公共安全行业关于如何提高数据传输安全的分析与方法研究

杨舒玮

公安部第三研究所，上海市，200030；

摘要：在数字时代背景下，公共安全行业数字化转型持续深化，数据已成为支撑执法办案、应急处置、治安防控等核心业务的关键生产要素。跨部门、跨终端、跨地域的数据传输频次大幅提升，传输环节的安全漏洞的风险隐患愈发突出，直接威胁公共安全数据的机密性、完整性与可用性，影响行业治理效能与社会稳定。本文聚焦公共安全行业数据传输安全核心问题，系统识别数据传输全流程的安全风险，深入剖析风险形成的核心成因，从技术、管理、基础设施、人员四个维度提出针对性提升方法，重点分析了如何提高端侧数据安全以及建立数据完整性保障方案，为公共安全行业筑牢数据传输安全防线、保障数据安全合规传输提供实践参考。

关键词：公共安全；数据传输；数据安全；风险管理

DOI：10.64216/3104-9672.25.04.021

1 绪论

在数字时代背景下，公共安全行业数字化转型持续深化，数据已成为支撑执法办案、应急处置、治安防控等核心业务的关键生产要素。跨部门、跨终端、跨地域的数据传输频次大幅提升，传输环节的安全漏洞的风险隐患愈发突出，直接威胁公共安全数据的机密性、完整性与可用性，影响行业治理效能与社会稳定。本文聚焦公共安全行业数据传输安全核心问题，系统识别数据传输全流程的安全风险，深入剖析风险形成的核心成因，从技术、管理、基础设施、人员四个维度提出针对性提升方法，为公共安全行业筑牢数据传输安全防线、保障数据安全合规传输提供实践参考。

2 数据传输安全风险的核心成因剖析

技术层面，核心防护能力不足且适配性欠缺。部分单位采用的加密技术较为传统，对新型传输场景的适配性差，如移动终端、低带宽场景下的轻量级加密技术应用不足，核心涉密数据传输的高端加密技术自主可控性不强。同时，技术融合应用深度不够，人工智能、区块链等新技术与数据传输安全防护的结合不充分，缺乏对传输过程中异常行为的实时检测与溯源能力，传统防护技术难以应对新型网络攻击手段。

管理层面，制度体系不完善且落地执行不到位。数据传输安全管理制度缺乏精细化设计，未针对不同数据类型、不同传输场景制定差异化的操作规范，数据分级分类管理流于形式，无法为安全防护提供明确依据。全流程管控机制缺失，数据传输的申请、审批、校验、归档等环节缺乏严格规范，跨部门传输的备案与责任界定机制不清晰，导致违规传输、随意传输等行为时有发生[1]。

基础设施层面，硬件支撑能力薄弱且运维不足。部分基层公共安全单位的传输网络基础设施老旧，光纤化、高速化升级滞后，带宽不足难以支撑大数据传输需求，且安全防护设备配置缺口较大，防火墙、入侵防御设备、访问控制设备等核心设备老化或缺失。终端设备同质化管理难度大，执法终端、监控设备等型号繁杂，安全固件升级不及时，设备的软硬件漏洞发现不及时。

人员层面，同时具备安全素养与专业能力的人员欠缺。行业内缺乏兼具公共安全业务知识与网络安全技术的复合型人才，安全从业人员的技术水平难以应对新型安全威胁，应急处置能力不足。一线执法人员、管理人员的安全意识有待提高，对数据传输安全的重要性认知需要提升，对于违规接入非安全网络、随意传输敏感数据、忽视终端设备安全等行为缺少有效的管控机制。

3 公共安全行业提高数据传输安全的方法

3.1 提高端侧数据安全，建立数据完整性保障方案

应用密码学技术保障网络传输数据的机密性，是一个系统性的工程，其核心思想是在不可信的信道上，通过密码学协议建立一条安全的“隧道”，确保只有通信双方能读懂内容。如何建立“安全隧道”是保障传输机密性的基石，需要在传输层和网络层通过安全协议进行数据传输，同时在应用层加密，实现端到端加密，加强敏感数据在网络传输过程中的机密性。

对于重要数据（如重要点位视频、医疗记录、金融交易详情、私密通讯等），在应用层实施端到端加密，

确保数据在发送方设备加密，仅在接收方设备解密，并对数据的访问控制进行授权。对于任何试图访问重要资源的用户、设备和应用程序都需要在每次访问请求时，进行严格的身份验证和授权，比如可以采用零信任架构；在公共安全行业的数据传输中，零信任架构可以确保数据在传输过程中的安全性，防止内部和外部的潜在威胁。

