物联网多维度安全防御模型研究*

黎　珂

（工业信息安全（四川）创新中心有限公司，四川　成都　610041）

摘　要：传统物联网“感知－网络－应用”三层架构在边缘侧存在防护盲区，而“六域模型”因实施成本高、域间协同机制缺失导致工程落地困难。基于物理域、网络域、服务域的威胁分析，重构“终端域－边缘域－核心网域－云应用域”四域架构，并引入数据面与控制面解耦的双层控制机制，提出“四域双层”安全框架。该框架系统揭示硬件渗透、协议缺陷、量子计算冲击及API语义冲突等多维威胁，构建了终端轻量化防护、量子增强传输、服务端主动防御及全生命周期安全管控模型。银行零信任场景与工业物联网场景的实测表明，该架构下攻击检出率≥98%，平均响应时间≤500 ms。研究结果可为规模化物联网安全工程提供可复用的体系化方法。

关键词：物联网安全；四域双层架构；零信任；全生命周期防御；内生安全

中图分类号：TP393. 08；TP309　　**文献标识码**：A　　**DOI**：10. 19358/j. issn. 2097－1788. 2025. 12. 004

引用格式：黎珂. 物联网多维度安全防御模型研究［J］. 网络安全与数据治理，2025，44(12)：26－33.

Research on a multi-dimensional security defense model for the Internet of Things

Li Ke

(Sichuan Innovation Center of Industry Cyber Security Co., Ltd., Chengdu 610041, China)

Abstract: The traditional "perception-network-application" three-layer architecture of the Internet of Things (IoT) exhibits security blind spots at the edge. Meanwhile, the "six-domain model" faces challenges in practical implementation due to high deployment costs and lack of inter-domain coordination mechanisms. Based on threat analysis across the physical, network, and service domains, this paper reconstructs a "terminal domain-edge domain-core network domain-cloud application domain" four-domain architecture and introduces a dual-layer control mechanism that decouples the data plane and control plane, proposing a "four-domain dual-layer" security framework. This framework systematically reveals multi-dimensional threats including hardware infiltration, protocol vulnerabilities, quantum computing impacts, and API semantic conflicts. It constructs models for terminal lightweight protection, quantum-enhanced transmission, server-side proactive defense, and full-lifecycle security management. Practical tests in banking zero-trust scenarios and industrial IoT scenarios demonstrate that the attack detection rate is ≥98%, and the average response time is ≤500 ms. The results provide a reusable, systematic methodology for large-scale IoT security engineering.

Key words: Internet of Things (IoT) security; four-domain dual-layer architecture; zero trust; full-lifecycle defense; endogenous security

0　引言

物联网技术正深度融入智能家居、工业控制、智慧城市等领域，推动社会生产方式变革。国际数据公司（International Data Corporation，IDC）预测，到2027年全球物联网设备数量将超过400亿台。设备密度与数据流量的指数级增长促使攻击面向物理空间延伸，形成跨域协同威胁。传统“感知－网络－应用”三层架构[1]未对边缘计算节点进行安全定义，存在结构性盲区；六域模型[2]虽引入用户、目标对象等维度，但域间接口复杂、协同成本高昂，难以工程化落地。

本研究结合最新威胁态势与技术演进，面向可部署、可扩展、可验证目标，提出“四域双层”安全框架，重构“终端－边缘－核心网－云应用”四域责任边界，细化各域威胁模型与对策；设计数据面与控制面解耦机制，实现策略计算与执行的分离；构建覆盖开发、部署、运维、退役全生命周期的安全管控模型，并在银行与工业

*基金项目：四川省重大科技专项（2022ZDZX0009）

场景完成验证。

1 威胁分析

1.1 物理域

终端设备层面临硬件化、物理化的安全风险，主要有两类攻击模式：

（1）侧信道攻击：通过物理信号分析破解安全机制，利用设备运行时泄露的功耗、电磁辐射等物理信息，直接威胁加密模块安全。具体而言，功耗波动分析技术可提取 89% 低成本射频识别芯片密钥[3]。

（2）供应链攻击：在设备制造/交付环节植入恶意硬件，触发物理破坏。例如，2024 年黎巴嫩寻呼机爆炸事件中，攻击者在供应链中植入微型爆炸装置，触发用户接近后自动引爆，造成严重人员伤害。此类攻击产生的主要原因有：

