档号：2-2024-D30-JX16-\*\*\*\*

**学科分类号 630.4020**



本科学生毕业论文（设计）

**题 目 基于边缘计算的小米AIoT设备安全防护研究**

**姓 名 袁烨**

**学 号 21150069**

**院 （系） 数据科学与工程学院**

**专 业 计算机科学与技术**

**指导教师 刘品**

2025**年　4　月**

原 创 性 声 明

本人声明所呈交的毕业论文（设计）是本人在老师指导下进行的研究工作及取得的研究成果。据我查证，除了文中特别加以标注和致谢的地方外，论文（设计）中不包含其他人已经发表或撰写过的研究成果，也不包含为获得其他教育机构的学位或证书而使用过的材料。我承诺，论文（设计）中的所有内容均真实、可信。若发生版权、抄袭、剽窃等所发生的任何法律纠纷和刑事责任，由个人负责，与学院无关。

毕业论文（设计）作者签名：　　　　　日期：　　年　　月　　日

版权使用授权书

本学位论文作者完全了解云南师范大学商学院有关保留、使用论文的规定，学校有权保留并向国家有关部门或机构送交论文的复印件和磁盘，允许论文被查阅和借阅。学校可以公布论文的全部或部分内容，可以采用影印、缩印或其他复制手段保存论文，对优秀论文（设计）编印成册。学生毕业论文（设计）成果转让按相关法规执行。

（保密的学位论文在解密后适用本授权书）

毕业论文（设计）作者签名：　　　　　指导教师签名：

日期：　　年　　月　　日　　　　　　日期：　　年　　月　　日

摘 要

本文研究了基于边缘计算的小米AIoT（人工智能物联网）设备的安全防护机制。随着物联网技术的快速发展，小米AIoT设备在智能家居、智能穿戴、智能安防等领域得到了广泛应用。然而，这些设备在提供便捷服务的同时，也面临着严峻的安全挑战。边缘计算作为一种将计算和数据存储移动到网络边缘的新型计算模式，能够有效降低网络传输负担，提高数据处理的实时性。本文分析了小米AIoT设备在边缘计算环境下的安全需求，探讨了现有的安全防护技术，并提出了一种综合性的安全防护方案。该方案结合了身份认证、数据加密、访问控制等多种技术手段，旨在保障小米AIoT设备在边缘计算环境下的数据安全和隐私保护。通过模拟实验和实际应用验证，本文证明了所提方案的有效性和可行性。

**关键词：**边缘计算；小米AIoT设备；安全防护；身份认证；数据加密；访问控制

Abstract

This paper studies the security protection mechanism of Xiaomi AIoT (Artificial Intelligence Internet of Things) devices based on edge computing. With the rapid development of the Internet of Things technology, Xiaomi AIoT devices have been widely used in smart home, smart wearables, smart security and other fields. However, these devices also face severe security challenges while providing convenient services. Edge computing, as a new computing mode that moves computing and data storage to the network edge, edge computing can effectively reduce the burden of network transmission, and improve the real-time performance of data processing. This paper analyzes the security requirements of Xiaomi AIoT equipment in the edge computing environment, discusses the existing security protection technology, and puts forward a comprehensive security protection scheme. The solution combines identity authentication, data encryption, and access control, aiming to ensure the data security and privacy protection of Xiaomi AIoT devices in the edge computing environment. Through simulation experiments and practical applications verification, this paper proves the effectiveness and feasibility of the proposed scheme.

**Key words:** edge computing; Xiaomi AIoT device; security protection; identity authentication; data encryption; access control

**目 录**

[摘 要 I](#_Toc195476649)

[Abstract II](#_Toc195476650)

[1引言 1](#_Toc195476651)

[1.1 研究背景与意义 1](#_Toc195476652)

[1.2 研究目的与方法 2](#_Toc195476653)

[1.3 研究创新点与难点 3](#_Toc195476654)

[2相关理论基础 5](#_Toc195476655)

[2.1 AIoT 设备概述 5](#_Toc195476656)

[2.2 边缘计算技术原理与优势 6](#_Toc195476657)

[2.3 设备安全防护相关理论 8](#_Toc195476658)

[3小米 AIoT 设备安全威胁分析 9](#_Toc195476659)

[3.1 常见攻击场景分类 9](#_Toc195476660)

[3.2 传统安全防护措施及其局限性 9](#_Toc195476661)

[3.3 小米 AIoT 设备安全现状分析 10](#_Toc195476662)

