# 物联网环境下智能家居系统的安全防护措施探讨

杨　强
杭州安恒信息技术股份有限公司　浙江　杭州　310000

**摘　要：**伴随物联网技术迅猛革新，智能家居系统的运用愈发普及，给大众生活带来诸多便利，不容忽视的是，安全隐患也逐渐暴露，设备存在的缺陷、遭受的网络侵袭以及数据泄露等风险，对用户隐私和生活安全构成严重威胁。本文全面探究物联网背景下智能家居系统于设备、网络、数据层面遭遇的安全挑战，深入钻研设备安全强化、网络安全防范、数据安全维护等防护办法，同时给出安全管理以及人才培育等落实保障策略。研究成果显示，将技术手段与管理措施相融合，能够切实增强智能家居系统的安全性，助力用户打造值得信赖的智能化生活空间。

**关键词：**物联网；智能家居系统；安全防护；设备安全；数据安全

## 引言

物联网技术蓬勃发展推动智能家居系统广泛应用，智能门锁、智能照明到全屋智能控制系统等各类设备实现互联互通，大幅提升生活便利性与智能化水平。但物联网环境下智能家居系统开放又复杂，存在诸多安全风险，攻击者可利用设备漏洞入侵家庭网络，窃取用户隐私数据，甚至操控设备威胁人身安全。现实中智能摄像头被破解导致家庭生活遭窥视，智能门锁被非法控制造成财产损失等事件频发，探究物联网环境下智能家居系统安全防护方法，对保障用户安全、促进智能家居产业健康发展意义重大。

## 1 物联网环境下智能家居系统的安全威胁分析

### 1.1 设备层面安全威胁

因成本控制和设计缺陷，智能家居设备存在硬件安全问题，部分厂商为节省成本，采用运算能力差的低性能微控制器与存储有限的存储器，某经济型智能插座搭载8位单片机，无法满足复杂加密算法运行，导致数据传输难以有效加密。物理防护不到位，攻击者能用专业工具拆解设备，以探针技术读取智能门锁固件数据，篡改开锁代码，软件安全漏洞也不少，某知名智能摄像头旧版本有未修复的缓冲区溢出漏洞，攻击者构造恶意数据触发后，就能获取设备最高权限，远程窥视用户隐私。很多智能家居设备出厂设简单密码如“123456”，甚至无密码，用户安全意识低未及时修改，调查显示超60%智能音箱用户从未换初始密码，这种弱认证让攻击者可借暴力破解或网络扫描轻松控制设备。

### 1.2 网络层面安全威胁

智能家居系统网络架构多样且复杂，多种通信协议交错，加剧安全风险，Wi-Fi 是主要连接方式，其安全依赖加密协议，早期 WEP 协议因密钥管理缺陷已被破解，WPA2 协议存在 KRACK 漏洞，攻击者能借此重放握手数据包获取 Wi-Fi 密码[1]。实际中攻击者常设钓鱼 Wi-Fi 热点伪装正规网络，用户设备接入后，智能家居控制指令和数据易被盗取，Zigbee 协议虽有低功耗、自组网优势，但 AES - 128 加密算法存在密钥管理问题，攻击者可嗅探网络流量，截获初始密钥协商环节解密数据，恶意修改智能灯泡亮度指令或关闭智能窗帘。家庭网关是网络核心，一旦遭攻击，攻击者可利用固件漏洞植入恶意程序将其变成“僵尸节点”，操控家庭网络内所有设备，发动 DDoS 攻击，致使网络瘫痪、智能安防系统失效。

## 2 智能家居系统安全防护技术措施

### 2.1 设备安全加固措施

采用搭载可信执行环境（TEE）的芯片，如ARM TrustZone技术，从硬件层面划分安全和普通区域，将设备密钥管理、身份验证等核心操作隔离在安全区，防止恶意软件篡改。一款高端智能门锁内置TEE芯片，解锁密钥存于安全区域，即便设备受恶意程序入侵，密钥也无法读取。增加防拆卸传感器与硬件加密模块，智能设备外壳若被非法拆解，防拆卸传感器启动自毁程序清除敏感数据；硬件加密模块运用国密SM4算法等，对存储数据进行硬件级加密，保障数据存储安全。软件安全方面，厂商要构建完善的安全开发生命周期（SDL）流程，需求分析确定安全要求，设计阶段采用分层隔离等安全架构，分离设备控制逻辑与数据存储，代码编写遵循安全编码规范，避免缓冲区溢出、SQL注入等常见漏洞，定期发布安全补丁是修复软件漏洞的关键，某智能电视厂商建立月度安全更新机制，及时处理新发现漏洞，确保设备安全运行。

