

AIoT 智慧社区安防与服务一体化系统建设

回立伟 王义博 张玉兰

北京华科软科技有限公司，北京，100037；

摘要：在新型城镇化与数字化转型融合背景下，社区安防与服务升级是民生改善及基层治理现代化的核心诉求。AIoT 技术为破解传统社区“安防孤立化、服务碎片化”困境提供关键路径。本文基于“感知-传输-平台-应用”技术逻辑，阐述 AIoT 智慧社区安防与服务一体化系统核心架构，分析前端感知融合、数据中台构建等关键建设环节，剖析技术、安全与运营挑战，提出优化策略，为构建以人为本的社区治理新生态提供理论支撑与实践指引。

关键词：AIoT 智慧社区安防与服务一体化系统；智慧社区系统架构；社区安防与民生服务协同

DOI：10.64216/3104-9672.25.03.019

1 AIoT 智慧社区安防与服务一体化系统的理论基础

1.1 核心概念界定

AIoT 是人工智能与物联网的深度融合技术，通过物联网实现设备互联与数据采集，依托人工智能算法进行数据解析与智能决策，形成“感知-分析-响应”的闭环系统。智慧社区安防与服务一体化系统是以 AIoT 技术为核心，整合前端感知设备、网络传输设施与智能应用平台，实现安全防控与民生服务功能协同的综合性信息系统，其核心特征体现为技术融合性、功能协同性与服务主动性。

1.2 技术支撑体系

系统建设依赖多技术协同支撑，其中物联网技术实现社区人、车、物、环境的全域感知，为一体化系统提供数据基础；人工智能技术承担数据解析重任，通过计算机视觉、机器学习等算法实现异常识别与需求预判；5G 技术提供高速低时延的传输通道，保障视频流、感知数据的实时传输；云计算与边缘计算构成混合计算架构，边缘端负责实时响应与本地分析，云端承担数据存储与全局决策，兼顾响应速度与计算效能；大数据技术实现多源数据的清洗、融合与价值挖掘，为安防预警与服务优化提供决策支持^[1]。

2 AIoT 智慧社区安防与服务一体化系统架构设计

2.1 前端感知层：全域数据采集基础

前端感知层是系统数据入口，通过多类型智能设备实现社区全域感知，分安防与服务两大维度。

安防感知聚焦风险监测，含智能视频监控、周界防护、消防感知子系统。智能摄像头为 400 万像素以上 AI 款，支持宽动态与逆光补偿，可识别高空抛物等异

常，识别率超 95%；周界防护用振动传感器、红外对射设备防入侵；消防感知靠烟雾、电气等传感器监测火灾相关指标。

服务感知侧重需求捕捉，有出入管理、环境监测、设施状态传感器。出入管理设备实现人员、车辆识别；环境监测设备测 PM2.5 等数据；设施传感器采集公共设施参数。同时对接水电煤气接口，间接感知居民需求。

2.2 联网传输层：数据流转关键通道

联网传输层负责感知数据可靠传输，构建“多维感知网关+骨干网络+云边互联”体系。采用 5G、光纤等高速技术，结合 PVG 视云联网、羚羊云等方案，分类传输视频流、图片、结构化数据等。

依数据特性实施差异化策略：视频监控、实时告警等低时延数据，经边缘节点本地处理后仅传关键结构化信息；历史数据、统计报表等非实时数据，批量传输至云端存储。同时部署多维感知网关实现多协议转换，解决不同厂商设备互联互通问题，保障数据从感知端顺畅流转至平台层。

2.3 平台支撑层：智能协同核心中枢

平台支撑层是系统“智慧大脑”，整合云计算、大数据、AI 技术，实现数据存储、处理与智能分析，为应用层提供支撑，含数据中台与智能引擎^[2]。

数据中台采用“边缘计算+云端存储”架构：边缘端快速分析实时数据并本地报警，减轻带宽压力；云端建社区数据仓库，标准化处理、分类存储海量数据，形成“一标六实”主题库及专题数据库，经数据治理保障安全，提供统一数据服务。

智能引擎集成安防与服务类算法，安防算法支持黑名单布控等功能，服务算法实现精准服务推送，还构建十余种技战法模型，支撑智能决策。

2.4 智能应用层：一体化功能落地载体

智能应用层依托平台支撑层数据分析结果，面向不同用户提供差异化服务，实现安防与服务深度融合，核心包含综合管理平台与多端应用入口。

综合管理平台整合安防、服务管理模块，达成“一屏统管”：安防模块含警情预警、重点管控等功能，动态展示感知信息，异常事件自动报警且响应时间 ≤ 30 秒，还能布控追踪重点对象，构建应急闭环流程；服务模块含基础、便民、主动关爱功能，实现人房车“一档式”管理，支持无接触通行、车位预约，可智能分析特殊群体数据并推送异常。