① 物理防护缺失：终端设备缺乏抗拆解、抗探测的硬件防护；

② 固件更新机制失效：无法及时修复已知漏洞；

③ 供应链监管盲区：从芯片生产到设备集成的多环节缺乏安全审计。

1.2 网络域

通信网络层的脆弱性集中在无线协议设计缺陷和量子计算威胁两大维度：

（1）协议级攻击：利用 ZigBee、CoAP、MQTT 等协议缺陷实施拒绝服务（Denial of Service，DoS）、重放或放大攻击。实验数据显示，CoAP 放大比例可达 1∶50。

（2）量子计算威胁：Shor 算法可在多项式时间内分解大整数，危及 RSA/ECC 密钥。国家电网攻防演练表明，未部署量子密钥分发（Quantum Key Distribution，QKD）的系统被量子算法攻破的概率提升 3～5 倍[4]。

1.3 服务域

云应用层面临虚拟化逃逸和应用程序接口（Application Programming Interface，API）攻击的新型威胁，主要包括：

（1）容器逃逸攻击：利用容器运行时或编排工具（如 Docker、Kubernetes）的配置错误或漏洞，突破容器隔离机制，获取宿主机或宿主机上其他容器的控制权，从而横向移动并窃取敏感数据。某平台因 Kubernetes 配置错误导致数据泄露，攻击者利用容器内 procfs 挂载漏洞访问宿主机进程，最终获取 etcd 数据库密钥。

（2）API 语义冲突攻击：跨域指令本体不一致导致误操作。例如，医疗场景“紧急关闭”表示生命维持设备停机，而家居场景仅关闭普通电器，该类攻击占 API 攻击的 32%。