### 2.2 网络安全防护策略

选用WPA3加密协议，其搭载的同时身份验证（SAE）机制能够有力抵御字典攻击，稳固网络连接安全防线。设定高强度Wi-Fi密码（字符长度超12位，混合大小写字母、数字及特殊字符）并定期更换，同时隐藏网络SSID，以此降低网络被探测发现的可能性。针对Zigbee网络，改进密钥管理体系，运用动态密钥更新算法，比如实施24小时自动更换网络密钥策略，提升攻击者破解的难度系数，部署网络入侵检测系统（IDS）与入侵防御系统（IPS），借助机器学习算法剖析网络流量特征，精准识别异常活动。一旦监测到短时间内同一IP发起大量设备连接请求，IDS系统即刻触发警报，IPS系统随即自动拦截该IP访问，采用防火墙分区管理模式，将智能家居设备网络与用户办公、娱乐网络划分为独立子网，制定严苛的访问控制规则，仅允许必要设备间通信，像限定智能摄像头仅能向家庭NAS设备传输视频数据，从而防范攻击者借办公设备侵入智能家居网络。

## 3 智能家居系统数据安全与管理策略

### 3.1 数据安全保护方案

智能家居系统运行生成的庞大数量数据，包含作息规律、环境参数以及生物特征等敏感内容，一旦出现泄露，会对用户隐私和安全造成严重威胁，这就需要构建覆盖全流程的数据安全保护体系[2]。数据采集阶段，依循最小必要准则，严格界定设备数据采集范畴，智能睡眠监测设备仅收集与睡眠质量有关的心率、体动数据。运用差分隐私技术，通过注入可控噪声对数据进行脱敏处理，在确保数据可用的同时隐匿个体特性，某智能手环厂商运用此技术后，用户数据隐私保护程度显著增强，数据统计分析准确性仍维持在较高水平。

底层运用磁盘加密技术守护存储介质安全，上层根据数据敏感程度进行分级加密，普通设备日志等采用AES-128对称加密，在保障安全的同时兼顾效率；用户身份认证等敏感数据则综合AES-256与RSA非对称加密，借助RSA实现AES密钥安全传递。存储架构融入区块链技术，将数据分片存放于不同节点，通过哈希值校验和共识机制，确保数据完整且无法篡改，某智能家居云平台以此多次成功抵御数据篡改攻击。数据传输存在中间人攻击等风险，需要搭建端到端的安全通信体系，采用TLS 1.3协议，利用椭圆曲线Diffie-Hellman密钥交换生成会话密钥，配合AES-GCM加密，保障数据机密性和完整性，引入零信任架构，对每次传输请求进行严格身份核验和权限确认，某企业部署后有效拦截绝大多数非法数据访问，有力巩固了传输安全屏障。

### 3.2 安全管理与应急响应机制

完善的安全管理制度是智能家居系统稳定运行的关键支撑，需从全生命周期管理、应急响应及安全意识培育等多个维度构建，产品设计阶段企业应将安全需求深度嵌入开发流程，严格参照ISO/IEC 27001信息安全管理体系标准，制定详实的安全设计准则与风险评估流程，以此保障产品安全架构的合理性。生产过程中重点管控供应链安全，要求零部件供应商出具权威安全检测证明，防止芯片、传感器等核心部件出现后门或漏洞，某国际知名企业设立供应商安全评分制度，对不符合标准的供应商进行整改或淘汰，显著降低供应链风险，从源头保障产品安全。

企业需制定分类分级应急响应方案，将安全事件分成一般（单设备异常）、重大（局部网络瘫痪）、特别重大（大规模数据泄露）三个等级，明确各级事件响应时限与处理流程[3]。特别重大数据泄露事件须1小时内启动应急响应，包括切断受影响设备网络连接、通知用户并提供密码重置服务，组织专业团队协同调查，72小时内完成漏洞修复与系统加固，某智能家居平台凭借完备预案，遇DDoS攻击时30分钟完成网络切换，服务中断仅5分钟，最大程度减少用户影响。安全意识培训教育机制不可或缺，企业内部定期开展网络安全法规、数据保护政策培训，通过模拟钓鱼演练、漏洞挖掘竞赛提升员工安全操作技能与防范意识，面向用户，企业经官网、社交媒体发布安全指导手册，制作科普视频讲解强密码设置、固件更新等操作，某品牌“安全家庭月”活动后，六成用户掌握基础防护技能，用户主动上报安全隐患数量增至原来3倍，形成企业与用户共护安全生态的良好局面。

