，传统基于角色的访问控制（RBAC）凭借静态权限分配模式，难以适配视联网内用户身份的动态转变（诸如直播场景中观众向主播的角色转换）、设备的临时接入（好比会议系统中的自带设备使用情形）等状况。某在线教育平台因未能及时

收回离职教师的课程录制权限，致使其非法获取 3000 余名学生的课堂视频，凸显出权限生命周期管理的缺位。面向视频流的细粒度访问控制（例如按帧级进行权限管理）尚无成熟技术方案，当前系统仅能实现文件级或会话级管控，难以契合医疗影像共享、司法视频存证等场景对精准授权的需求。

（二）合规框架与技术实现的协同不足

数据分类分级标准在视联网场景下的实施面临重重阻碍，现有法规明确规定需对个人信息开展分类管理，然而视频数据所具备的多模态属性，使得分类维度变得模糊不清^[2]。以一段家庭监控视频为例，其中可能同时涵盖生物特征（人脸信息）、位置信息（室内空间布局）以及行为数据（活动轨迹情况），传统依赖单一数据类型的分类方式，难以精准判定其应有的安全保护级别。某智能家居企业由于未对含有儿童面部信息的监控视频采取特殊保护措施，在数据泄露事件发生后引发一系列社会风险，这一案例充分暴露出分类标准在场景化适配方面存在的问题。

跨境数据流动管理遭遇技术验证困境，视联网业务多涉及跨国内容分发，诸如国际直播、跨境会议等场景频现，可当下技术难以对数据出境状况进行实时监测与风险评估。某视频平台海外 CDN 节点被发现缓存用户直播视频流，且未开展数据去标识化操作，明显违背《数据出境安全评估办法》规定。司法取证领域，视频数据完整性保护存在技术缺失，部分平台视频存证系统未运用区块链等防篡改技术，致使诉讼过程中出现数据遭恶意剪辑的纠纷，凸显电子数据法律效力保障的技术薄弱环节。

三、视联网隐私保护与数据安全优化策略

（一）构建多模态隐私增强技术体系

着眼视联网数据实时交互与多模态融合特质，技术层面解决方案着重于轻量化加密技术和隐私计算的深度结合，在视频流处理实践里，创新性构建“选择性加密 + 隐私计算”分层防护体系。借助目标检测算法（如 YOLOv5）实时锁定视频帧内隐私区域，当人脸置信度达 0.8 及以上、车牌字符数不少于 7 个时，便对这些区域进行动态同态加密，而对非隐私区域则运用高效 H.266 编解码技术传输数据，在边缘计算节点依靠安全多方计算（MPC）协议实现加密区域的特征提取^[3]。以某智慧零售企业门店监控系统应用来看，此技术方案使人脸特征提取时延从传统全帧加密的 120ms 缩减至 70ms，效率提升约 40%，同时通过边缘节点本地化处理方式，保障日均采集的 200 万余条顾客图像数据留存门店局域网内，相较传统云端处理模式，相关区域数据泄露风险降低 75%。

多模态数据去标识化技术打破传统像素模糊处理局限，借助生成对抗网络（GAN）搭建隐私保护合成模型，以直播场景的人脸处理为例，生成器对真实人脸的肤色分布、五官比例等统计特征加以学习，在保留面部表情、姿态等语义信

息的同时,对瞳孔间距、颧骨高度等生物特征实施扰动处理,让合成人脸与原始人脸的余弦相似度降低至 0.1 以下(生物特征差异度超 90%)。同时借助感知损失函数(Perceptual Loss)维持合成图像的语义完整性,视频推荐算法的准确率仅降低 3%。某社交平台运用该技术后,用户主动上传的含人脸视频的隐私合规率从 68%上升到 94%,且未对内容审核效率产生明显影响。在音频处理方面,研发出基于变分自编码器(VAE)的语音变声技术,在视频会议中实时替换敏感词汇对应的声纹特征,语音特征保护率达 85%,同时通过上下文语义分析保证关键词替换的语义准确性,沟通效率维持在 92%以上。

(二) 实施全生命周期数据治理

数据治理体系搭建依托 ISO/IEC 27005 风险评估框架,打造贯穿数据全生命周期的管控模式,在数据采集阶段引入动态权限协商技术,智能终端凭借设备指纹与用户生物特征双重认证发起采集申请,UI 界面同步以半透明蒙版标识摄像头取景框等采集范围,用户还能通过手势滑动等操作自定义隐私保护区域^[4]。某视频会议软件应用此功能后,用户主动管理摄像头权限次数增加 60%,因误操作引发的隐私泄露事件减少 80%,数据存储环节采用“区块链+零知识证明”分布式加密架构,将监控视频分割成 1MB 数据块,经 SM4 算法加密后存于跨地域分布式节点,用户查询时无需解密数据,借助 ZK-SNARKs 证明即可验证数据完整性。某安防企业实践该架构后,视频调阅时间从传统中心化存储的 3 分钟缩减至 1.5 分钟,同时实现数据篡改行为的秒级监测。

