基于边缘计算的物联网设备零信任安全架构设计

朱志锋

成都颐玖信息技术有限公司　四川成都

【摘要】随着物联网快速发展，海量设备接入网络。边缘计算虽提升了数据处理效率，却也带来新的安全挑战。传统安全架构已无法满足物联网设备的复杂需求，零信任安全理念“从不信任，始终验证”为其提供了新方向。本文聚焦边缘计算下物联网设备的身份伪造、数据泄露、网络攻击等问题，通过构建包含身份认证、访问控制、数据加密与安全监测的零信任安全架构，增强设备安全性与稳定性，降低安全风险。

【关键词】边缘计算；物联网设备；零信任；安全架构；身份认证

【收稿日期】2025 年 5 月 16 日　　【出刊日期】2025 年 6 月 7 日　　【DOI】10.12208/j.aics.20250015

Design of a zero trust security architecture for IOT devices based on edge computing

Zhifeng Zhu

Chengdu Yijiu Information Technology Co., Ltd. Chengdu, Sichuan

【**Abstract**】With the rapid development of the Internet of Things (IoT), a vast number of devices are now connected to networks. While edge computing has enhanced data processing efficiency, it also introduces new security challenges. Traditional security architectures can no longer meet the complex requirements of IoT devices, and the zero trust security concept, which emphasizes 'never trust, always verify,' offers a new direction. This paper focuses on issues such as identity forgery, data leakage, and network attacks in IoT devices under edge computing. By constructing a zero trust security architecture that includes identity authentication, access control, data encryption, and security monitoring, this paper aims to enhance device security and stability and reduce security risks.

【**Keywords**】Edge computing; IoT devices; Zero trust; Security architecture; Identity authentication

引言

物联网的蓬勃兴起，让海量设备互联互通，极大地改变了人们的生活与生产模式。其安全问题也日益突出，传统以网络边界为基础的安全架构，在面对复杂多变的物联网环境时，显得力不从心。边缘计算将数据处理推向网络边缘，虽提升了效率，却使设备面临更多安全隐患。在此背景下，设计基于边缘计算的物联网设备零信任安全架构迫在眉睫，旨在攻克物联网设备安全难题，保障其安全、稳定运行。

1 物联网设备安全隐患

在当今数字化浪潮中，物联网设备的广泛应用已渗透到生活的方方面面。从智能家居里的智能门锁、恒温器，到工业领域的精密机械控制器，设备类型的多样性带来了管理与安全防护的巨大挑战。受制于成本限制，许多厂商为压缩开支，在硬件设计上选用性能较低的处理器与存储芯片，导致设备难以承载复杂的安全防护程序。与此设备体积的约束使得无法内置更多安全模块，为安全防护埋下隐患。制造商对安全重视不足更是雪上加霜，部分厂商为抢占市场，在产品研发时将功能实现置于首位，忽略安全设计，导致设备出厂便存在诸如默认密码、未修复的代码漏洞等问题，为攻击者提供了可乘之机。

物联网设备运行环境的特殊性加剧了安全风险。大量设备长期处于无人值守状态，例如分布在偏远地区的气象监测传感器、野外的环境监测设备等，难以安排专人定期维护与更新[1]。即便设备厂商发布了固件更新包，由于网络环境、设备部署位置等因素，也无法及时推送更新，使得安全漏洞长时间暴露在网络空间中。攻击者通过扫描工具便可轻易发现这些漏洞，利用未修复的远程代码执行漏洞、缓冲区溢出等问题，远程控制设备，窃取数据或发动攻击。

物联网设备的数据安全问题不容忽视。随着物联

网的发展，设备收集的数据量呈爆发式增长，涵盖了用户身份、健康状况、生活习惯等高度敏感信息。在智能家居场景中，智能摄像头记录用户生活画面，智能手环收集运动与健康数据；在智能交通领域，车载设备记录行驶轨迹与驾驶行为[2]。这些数据一旦泄露，不仅会侵犯用户隐私，还可能被用于精准诈骗、身份盗用等犯罪活动。传统基于边界的安全防护策略在物联网时代逐渐失效，过去通过防火墙、入侵检测系统构建的网络边界，在物联网设备的广泛接入下变得模糊不清。