2 四域双层架构设计

四域负责纵向防御，双层实现横向策略闭环，零信任贯穿身份与访问控制，全生命周期覆盖时间维度。物联网“四域双层”总体架构如图 1 所示。

2.1 四域架构设计

四域安全防护机制如图 2 所示。

2.1.1 终端域

终端域按资源量级划分为三类设备，并针对其特点强化物理防护：

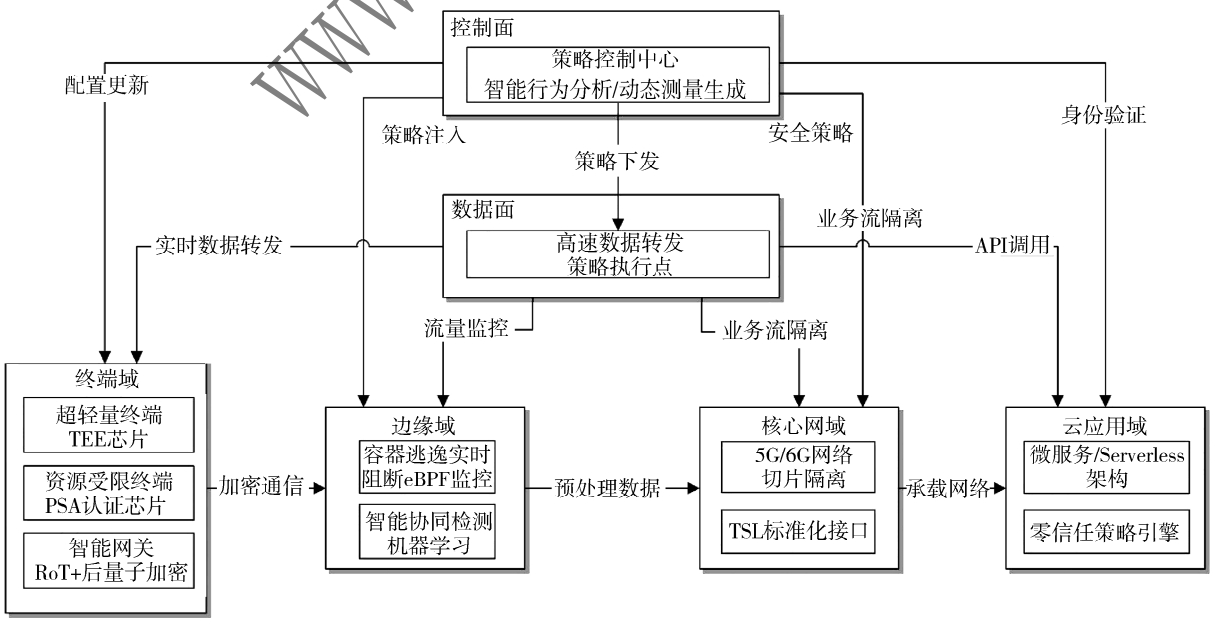

图 1 物联网“四域双层”架构图

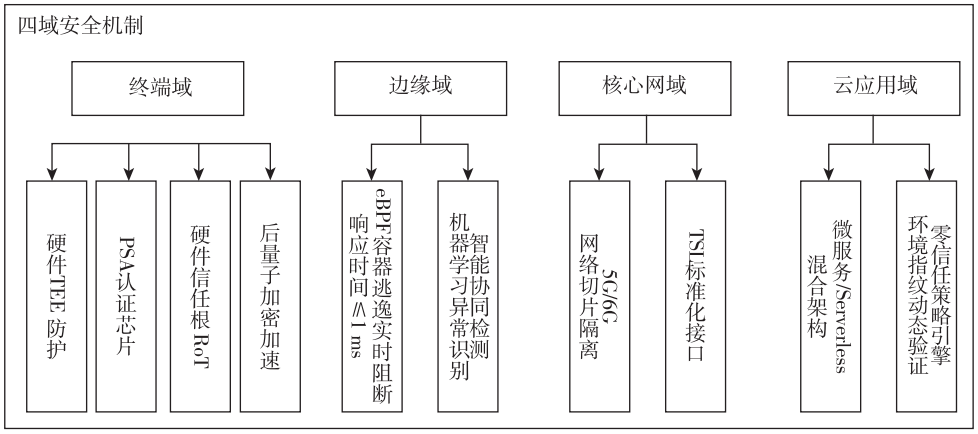

图 2　四域安全防护机制示意图

（1）超轻量终端（功耗 < 1 mW）：选用低功耗、高性能的可信执行环境（Trusted Execution Environment，TEE）芯片，部署轻量级 TEE，通过硬件隔离技术为关键数据和代码提供安全运行空间，确保密钥存储与运算的安全性，并针对物联网设备的低功耗需求优化电源管理策略。

（2）资源受限终端（内存 < 128 KB）：采用平台安全架构认证芯片，该芯片具备高安全性和低功耗特性，能够有效抵御物理攻击和侧信道攻击，同时满足资源受限设备的性能要求，并对加密算法进行优化，减少其对内存和计算资源的占用（资源占用率降低 40%）。

（3）智能网关：在硬件层面设计专用的加密模块，实现对后量子密码算法的加速处理；集成硬件信任根（Root of Trust，RoT），为网关设备提供强大的身份认证和加密通信能力，抵御量子计算攻击对传统加密算法的威胁，同时确保其与现有通信协议的兼容性。

2.1.2　边缘域

边缘域负责数据预处理和初步分析：

（1）容器逃逸实时阻断：基于扩展伯克利数据包过滤器（extended Berkeley Packet Filter，eBPF）技术，通过内核级流量监控与策略执行，实时检测并阻断容器逃逸行为（响应时间≤1 ms），捕获和分析网络流量中的异常行为，结合实时策略更新机制，确保快速响应容器逃逸事件。

（2）智能协同检测：采用边缘智能处理技术，利用本地内存加载机制构建指标图关系模型，优化本地内存管理策略，提高数据加载和处理速度，结合机器学习算法精准识别异常行为，降低误报率，通过时间窗口滑动与信息量分析实现毫秒级异常检测。

2.1.3　核心网域

整合 5G/6G、低轨卫星、工业场景时间敏感网络（Time-Sensitive Networking，TSN）等承载网络，引入“切片级安全隔离”机制，实现不同业务流的隔离与保护：

（1）5G 切片隔离：每个切片具有独立网络拓扑、资源分配和安全策略，根据业务优先级和安全需求动态调整资源分配和安全策略，实现资源逻辑隔离，确保通信安全性和独立性，防止攻击在不同业务间传播，实现最优网络性能和安全性[5]。

（2）物模型（Thing Specification Language，TSL）：通过统一 TSL 实现设备功能标准化，简化设备接入和开发流程，充分考虑不同设备兼容性和互操作性，通过标准化接口和协议实现无缝连接和协同工作。

2.1.4　云应用域

采用微服务与 Serverless 混合架构，按《信息安全技术 网络安全等级保护基本要求第 4 部分：物联网安全扩展要求》划分四级安全域，针对服务网格侧车代理的策略风险，实施零信任策略注入：

（1）微服务与 Serverless 混合架构：通过合理服务划分和资源调度策略，将复杂系统拆分为多个独立小型服务，每个服务独立部署和运行，具有高度灵活性和可扩展性，实现微服务与 Serverless 服务高效协同，提高系统性能和可靠性。

（2）零信任策略引擎：对每个服务调用进行实时身份验证和授权检查，结合环境指纹技术，每个服务调用动态验证身份凭证与环境指纹，确保只有合法且可信的请求被处理，防止攻击者通过伪造身份或篡改环境信息进行攻击。