构建三维分类治理模型用于数据处理,层次分析法(AHP)确定权重,内容类型安防占 40%、社交 30%、教育 30%;敏感程度核心数据 50%、敏感数据 30%、普通数据 20%;应用场景私密场景 40%、内部场景 30%、公开场景 30%。某远程医疗平台依此模型开发数据标签管理系统,给每个视频帧生成 12 位特征码的复合标签,像"E-02-P"表示教育类核心敏感私密数据,结合属性基加密(ABE)技术实现动态访问控制,医生越权访问肿瘤患者手术视频次数从年均 56 次减至 8 次,降幅 85%。数据销毁部署时间触发自动化引擎,数字水印标记临时数据,直播流标记有效期 72 小时、会议录像 30 天,到期启动分片粉碎算法保障数据无法恢复,某在线教育平台应用后存储成本降 40%,再无历史数据泄露事件。

参考文献

- [1]尹锐.社交媒体中的数字孪生技术应用与用户隐私保护探讨[J].新媒体研究,2025,11(05):20-23+29.DOI:10.16604.
- [2]钟煜焱,黄鉴泉.大数据环境下用户隐私保护与网络安全策略研究[J].数字通信世界,2025,(01):46-48.
- [3]韩永秀.大数据时代社交媒体用户隐私保护研究[J].声屏世界,2024,(22):30-32.
- [4]赵鑫镖.传播隐私管理视角下互联网平台功能体系与用户隐私保护研究[D].浙江传媒学院,2023.DOI:10.27852/d.cnki.gzjcm.2023.000079.
- [5]王杨.大数据环境下网络用户隐私保护研究[J].网络安全技术与应用,2022,(10):56-59.

(三) 构建跨域协同安全架构

围绕提升系统互操作性与威胁响应效率建设行业协同机制,推动成立含 32 家主流厂商的视联网安全联盟,制定《视联网终端设备安全接入规范》团体标准。智能摄像头领域强制采用基于国密算法的 SM9 身份认证协议,设备接入执行“证书申请-双向认证-密钥协商”三阶段流程,某城市安防项目里不同品牌摄像头安全接入时间从 15 分钟缩至 6 分钟,效率提高 60%,设备伪造攻击次数从年均 230 次减到 23 次,降幅达 90%。跨平台威胁情报共享机制借助联邦学习构建分布式检测模型,各平台提供本地训练的模型参数,像暴恐视频关键帧特征向量,运用安全聚合算法保护原始数据隐私,某短视频平台联盟应用后,新型违规内容平均检测时间从 2 小时缩短至 5 分钟,检测准确率升至 98.7%。

技术透明化与共治体系建设围绕用户赋权和监管合规,开发基于自然语言处理(NLP)的隐私影响评估(PIA)工具^[5]。该工具自动解析应用代码数据处理逻辑,生成含 18 个评估项的风险报告,涵盖生物特征采集必要性、数据跨境路径合规性等。某直播平台采用后,在美颜滤镜功能添加“面部特征仅本地处理”可视化提示,用户对数据用途理解度从 42%升至 97%,隐私投诉量从月均 1200 例减至 450 例,降幅 62%。数据跨境治理构建“技术验证+第三方评估”双层管控机制,CDN 节点部署数据出境监测探针实时扫描视频帧敏感特征,如身份证号 OCR 识别,委托 CNAS 资质机构开展年度合规审计,某视频平台应用后,数据出境合规率从 75%提至 100%,通过 GDPR 与个人信息保护法双重认证。

结语

视联网迅猛发展,给用户隐私保护和数据安全带来场景化、动态化、体系化新要求。本研究剖析多模态数据采集、实时处理、跨域流动核心挑战,提出技术创新、管理升级、生态协同立体化方案。实践显示,单一技术无法满足复杂场景安全需求,要构建“技术防护深、治理流程全、生态协同广”的安全体系。后续研究可探索人工智能在隐私风险预测应用,推进区块链技术在视频存证落地,创新适配元宇宙等新型视联网形态的安全架构,为数字视频产业筑牢隐私安全屏障。