2 零信任架构搭建

零信任安全架构以“永不信任，始终验证”为核心理念，颠覆了传统网络安全中对内部网络的盲目信任。在设备接入环节，多因素认证机制成为第一道防线。这一机制并非简单的用户名与密码组合，而是将设备硬件特征、数字证书与用户密码深度融合。设备硬件特征包括独特的 MAC 地址、硬件指纹等，这些信息如同设备的“身份证”，具有唯一性与不可复制性；数字证书由权威机构颁发，包含设备身份信息与公钥，通过加密验证确保设备合法性；用户密码则作为用户操作设备的凭证。三者结合，从不同维度对设备身份进行验证，即便攻击者获取了用户密码，也难以绕过硬件与证书验证，极大提升了设备身份验证的准确性与安全性。

微分段技术是零信任架构的关键支撑，它打破了传统网络的单一防护模式，将物联网网络分割为多个独立的安全区域。每个区域根据设备功能、业务需求与安全等级进行划分，例如在智能工厂中，将生产控制区域、办公区域、数据存储区域严格分离。针对每个区域制定独立的访问控制策略，只有符合策略要求的设备才能进行跨区域通信。这种精细化的管控方式，有效阻断了攻击者在网络内的横向移动路径[3]。当攻击者入侵某个区域后，由于区域间严格的访问限制，无法轻易渗透至其他区域，从而将攻击范围控制在最小限度，降低攻击造成的损失。在数据安全方面，零信任架构贯穿数据全生命周期。

先进的安全监测系统是零信任架构的“眼睛”，它通过实时监测物联网设备的网络流量、行为模式等信息，及时发现潜在安全威胁。借助机器学习与行为分析技术，系统能够学习设备正常运行时的行为模式，建立精确的行为模型。这些模型涵盖设备的通信频率、数据传输量、访问对象等多维度信息。当设备行为偏离模型设定的正常范围时，如异常的高频数据传输、陌生地址访问，系统将立即触发警报[4]。一旦检测到安全事件，系统会迅速启动应急响应机制，自动隔离受攻击设备，切断其与网络的连接，防止攻击扩散；同时阻断恶意流量，避免更多设备受到影响。集中式的安全策略管理中心则是零信任架构的“大脑”，它统一管理访问控制策略、加密策略、监测策略等核心安全策略。

3 边缘计算与零信任融合方法

边缘计算与零信任安全架构的融合，旨在解决传统安全架构在物联网场景下的性能瓶颈与延迟问题。将零信任架构的核心功能下沉至边缘计算节点，是这一融合的关键举措。设备身份认证与访问控制决策等操作在边缘侧完成，边缘计算节点凭借其强大的本地计算能力，可快速对设备访问请求进行验证与授权。相较于传统模式下将请求上传至云端处理，这一方式极大缩短了数据传输路径，减少了延迟，提高了设备接入效率。在智慧交通场景中，车载设备通过边缘计算节点快速完成身份认证，即可实时接入交通信息网络，获取路况与导航数据，无需等待云端处理，确保信息传输的及时性。边缘计算节点与云端安全管理中心保持紧密通信，实时同步安全策略与设备状态信息，保证整个安全架构的协同运作，实现安全策略的统一管理与灵活调配。

在数据处理层面，边缘计算充分发挥其本地处理优势，助力零信任安全架构更好地应对物联网海量数据。物联网设备产生的数据量庞大且类型复杂，若全部上传至云端处理，不仅会造成网络拥塞，还会增加数据泄露风险。边缘计算节点能够对数据进行初步筛选与分析，提取关键安全信息，如设备异常行为日志、可疑通信记录等，将这些信息上传至云端进行深度分析[5]。以智能安防系统为例，摄像头采集的视频数据在边缘侧进行画面分析，识别出异常行为（如人员徘徊、物品移动）后，仅将相关报警信息与关键视频片段上传至云端，减少了数据传输量，提高了安全威胁发现的及时性。