应确保信息在存储或传输过程中不被未授权地篡改、破坏或删除，即保证数据的完整性。为保证数据在网络传输过程中的完整性，可从数据校验、传输协议、加密技术、数字签名、密钥管理、监控审计等多个方面采取措施。数据校验就是在发送方计算原始数据的哈希值/MAC/签名，并将数据与完整性校验值一起发送，然后在接收方接收数据并分离校验值，使用相同算法重新计算校验值，再比对两个校验值是否一致，不一致则说明数据被篡改/破坏/删除。

保证数据传输完整性需要多层次防御，不仅要选择合适的完整性算法，还要正确实施协议配置，并加强密钥管理，同时还要建立持续监控机制。本文考虑将区块链作为保障数据完整性的核心技术方法，建立一个基于区块链技术的数据完整性保障方案，核心架构组件如下图所示。

应用层(业务系统)
数据完整性服务层 ◦哈希计算◦签名生成◦验证逻辑
区块链交互层 ◦智能合约◦交易构造◦节点通信
区块链网络层 ◦公有链/联盟链◦共识机制◦存储

公共安全领域通常采用联盟链，经授权后加入，将关键数据的哈希值、元数据、操作日志上链，平衡效率与可控性无需将所有敏感原始数据上链。按照以下流程进行，首先是将采集的重要数据生成哈希，然后在哈希与时间戳等信息打包上链，后续任何环节均可实时验证哈希一致性。该方案有的优势，一是可以抗篡改，从技术上根除内部或外部人员单点篡改数据的可能性；二是增强可信，为跨部门、跨区域协作提供可信数据底座；三是可追责，所有操作行为链上留痕，实现精准审计与问责。

3.2 创新适配性传输安全技术，构建全维度技术防护体系

以技术创新为核心，结合公共安全行业传输场景特性，构建多技术融合、全场景覆盖的技术防护体系。优化加密技术应用，针对不同数据类型与传输场景，采用以国密算法为主的对称与非对称加密结合模式，对核心涉密数据实施端到端加密，确保数据传输全程不可破解。推广轻量级加密算法在移动执法终端、低带宽场景的应用，在保障安全的同时兼顾传输实时性，避免过度防护影响业务效率。

优化传输协议与通道建设，全面替代传统非安全协议，采用 SSL/TLS 升级版本等专用安全传输协议，提升传输过程的安全性。搭建公共安全行业专属虚拟专用网络与涉密数据传输专线，实现核心数据物理隔离传输，杜绝跨网络泄露风险。针对 5G、物联网等新型网络场景，优化传输协议设计，增强无线传输的抗干扰、防截获能力，满足户外执法、应急处置等移动传输需求。可以从以下几方面进行加强：一是强制使用 TLS/HTTPS，对所有网站、API 接口、移动应用后端通信强制启用 HTTPS，并禁用不安全的 HTTP。使用权威 CA 颁发的证书，避免自签名证书在公共场景使用。二是配置安全的 TLS 参数：使用高版本协议：优先使用 TLS 1.3，它更安全、更快速。禁用已不安全的 SSL 2.0/3.0 和 TLS 1.0/1.1。同时选用强密码套件，优先支持基于 ECDHE 的密钥交换和 AES-GCM 或 ChaCha20-Poly1305 的加密套件，禁用弱加密算法（如 RC4、DES）。

另外，还可以提高设置启用 HSTS，通过 HTTP 响应头告诉浏览器“以后只允许用 HTTPS 连接我”，防止降级攻击。对于企业内网访问、远程办公或连接不同数据中心，使用 IPsec VPN 或 WireGuard 等现代 VPN 技术，加密整个网络通道。更进一步的，不依赖单一的安全措施，而是建立多层次、重叠的安全控制体系。即使一层防御被突破，后续层仍能提供保护。层次通常包括：物理安全、网络安全、主机安全、应用安全、数据安全。公共安全数据传输安全不能只靠“一道防火墙”或“一种加密算法”，而需要构建从物理链路、网络边界、身份认证、应用到数据本身的全链条防护。根据深度防御原则，建立的安全防御体系不仅部署传输层加密，同时在前端集成设备指纹认证，在后端实施异常流量监测，形成协同防御。

3.3 完善精细化管理制度，规范全流程传输管理

健全制度体系，推动数据传输安全管理精细化、规范化。落地数据分级分类管理制度，制定公共安全行业数据分级分类细则，明确涉密数据、敏感业务数据、普通数据的划分标准，针对不同等级数据制定差异化的传输安全要求，明确允许传输的通道、终端与授权访问范围，实现“一类数据一策”精准防护。