2.2　双层控制机制

（1）数据面

优化 SRv6 协议实现机制，减少协议开销，采用高效策略执行算法，确保策略快速执行和跨域业务流高速转

发（转发延迟≤5 ms）。数据面部署轻量级策略执行点，仅承载策略判决结果的执行功能，确保数据传输高效性和安全性。

（2）控制面

采用智能行为分析算法和漏洞检测机制，实时监测设备行为和安全状态，根据实时安全评估结果动态调整安全策略，并将策略推送到数据面执行点，确保系统始终处于最佳安全状态，应对不断变化的安全威胁，并基于行为分析、漏洞状态与威胁情报持续评估设备信任等级。

数据面与控制面解耦的工作流程如图 3 所示，包括控制面的策略计算、决策下发，以及数据面的高速转发与策略执行，实现策略计算与执行分离。

3 多维度安全防御模型

3.1 终端轻量化防护

3.1.1 硬件级信任根

基于安全芯片，将密钥存储与运算置于硬件安全区，采用新型加密电路优化模乘法器架构，将公钥加密功耗大幅降低（功耗降低 60%）。在实现过程中，通过优化安全芯片架构和算法，提高系统安全性和性能，同时降低硬件资源需求，使其适用于资源受限物联网设备[6]。

3.1.2 动态行为防护

基于设备指纹构建轻量级机器学习（Machine Learning，ML）模型，从网络流量模式、CPU 周期特征和能量

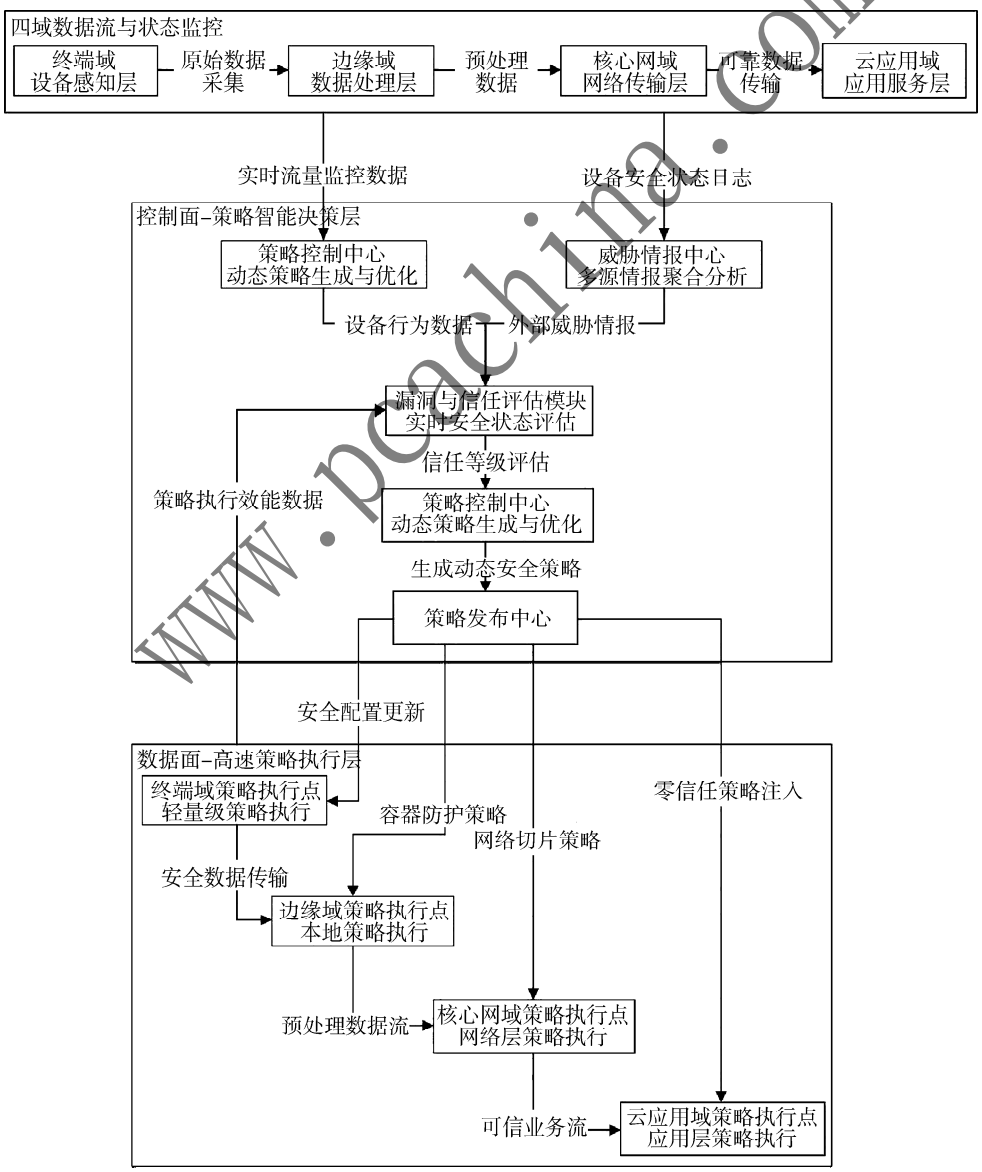

图 3 数据面与控制面解耦流程图

消耗模式三维度分析设备行为，及时发现异常行为并采取措施，检测精度≥98%，误报率≤1.2%，平均响应时间≤100 ms。终端动态行为检测流程如图4所示，具体实现步骤如下：

（1）数据采集：通过设备网络接口、CPU监控模块和电源管理模块采集相关数据，采用高效采集算法确保数据准确性和完整性，减少对设备性能影响（资源占用率≤5%）。

（2）特征提取：对采集数据预处理，提取代表性特征，包括数据包时序特征、指令执行周期分布和充放电曲线等，通过优化特征选择算法减少特征冗余度，提高模型训练效率和准确性。