多端入口含政府、物业、居民端，分别助力宏观治理、提升管理效率、增强居民体验，通过权限管理实现数据有限共享。

3 AIoT 智慧社区安防与服务一体化系统关键建设内容

3.1 数据标准化与共享机制建设

数据标准化是打破信息孤岛的基础，需建立统一的数据采集、编码与交换标准。明确感知数据格式，对人脸数据、视频流、传感器数值等制定统一采集规范；建立社区统一编码体系，对房屋、设备、人员等赋予唯一标识；制定数据交换接口标准，实现不同子系统与平台间的数据互通^[3]。

在数据共享方面，构建“分级授权、有限共享”的机制。按照“谁采集、谁负责”的原则明确数据权责，对敏感数据如人脸信息进行脱敏处理；建立跨主体数据共享平台，实现公安、综治、街道、物业等多方数据的安全共享，公安部门可获取重点人员管控数据，物业可调用设备运行数据，居民可查询个人相关服务信息，通过权限管控平衡数据利用与隐私保护。

3.2 智能算法模型优化与迭代

算法模型的性能直接决定系统智能化水平，需结合社区场景持续优化。针对安防场景，优化异常行为识别算法，通过增加社区特定场景样本训练，降低复杂环境下的误报漏报率；升级人脸比对算法，提升逆光、遮挡等情况下的识别准确率，保障门禁通行效率。

服务算法方面，基于居民行为数据训练需求预测模型，实现家政服务、健康咨询等需求的精准预判；优化资源调度算法，对社区保安、维修人员等服务力量进行智能分派，缩短响应时间。建立算法迭代机制，定期收集应用反馈数据，通过持续训练更新模型参数，提升算法适配性。

3.3 安全防护体系构建

系统涉及大量敏感数据与关键基础设施，需构建“

多层次、全流程”的安全防护体系。数据安全层面，采用加密存储技术保护居民隐私数据，建立数据访问日志与审计机制，实现数据操作全程可追溯；部署数据泄露检测系统，及时发现异常数据访问行为。

设备与网络安全方面，对前端感知设备进行安全加固，设置唯一访问密码并定期更新；采用防火墙、入侵检测系统保障传输网络安全，防范恶意攻击；对边缘节点与云端之间的通信进行加密处理，确保数据传输安全。

应用安全层面，建立用户身份认证与权限管理体系，采用多因素认证提升账户安全性；定期开展应用漏洞扫描与渗透测试，及时修复安全隐患，保障系统稳定运行^[4]。

3.4 运维与运营体系建设

建立“技术运维+服务运营”的双重保障体系，确保系统长期有效运行。技术运维方面，开发智能运维模块，实现设备在线监测、故障自动告警与远程诊断，通过设备运行数据预测故障风险，实现预防性维护；建立运维工单系统，实现故障处置的闭环管理。

服务运营方面，组建专业运营团队，负责应用更新、需求对接与居民培训；建立居民反馈机制，通过 APP 评价、线下调研等方式收集意见，持续优化服务内容；探索多元化运营模式，整合商业服务资源，通过增值服务实现成本平衡，保障系统可持续运营。

4 AIoT 智慧社区安防与服务一体化系统建设的挑战

4.1 技术整合难度大

当前系统建设面临多技术融合与多设备兼容难题。不同厂商的感知设备采用差异化通信协议与数据格式，缺乏统一标准，导致设备互联与数据共享成本较高；AI 算法与社区场景适配性不足，通用算法在复杂社区环境下易出现识别偏差；边缘计算与云计算的协同机制尚不完善，部分场景存在响应延迟或资源浪费问题，影响系统整体效能。

4.2 数据安全与隐私保护压力

系统运行依赖大量居民隐私数据，包括人脸信息、居住轨迹、生活习惯等，数据安全风险突出。部分社区存在数据存储不规范、访问权限管控不严等问题，易引发数据泄露风险；人脸等生物特征数据具有不可再生性，一旦泄露危害深远；数据共享过程中缺乏明确的权责界定与安全保障机制，存在数据滥用隐患，引发居民信任危机。