## 4 智能家居系统安全防护实施保障

### 4.1 技术研发与创新保障

技术创新是打破智能家居系统安全困境的关键所在，突出表现在加密技术创新、人工智能运用以及产学研协作这三个方面，加密技术范畴内，量子密码学和同态加密为数据安全开拓新境界。量子密钥分发（QKD）技术依据量子力学原理，借助光子量子态进行密钥传输，一旦出现窃听行为，量子态便会改变，进而被通信双方感知，达成理论层面绝对安全的密钥传输，我国建成的“京沪干线”量子保密通信骨干网络，为这项技术的应用提供支撑，倘若将其引入智能家居系统，能够抵御量子计算对传统加密算法构成的破解威胁。同态加密技术支持在加密数据上直接开展运算，无需解密操作，于智能家居数据分析场景里，既能守护用户隐私，又能契合数据处理要求，具备广阔的应用前景。

采集智能家居设备正常运行数据，运用深度学习算

法构建行为分析与异常检测模型，可精准识别智能摄像头未经授权转动、智能电表异常用电等攻击行为，某AI安全防护系统在5000户家庭测试中，成功检测出92%的未知攻击，误报率保持在3%以内[4]。强化学习算法能依据实时攻击情况，动态优化防火墙规则与入侵检测阈值，实现智能化安全防护，产学研协同创新推动技术快速落地，高校和科研机构发挥基础理论研究长处，开展物联网安全协议、密码学算法等前沿研究；企业根据市场需求，将科研成果转化为实际产品。清华大学与企业合作，把设备漏洞自动化检测技术融入生产流程，使设备出厂前漏洞修复率从70%提高到95%。政府设立专项科研基金，鼓励校企联合申报项目并奖励创新成果，促进技术创新与产业发展深度融合。

4.2 人才培养与用户教育保障

构建智能家居安全生态，专业人才培养和用户安全意识提升很关键，要从高校教育、企业培训和用户科普协同推进，高校是人才培养摇篮，得优化物联网安全专业建设，课程体系里，除传统网络安全课，要建设智能家居安全开发、设备逆向工程等特色课程，加强实践教学。毕业设计引入企业真实项目，像模拟智能家居攻防演练、设计安全认证协议，培养学生解决实际问题能力，高校还应与企业共建实训基地，给学生接触前沿技术实习机会，有高校和企业共建的物联网安全实训基地，每年培养超200名专业人才，八成进入智能家居行业，缓解人才短缺状况。

企业内部要搭建分层分类人才培训体系，技术研发人员参与安全编码规范、漏洞挖掘专项培训，去国际安全会议与竞赛开拓视野；运维人员接受网络设备操作、应急响应流程培训，借模拟攻击演练提高故障处理水平；管理人员学习安全战略规划、合规管理课程，强化决策和风险管理能力。有家智能家居企业推行“安全人才成长计划”，用导师带徒、技能认证等举措，让员工安全技能达标率达90%，团队防护能力大幅增强[5]。构建安全生态离不开用户安全意识教育，企业开发可视化安全管理工具，像图形化配置向导、安全状态监测APP，降低用户操作难度，还实时推送风险预警，举办多样宣传活动，比如安全知识竞赛、制作科普漫画，某品牌“安全小卫士”线上竞赛吸引超10万用户，以有趣方式提升用户安全意识和防护能力，推动形成全民参与的安全防护局面。

**结语**

物联网环境下智能家居系统安全防护是复杂工程，关联设备、网络、数据等多层面。设备漏洞、网络攻击、数据泄露等威胁当前，要用设备安全加固、网络防护、数据保护等技术，还得建立安全管理和应急响应机制。靠技术研发创新、人才培养教育提供持续动力，多方面协同发力，才能提升智能家居系统安全性，打造安全便捷智能生活环境，推动智能家居产业稳健发展。

**参考文献**

[1]侯国辉.物联网中常见安全事件及存在的安全风险[J].中国科技信息,2025,(09):67-69.

[2]朱冰雁.基于物联网的智能家居安全加密方法分析[J].网络安全和信息化,2025,(04):113-115.

[3]魏政花.物联网在智能家居中的安全防护技术研究[J].信息与电脑,2025,37(03):81-83.

[4]王晓斐.基于物联网技术的智能家居系统网络安全威胁与防护策略[J].网络安全和信息化,2025,(01):101-103.

[5]王奂,宋波,戚伟佳,等.智能家居系统中数据安全与隐私保护措施及其发展趋势探析[J].电子产品世界,2024,31(12):16-19.