（3）模型训练：利用机器学习算法对提取特征训练，构建轻量级行为分析模型，通过调整算法参数和优化训练策略，提高模型性能和泛化能力。

（4）实时检测：将训练好的模型部署到终端设备，实时监测设备行为，一旦发现异常行为立即触发报警或采取防护措施，通过优化模型推理算法提高检测速度和准确性。

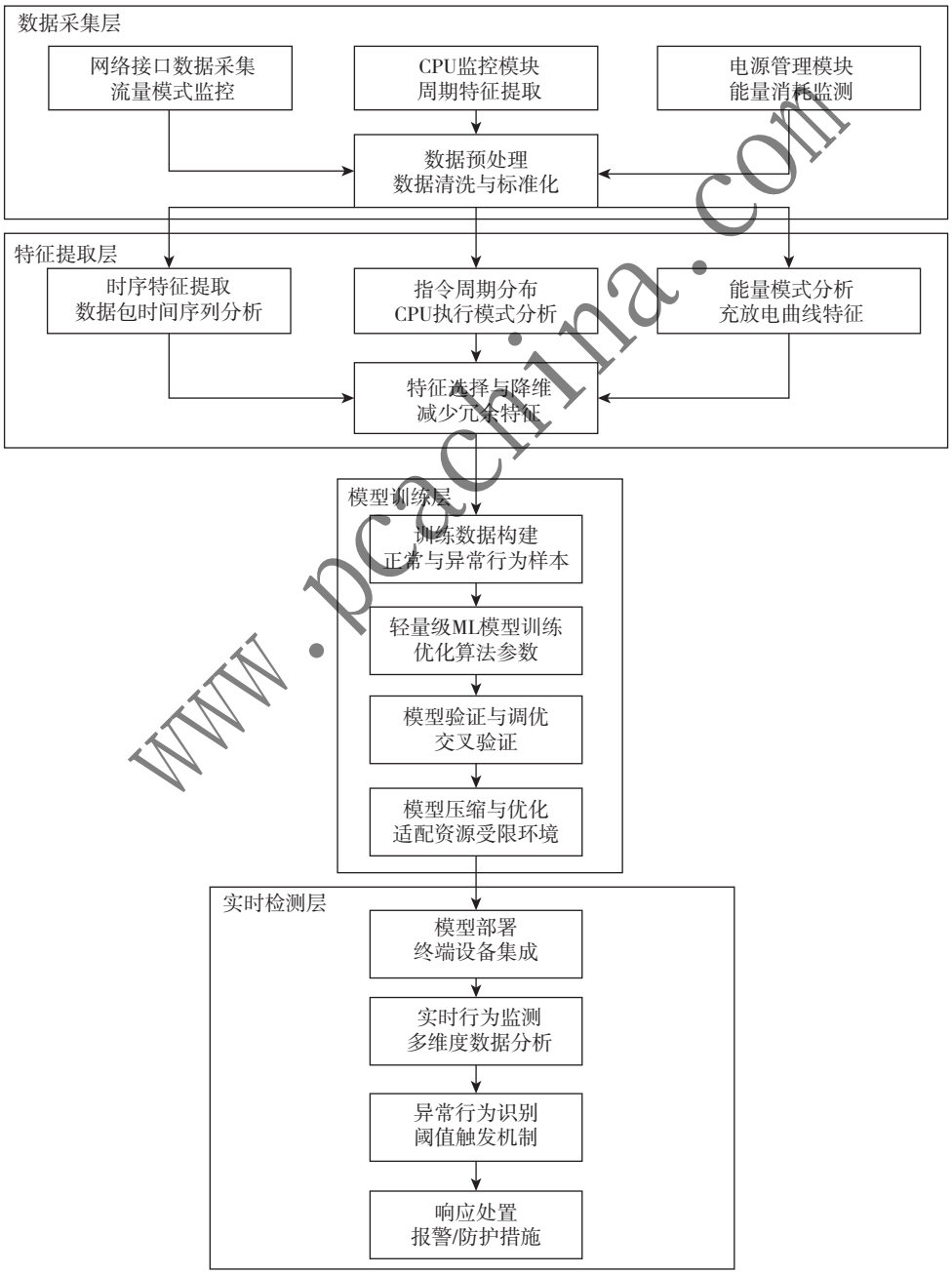

图4　终端动态行为检测模型图

3.1.3 零信任设备认证

融合轻量级生物特征、不可克隆设备指纹与一次性动态令牌的多因子绑定机制，确保每台设备身份唯一且可信。实现过程中，通过优化生物特征提取算法和设备指纹生成算法提高认证准确性和安全性（认证成功率≥99.9%），通过动态绑定协议防止攻击者伪造身份或篡改设备信息。

3.2 网络传输层加密与控制

3.2.1 量子加密融合

基于网络关键节点部署 QKD，在多层次端口加密，通过分块传输与动态端口映射，有效抵御中间人攻击与端口扫描。实现过程中，通过优化 QKD 协议实现机制和端口加密算法，提高加密效率和安全性（密钥生成速率≥10 Mb/s），同时减少对网络带宽和计算资源的需求。

3.2.2 协议语义化

基于本体的跨域互操作框架实现上下文感知访问控制，主要技术特征包括语义推理引擎、策略冲突消解和异常语义标记，实时解析指令上下文含义，自动检测并协调跨域策略矛盾，识别违背领域常识的恶意指令。实现过程中，通过优化语义推理引擎和策略冲突消解算法，提高系统智能化水平和安全性，通过异常语义标记技术及时发现和阻止恶意指令执行（语义冲突识别率≥95%）。

3.2.3 区块链身份治理

基于分布式身份注册、轻量级共识机制和实时凭证吊销等技术，实现去中心化信任，有效防止设备身份伪造攻击和审计日志篡改。在实现过程中，通过优化区块链框架和共识机制提高系统性能和安全性（交易确认延迟≤200 ms），通过实时凭证吊销技术及时撤销被攻击或失效的设备身份，防止其继续对系统造成威胁[7]。