4.3 用户适配与接受度差异

不同群体对系统的适应能力存在显著差异。老年群体对智能设备与 APP 操作不熟悉，面临“数字鸿沟”问题，

难以充分享受一体化服务；部分居民对数据采集存在抵触心理，担心隐私泄露，主动配合度不高；系统界面与操作流程的设计未能充分考虑各类用户需求，影响使用体验与推广效果。

5 AIoT 智慧社区安防与服务一体化系统建设的优化策略

5.1 完善技术标准与协同机制

加快制定 AIoT 智慧社区技术标准体系，明确设备通信协议、数据格式、接口规范等统一要求，推动跨厂商设备互联互通。建立“政产学研用”协同创新机制，联合高校、企业研发社区专用 AI 算法，通过场景化训练提升算法精准度；优化“边缘-云端”协同架构，根据业务需求合理分配计算资源，对实时性要求高的安防告警采用边缘优先处理，对大数据分析类服务采用云端集中处理，提升资源利用效率^[5]。

5.2 构建全链条数据安全保障体系

建立数据全生命周期安全管理机制，从采集、存储、传输到应用各环节强化安全防护。采集阶段遵循“最小必要”原则，仅收集与服务相关的数据；存储阶段采用加密技术与分布式存储，定期开展数据备份与安全审计；传输阶段采用 SSL 加密等技术，防止数据中途被窃取；应用阶段完善权限管理体系，实施基于角色的访问控制，明确数据使用边界。

加强隐私保护制度建设，制定数据采集告知与同意机制，明确告知居民数据用途与保护措施；建立数据安全应急响应预案，发生泄露事件时及时处置并承担相应责任；引入区块链技术构建可信数据环境，实现数据操作全程可追溯，提升居民信任度。

5.3 推进用户适配性优化与宣传引导

开展系统适老化与普惠化改造，简化 APP 操作流程，增加语音交互、大字模式等功能；设立线下服务点与培训课程，帮助老年群体掌握智能设备使用方法，跨越“数字鸿沟”。加强宣传引导，通过社区公告、上门讲解等方式普及系统功能与数据保护措施，消除居民隐私顾虑；建立用户反馈机制，根据不同群体需求优化系统设计，提升使用体验与接受度。

6 结论

AIoT 技术为智慧社区安防与服务一体化提供了革命性解决方案，通过构建“感知-传输-平台-应用”的分层架构，实现了安全防控的精准化与民生服务的个性化，

推动社区治理从“被动管理”向“主动服务”转型。系统建设过程中需正视技术整合、数据安全、用户适配与运营可持续等关键挑战，通过完善技术标准、强化数据安全、优化用户体验、创新运营模式等策略，破解发展难题。未来，随着 5G、数字孪生等技术的进一步发展，一体化系统将向更智能、更协同、更人性化的方向演进，实现社区安防与服务的深度融合。通过技术创新与机制创新的双轮驱动，一体化系统将成为基层治理现代化的重要支撑，为居民创造更安全、便捷、舒适的社区生活环境，助力建设以人为本的智慧城市。

参考文献

- [1] 朱帅. 数据要素价值视角下智慧安防在智慧社区养老中的应用研究[J]. 中国建设信息化, 2025, (14): 74-78.
- [2] 邵巍巍. 面向老年用户体验的智慧社区安防系统人机交互优化设计研究[J]. 包装工程, 2025, 46(12): 557-565+578.
- [3] 李童. 智慧社区安防标准体系构建研究[J]. 标准科学, 2025, (04): 94-99.
- [4] 陈光辉. 面向智慧社区的安防系统设计与技术集成应用[J]. 中国宽带, 2024, 20(09): 25-27.
- [5] 洛向刚. 物联网智慧社区安防系统设计[J]. 中国安防, 2024, (08): 99-104.

作者简介：回立伟，性别：男，族：汉，出生日期：1986 年 11 月 21 日，籍贯：河北省邢台市柏乡县，职务/职称：项目经理/助理工程师，学历：大学本科，研究方向：水务行业数据治理、数据治理+AI、数据要素在水务行业开发与利用。

王义博，性别：男，民族：汉，出生日期：1990 年 9 月 1 日，籍贯：河北省廊坊市香河县，职务/职称：工程师（中级），学历：硕士研究生，研究方向：计算机技术与开发、信息化建设与规划、企业人力资源数字化平台的开发与效能优化研究、物联网技术在企业服务质量管理中的创新应用研究、企业级管理信息化系统的集成构建与协同应用研究（含软硬件）、数字化转型背景下企业管理信息化平台的定制化开发研究。张玉兰，性别：女，民族：汉，出生日期：1980 年 11 月 10 日，籍贯：吉林省延边自治州，职务/职称：部门副主任，学历：大学本科，研究方向：数据管理、数据治理、数据分析、数据智能治理和应用、企业管理软件设计。