[3.4 威胁影响与防护挑战 11](#_Toc195476663)

[4边缘计算在小米 AIoT 设备安全防护中的应用 12](#_Toc195476664)

[4.1 边缘计算在小米 AIoT 设备中的应用场景 12](#_Toc195476665)

[4.2 基于边缘计算的安全防护模型设计 13](#_Toc195476666)

[4.2.1分层防御架构 13](#_Toc195476667)

[4.2.2 关键技术实现 14](#_Toc195476668)

[4.3 基于边缘计算的安全防护架构与技术实现 16](#_Toc195476669)

[5边缘计算仿真平台构建 18](#_Toc195476670)

[5.1 开源框架选型与二次开发 19](#_Toc195476671)

[5.2 系统模块设计 19](#_Toc195476672)

[5.3 可视化界面与数据库 21](#_Toc195476673)

[6小米 AIoT 设备安全防护效果评估与优化建议 21](#_Toc195476674)

[6.1 安全防护效果评估指标与方法 21](#_Toc195476675)

[6.2 攻击场景模拟 23](#_Toc195476676)

[6.3 结果分析 24](#_Toc195476677)

[6.4 安全防护体系的优化建议 25](#_Toc195476678)

[7结论与展望 26](#_Toc195476679)

[7.1 研究成果总结 26](#_Toc195476680)

[7.2 未来研究方向 27](#_Toc195476681)

[8参考文献 28](#_Toc195476682)

[致 谢 30](#_Toc195476683)

基于边缘计算的小米AIoT设备安全防护研究

# 1引言

## 1.1 研究背景与意义

随着科技的飞速发展，物联网（IoT）技术的迅猛发展推动了智能社会的进程，使人类生活、工作、生产模式发生了深刻的变革。人工智能与物联网（AIoT）的融合已成为当今社会的重要趋势。据统计，物联网设备的数量预计将在2030年突破750亿台，涉及智能家居、工业4.0、智慧医疗和智能交通等诸多领域[15]。通过设备、网络和系统的互联互通，IoT显著提高了社会运行效率，拓展了人类的生活可能性。AIoT 技术将人工智能的智能决策能力与物联网的设备连接能力相结合，实现了万物数据化和万物智联化，为人们的生活和工作带来了极大的便利 。

然而，AIoT 设备的安全问题也日益凸显，成为制约其发展的重要因素。AIoT 设备通常收集、传输和存储大量的用户数据，包括个人信息、行为习惯等敏感信息。一旦这些设备的安全防护措施不到位，数据泄露、设备被攻击等安全事件就可能发生，给用户带来严重的损失。比如，2017 年，美国发生了大规模的物联网设备 DDoS 攻击事件，黑客利用大量被感染的物联网设备发动攻击，导致众多网站瘫痪，造成了巨大的经济损失。此外，AIoT 设备的安全漏洞还可能被攻击者利用，实现对设备的远程控制，从而威胁到用户的人身安全和财产安全。如智能摄像头被攻击后，黑客可能会实时监控用户的生活，侵犯用户的隐私。据相关统计，近年来，AIoT 设备的安全事件呈逐年上升趋势，安全问题已经成为 AIoT 行业发展的瓶颈。

小米作为全球领先的 AIoT 平台企业，在 AIoT 领域取得了显著的成就。截至目前，小米 AIoT 平台已经成为全球最大的消费级 AIoT 平台，全球联网设备数达到数亿台，接入设备数超过 2000 多种，合作伙伴有 1300 多家[4]。小米的 AIoT 设备涵盖了智能家居、智能穿戴、智能音箱等多个领域，为用户提供了丰富的智能生活体验。然而，随着小米 AIoT 设备数量的不断增加和应用场景的不断拓展，其安全防护面临着越来越严峻的挑战。如何保障小米 AIoT 设备的安全，保护用户的隐私和数据安全，成为小米亟待解决的问题。

边缘计算作为一种新兴的计算模式，为小米 AIoT 设备的安全防护带来了新的机遇。边缘计算将数据处理和决策能力从云端转移到设备端或网络边缘，减少了数据传输的延迟和带宽需求，提高了系统的实时性和可靠性。同时，边缘计算还可以在本地对数据进行处理和分析，减少了数据在网络传输过程中的暴露风险，增强了数据的安全性。在小米 AIoT 设备中应用边缘计算技术，可以实现对设备的实时监控和管理，及时发现和处理安全威胁，提高设备的安全防护能力。例如，通过在边缘设备上部署入侵检测系统，可以实时监测设备的网络流量，及时发现异常流量和攻击行为，并采取相应的防护措施。