3.3 服务端主动防御

3.3.1 PDRR 动态模型

基于“保护 - 检测 - 响应 - 恢复”（Protection-Detection-Response-Recovery，PDRR）框架，在检测层部署 AI 驱动的威胁狩猎系统，通过分析日志事件实现攻击发生后快速自动识别并阻断分布式拒绝服务（Distributed Denial of Service，DDoS）攻击。实现过程中，通过优化 AI 驱动的威胁狩猎系统和响应机制提高系统的检测和响应能力，通过恢复机制确保系统在遭受攻击后 15 min 内恢复正常运行。该防御模型在实验环境中实现了 95% 的攻击检测精度，误报率低于 2%，平均响应时间在 100 ms 以内，设备资源占用减少 30%。

3.3.2 TSL 标准化

依托 TSL 框架，将设备能力统一抽象为属性、服务、事件三元组，为跨域协同提供语义基础。实现过程中，通过优化 TSL 语法和接口协议提高系统互操作性和开发效率（设备接入效率提升 70%），通过标准化漏洞修复机制及时修复系统安全漏洞，提高系统安全性。

3.3.3 免疫防御机制

借鉴生物免疫原理抗体蠕虫与吞噬细胞蠕虫机制，实现自主响应。实现过程中，通过优化抗体蠕虫和吞噬细胞蠕虫的算法和机制提高系统自主响应能力（威胁处置时间≤1 s）和免疫记忆能力，通过修改设备漏洞提高系统安全性。

3.4 全生命周期安全管理

物联网全生命周期安全管理流程如图 5 所示。

3.4.1 开发阶段

基于集成威胁建模与模糊测试，提前发现和修复潜在安全漏洞（漏洞修复率≥95%）。实现过程中，通过优化威胁建模和模糊测试算法提高漏洞检测效率和准确性，通过修复机制及时修复发现的漏洞，提高系统安全性。