边缘计算与零信任融合的安全保障同样至关重要。在通信方面，边缘计算节点与物联网设备之间建立基于传输层安全（TLS）协议的加密通道，确保数据在传输过程中的机密性与完整性，防止数据被窃取或篡改。对边缘计算节点进行全方位安全加固，部署防火墙防止非法网络访问，安装入侵检测系统实时监测异常行为，定期更新系统补丁修复安全漏洞，构建起坚实的安全防护屏障。利用边缘计算节点的分布式特性，构建分布式安全防护体系，多个边缘节点协同工作，相互补充[6]。当某个节点检测到安全威胁时，可迅速将信息同步至其他节点，实现联防联控，共同抵御攻击，提高安全防护的可靠性与覆盖范围，有效应对分布式攻击、大规

模数据窃取等复杂安全威胁，为物联网设备提供更高效、更可靠的安全保护。

4 安全架构效能评估

基于边缘计算的物联网设备零信任安全架构效能评估，需通过严谨的测试流程确保其安全性与实用性。在实验室环境中搭建测试平台是评估的首要环节，该平台需高度还原真实物联网应用场景。以智能家居场景为例，模拟智能门锁、智能照明、智能家电等设备的互联互通；在智能工厂场景中，构建工业控制设备、传感器、数据采集系统的协同工作环境；智能医疗场景下，模拟医疗设备、电子病历系统、远程诊疗平台的交互过程[7]。设置多样化的安全攻击场景，涵盖设备身份伪造攻击，如攻击者模拟合法设备骗取网络信任；数据篡改攻击，恶意修改传输中的数据内容；分布式拒绝服务攻击，通过大量虚假请求使设备瘫痪。通过在测试平台上复现这些攻击，全面收集安全架构应对攻击时的性能数据，包括攻击检测的准确性、系统响应攻击的速度、数据在攻击下的损失情况等关键指标。

对测试数据的深入分析是优化安全架构的关键。通过对比不同场景下安全架构的表现，分析其在安全性与可靠性方面的优势与不足。若在某类攻击场景下攻击检测率较低，需深入研究检测机制存在的问题，是否是检测规则不完善、行为模型不准确导致；若响应时间过长，则需排查系统处理流程是否存在冗余环节[8]。针对发现的问题，提出具体可行的优化方案，如改进检测算法、优化数据处理流程、调整安全策略等，进一步完善安全架构设计。将优化后的安全架构投入实际物联网项目进行测试，是验证其有效性的重要步骤。在实际应用场景中，物联网设备面临的网络环境、用户行为、安全威胁更加复杂多变，通过实际运行，持续收集安全数据与用户反馈。

5 结语

基于边缘计算的物联网设备零信任安全架构设计，成功应对了物联网设备面临的诸多安全挑战。通过构建零信任安全架构，并与边缘计算优势相结合，实现了设备身份认证、访问控制、数据加密、安全监测等核心功能，显著提升了物联网设备的安全性与可靠性。展望未来，随着物联网技术的持续创新发展，安全威胁将愈发复杂多样。需不断优化和完善该安全架构，积极引入人工智能、区块链等新兴前沿技术，进一步提升安全防护能力。加强物联网安全标准的制定与推广，推动物联网行业健康、有序发展，为物联网的广泛应用提供坚实、可靠的安全保障。

参考文献

[1] 童盛富,姜成,王磊.大型体育赛事信息系统云网端协同的网络安全架构设计实践[J].网络安全技术与应用,2025,(04): 134-138.

[2] 罗思源,何蓉,拉巴多吉.物联网设备安全防护技术研究[J].网络安全技术与应用,2023,(12):24-26.

[3] 陈念标,杨亮,唐立明,等.企业零信任网络安全架构的应用实践研究[J].中国宽带,2023,19(09):157-159.

[4] 詹文华,魏盛春.新形势下特种设备安全监察模式探讨[J].中国电梯,2022,33(20):42-45.

[5] 宋阳.基于零信任的高速公路网络安全架构[J].长江信息通信,2022,35(10):218-220.

[6] 李同寒,张辉,樊林畅,等.基于 TL-BLP 模型的零信任安全架构研究[J].网络安全技术与应用,2022,(06):17-20.

[7] 李剑,张辉,戎国庆,等.5G 边缘计算端到端安全防护分析[J].广西通信技术,2022,(01):41-44.

[8] 粟栗,庄小君,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(02):205-216.

版权声明：©2025 作者与开放获取期刊研究中心（OAJRC）所有。本文章按照知识共享署名许可条款发表。
http://creativecommons.org/licenses/by/4.0/
OPEN ACCESS