规范全流程管理流程，制定数据传输申请、审批、执行、校验、归档的全环节操作规范，明确各环节的责任主体与操作标准。建立跨部门数据传输备案制度，凡涉及跨单位、跨领域数据传输，需提前报备传输内容、用途、安全措施等信息，明确双方安全责任，确保数据传输全程可控[2]。完善传输日志管理制度，要求所有数据传输行为均留存详细日志，包括传输主体、时间、路径、内容校验结果等，日志留存期限符合行业法规要求，实现传输行为全程留痕、可追溯。

3.4 升级智能化传输基础设施，夯实安全硬件支撑

推进基础设施升级改造，筑牢数据传输安全的硬件根基。加快网络基础设施优化，推进公共安全行业骨干网络与基层接入网络的光纤化、高速化升级，提升网络带宽与传输稳定性，满足大数据、视频监控等大容量数据传输需求。搭建专用无线传输网络，扩大户外、偏远区域的网络覆盖范围，提升移动传输场景的网络安全性与可靠性。部署网络流量监控与调度设备，实现传输带宽智能分配，优先保障应急处置、执法办案等核心业务数据传输。

补齐安全防护设备缺口，为基层单位配齐防火墙、入侵检测设备、数据加解密等核心安全设备，推动老旧设备升级换代，确保设备与新型防护技术适配。构建行业安全设备统一运维管理平台，对所有安全设备进行集中监控，实时掌握设备运行状态，实现故障自动报警与快速处置，提升设备运维效率。

3.5 强化专业化能力建设，提升全员安全素养

构建复合型人才培养体系，破解人才短缺难题。加强与高校、科研机构、网络安全企业的合作，开设公共安全+网络安全复合型专业课程，定向培养兼具业务能力与技术水平的专业人才。定期组织行业内安全从业人员开展技术培训与实操演练，聚焦加密技术应用、风险检测、应急处置等核心技能，提升专业能力。建立行业网络安全人才库，整合优质人才资源，实现跨区域、跨单位人才共享，为基层单位提供技术支撑。

开展常态化安全意识教育，针对一线工作人员、管理人员开展分层分类培训，普及数据传输安全法规、操作规范与风险隐患知识，强化全员安全意识。通过典型安全事故案例警示教育，曝光违规传输行为的危害与后果，引导工作人员自觉遵守安全制度，杜绝违规操作。将安全意识教育纳入新员工入职培训与在职人员定期考核，形成长效教育机制。

3.6 建立风险管理流程管理，进行风险预评估

公共安全数据传输面临的风险，比如实时视频流、警情等数据泄露或窃取、使用的传输协议配置不当，硬件基础设施老旧等，所以需要建立一套系统化的风险管理流程，包括风险评估、风险处置计划、风险监控等流程。其中，风险评估的目的是识别资产、威胁、脆弱性等，分析风险等级；制定风险处置计划包括对风险的规避、转移、减缓、接受等处置方案；风险监控用于全流程的监控，以便在风险发生时进行实时告警。

同时，考虑到公共安全涉及公安、应急、交通等多部门，数据需要在部门间安全、高效共享，所以安全的数据传输体系是实现“整体性公共安全治理”的技术基石，都是服务于跨部门的协同作战。应通过整合、协调和协同的方式，解决各部门间职能碎片化、信息孤岛等问题，而信息技术是实现整合的关键工具。

4 结论

数据传输安全是公共安全行业数字化转型的重要保障，直接关系到公共安全治理效能与社会稳定。公共安全行业数据传输安全工作是一项长期任务，需随着技术发展与业务拓展持续优化。现阶段为保证数据在网络传输过程中的完整性，可从加密技术、数据校验、传输协议、数字签名、密钥管理、监控审计、基础设施建设、管理流程管理等多个方面采取措施。未来，应进一步推动前沿技术与安全防护的深度融合，完善行业专属安全标准体系，强化跨部门协同防护能力，不断提升数据传输安全水平，为公共安全行业高质量发展提供坚实的数据安全保障。同时，需注重制度落地与人员素养提升的长效性，形成全员参与、全程管控、全域防护的安全格局，切实守住数据传输安全底线，保障公共安全领域的数据传输安全以至全流程的数据安全。

参考文献

[1]胡元.大型公共视频监控系统数据传输链路方式对比[J].绿色建造与智能建筑,2025(5):100-102,145.
[2]庞雪.物联网场景下基于边缘计算的数据传输安全性研究[D].山东:中国石油大学(华东),2022.