3.4.2 部署阶段

基于零信任配置，采用最小权限策略和环境指纹绑定，减少初始攻击面。实现过程中，通过优化零信任配置和最小权限策略减少系统攻击面，通过环境指纹绑定技术防止攻击者伪造环境信息进行攻击。

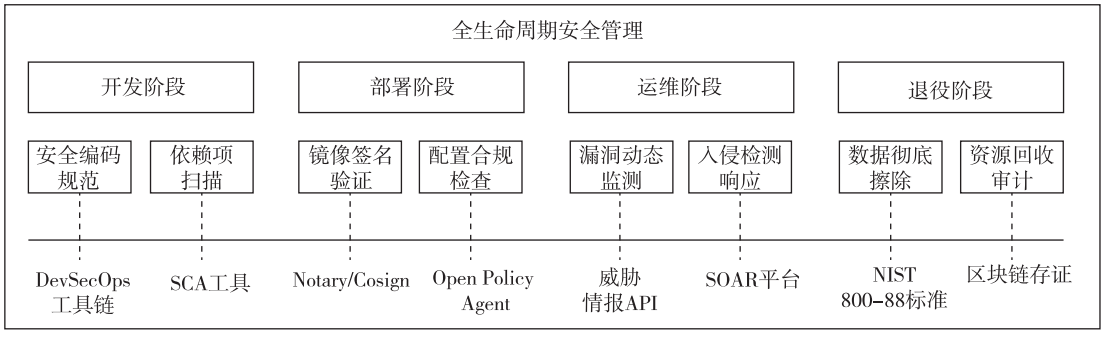

图 5 全生命周期安全管理流程图

3.4.3 运维阶段

基于“端 - 边 - 云”协同欺骗防御网格，通过动态诱饵生成、攻击链路追踪和自动策略生成等技术，实时监测和阻断异常行为。实现过程中，通过优化协同欺骗防御网格和攻击链路追踪算法提高系统实时监测和阻断能力，通过自动策略生成技术动态调整安全策略，应对不断变化的安全威胁。

3.4.4 退役阶段

基于密码学擦除和物理销毁认证，确保设备退役后数据安全擦除，降低数据残留风险。实现过程中，通过优化密码学擦除和物理销毁认证技术确保设备退役后数据安全擦除，防止数据泄露和二次利用[8]。

4 典型案例验证

为了验证“四域双层”安全框架及其多维度防御模型的有效性，本文选取了银行零信任与工业物联网两大典型场景进行实测。二者分别代表了高安全与高实时需求，能全面检验框架的适用性。

4.1 银行零信任实践

针对银行柜员业务中潜在的内部违规与外部欺诈风险，于某分行“柜员 - 反诈中心”系统进行了全栈部署。

终端域：为应对身份冒用，引入零信任设备认证，将柜员虹膜与终端设备指纹在硬件信任根内进行密码学绑定；同时，部署动态行为防护模型，采集操作轨迹与时序特征，通过轻量级 ML 算法实时判别异常行为。

边缘域：为解决交易欺诈识别延迟问题，在边缘节点植入协议语义化模块，对转账指令进行自然语言处理（Natural Language Processing，NLP）解析与上下文语义分析，实现高风险意图的本地化即时筛查。

核心网域：为保障交易数据跨域传输安全，采用 5G 切片级隔离技术，为金融业务建立端到端的逻辑专用网络，有效隔离潜在的网络层攻击。

云应用域：部署零信任策略引擎，对每一服务调用进行动态授权；并集成 PDRR 模型，利用 AI 狩猎系统关联分析日志，实现 DDoS 与复杂欺诈的自动化响应与业务快速恢复。

双层控制机制：控制面基于实时风险画像计算动态策略；数据面借助 SRv6 实现策略的跨域无损高速下发与执行，确保整体响应延迟≤500 ms 的设计目标。

如表 1 所示，本框架在提升安全性的同时，保障了业务的高效流畅运行。

4.2 工业物联网实践

面向智慧工厂中设备身份易伪造、边缘计算节点易受逃逸攻击等挑战，设计了 EdgeChainGuard 系统并进行落地验证。

表 1 银行零信任实践防御效果评估指标

评估指标	性能数值	测量方法	传统认证
攻击检出率	≥98.5%	注入 1 000 次攻击测试，记录成功检测次数	92.3%
误报率	≤1.2%	正常交易 10 万笔中误报次数	3.8%
平均响应时间	≤500 ms	从攻击发生到系统响应的时间间隔	1 200 ms
认证成功率	≥99.9%	万次认证尝试中成功次数	99.5%
资源占用率	≤5%	终端设备 CPU 和内存额外消耗	12% ~ 15%
电信诈骗阻断率	100%	9 起实际诈骗案例中的阻断情况	67%
非法控制次数尝试下降	92%	系统上线前后月均攻击尝试次数对比	45%

终端域：为强化设备本体安全，植入具备后量子密码能力的硬件信任根芯片，并基于区块链身份治理机制，实现设备身份的分布式注册与生命周期管理，杜绝身份克隆与篡改。

边缘域：为应对容器安全威胁，引入 eBPF 实时阻断技术，于操作系统内核层实现对容器非法操作的实时检测与拦截；运行自适应信任评估模型，依据设备行为动态收敛其权限，实现动态授权。

核心网域：为满足工业控制指令的实时性与确定性要求，采用 TSN 与 5G 切片融合组网，为核心控制流量提供带内安全与资源保障。

云应用域：构建免疫防御机制，通过模拟抗体扩散与吞噬细胞清除原理，实现未知威胁的分布式检测与协同处置；同时，PDRR 模型保障了从攻击识别到系统自愈的全程化管理。

双层控制机制：控制面综合设备行为、漏洞情报持续评估全局信任态势；数据面在工厂边缘侧协同执行控制策略，确保对供应链注入、异常扫描等攻击的快速遏制。

表 2 的测试结果验证了本框架在工业严苛环境下的高可靠性与实时防护能力。

5 结论

本文通过重构“四域双层”架构，系统性地剖析了物联网多维安全威胁，并针对性地提出涵盖终端、网络、服务端以及全生命周期管理的防御策略。实践验证表明，该防御体系能显著降低攻击成功率，显著提升系统韧性与运维效率。

表 2　工业物联网实践防御效果评估指标

评估指标	性能数值	测量方法	传统认证
容器逃逸检测率	≥99.2%	模拟 100 次容器逃逸攻击	88.7%
平均检测时间（MTTD）	≤50 ms	从攻击发生到检测告警的时间	850 ms
平均响应时间（MTTR）	≤15 s	从检测到攻击到完全阻断的时间	45 s
关键设备停机减少	83%	安全事件导致的停机时间对比	35%
身份认证延迟	≤50 ms	区块链身份认证增加的延迟	120 ms
供应链攻击阻断	100%	3 次实际供应链攻击测试	未能有效阻断
设备身份伪造防护	100%	尝试伪造设备身份测试	73.5%

物联网安全防御体系的未来发展需依赖技术创新、生态协同与标准建设的深度融合。在技术层面，应重点突破 6G 通感一体化架构下的无线 AI 对抗防御技术、跨域信任链构建机制及绿色安全协同机制[9]；在生态层面，应通过政产学研多方协同，推动威胁情报的高效共享与安全开发框架的规模化应用；在标准层面，需着力攻克后量子密码算法的轻量化实现、分布式密钥托管架构及经典－量子混合加密平滑过渡[10]。通过技术、生态与标准三维协同，为数字经济高质量发展提供可信赖的物联网安全基座。

参考文献

[1] 张登银，程春卯. 物联网概论［M］. 北京：人民邮电出版社，2021.

[2] 沈杰. “六域模型”打造物联网协同生态［J］. 网络传播，2017（5）：72－73.

[3] 戴立，董高峰，胡红钢，等. 针对真实 RFID 标签的侧信道攻击［J］. 密码学报，2019，6（3）：320－332.

[4] 郭凯，曹毅宁，许波，等. 基于区块链的量子加密通信方法：中国，CN202010950906.5［P］. 2023－06－27.

[5] 王卫华. 5G 网络切片安全防护技术研究［J］. 警察技术，2024（5）：50－54.

[6] 李毅，王飞. 基于硬件信任根的混合可信架构在云环境下的设计与实现［C］//首批可信计算认证产品发布会——主动免疫可信计算自主创新论坛论文集，2023：95－100.

[7] 李馥娟，马卓，王群. 区块链系统身份管理机制研究综述［J］. 计算机工程与应用，2024，60（1）：1－15.

[8] 姚凯. 物联网系统全生命周期安全管理［J］. 电子世界，2019（22）：92－93.

[9] 粟栗，崔小君，杜海涛，等. 6G 网络内生安全架构研究［J］. 中国科学：信息科学，2022，52（2）：205－216.

[10] 冯艺萌，刘昂. 迈向量子安全：后量子密码迁移研究与思考［J］. 计算机技术与发展，2024，34（5）：103－108.

（收稿日期：2025－08－20）

作者简介：

黎珂（1979－），男，硕士，高级工程师，主要研究方向：网络安全、数据安全。

版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视作该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付的稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部