本研究旨在深入探讨基于边缘计算的小米 AIoT 设备安全防护技术，具有重要的理论和实践意义。从理论层面来看，当前关于 AIoT 设备安全防护的研究虽然众多，但结合边缘计算技术进行的研究还相对较少。本研究将边缘计算与小米 AIoT 设备安全防护相结合，有助于丰富和完善 AIoT 设备安全防护的理论体系，为后续的研究提供新的思路和方法。

## 1.2 研究目的与方法

本研究的主要目的是借助开源边缘计算平台进行二次开发，设计并实现一种高效、可靠的基于边缘计算的小米 AIoT 设备安全防护模型。具体而言，旨在通过对边缘计算在物联网设备中的应用现状进行深入分析，识别并分类针对小米 AIoT 设备的常见安全威胁，如中间人攻击、DDoS 攻击等，并研究其对 IoT 设备及其网络的影响。基于此，设计相关的安全模型和入侵检测框架，通过模拟环境中的实验验证，评估其有效性和性能，确保系统可用性和稳定性、数据交换的准确性和不可追溯性，以及源认证和消息完整性。

在研究过程中，综合运用了多种研究方法，力求从多个维度对研究对象进行深入分析。首先是文献研究法，通过广泛查阅国内外关于 AIoT 设备安全、边缘计算技术以及小米 AIoT 发展的相关文献资料，包括学术期刊论文、行业报告、专利文献等，梳理出该领域的研究现状、发展趋势以及存在的问题，为后续的研究奠定坚实的理论基础。例如，通过对相关学术期刊论文的研读，了解边缘计算在物联网安全领域的应用原理和技术优势。

采用模块化设计方法，将分布式安全防护框架拆分为数据加密、身份认证、入侵检测和协同防护等功能模块。每个模块独立开发和优化，同时保证模块间的接口标准化，便于后期的集成和扩展。分析这些技术的原理、特点以及在实际应用中的优势和局限性，为进一步优化安全防护技术提供依据。例如，研究加密技术在保护 AIoT 设备数据传输和存储过程中的应用，探讨如何提高加密算法的安全性和效率，以更好地应对日益复杂的安全威胁。

在研究过程中，充分参考小米 2020 年发布的消费级物联网安全基线，从硬件安全、通信加密、系统权限控制等多个维度构建小米 AIOT 安全防护的基础框架。在硬件安全方面，严格把控硬件组件的选择和使用，确保蓝牙 SoC SDK 版本具备最新的安全特性，加强蓝牙配对过程中的合法性和完整性校验，同时采用防强电磁攻击和物理拆除的防护机制，防止物理攻击对设备造成损害。在通信加密方面，针对不同的通信链路，如低功耗蓝牙（BLE）通信、Zigbee 通信、以太网和 WiFi 通信等，分别制定相应的加密和鉴权策略，保护数据传输的机密性和完整性。在系统权限控制方面，对固件升级包进行严格的完整性和合法性检查，限制高风险网络服务，加强对嵌入式 Linux 系统的安全管理，包括地址空间布局随机化、Bootloader 启动安全、串口权限管理等，防止系统漏洞被利用。

结合边缘 AI 在物联网安全中的应用研究成果，引入联邦学习、可信执行环境（TEE）、轻量级入侵检测等先进技术，进一步增强边缘设备的安全性。联邦学习技术可以在保护数据隐私的前提下，实现多个设备之间的数据协同学习，提高模型的准确性和泛化能力。可信执行环境（TEE）则为敏感数据和关键计算提供了一个安全的执行空间，防止数据被窃取和篡改。轻量级入侵检测技术能够实时监测设备的网络流量和行为，及时发现并预警潜在的安全威胁，为系统的安全运行提供保障。

本研究还将运用 Wireshark、MQTT.fx 等专业软件进行抓包分析，深入了解小米 AIoT 设备的通信协议和数据传输特征，为安全防护模型的设计提供数据支持。通过 Matlab 进行数据图表的绘制和分析，直观展示实验结果和系统性能指标，以便更好地评估安全防护模型的有效性和性能表现。

## 1.3 研究创新点与难点

本研究的创新点主要体现在以下几个方面：基于开源边缘计算平台进行二次开发，构建了一个具有可视化界面和分析总结模块的边缘计算仿真平台，实现了对边缘计算设备状态、网络流量、安全事件等信息的实时监控和管理，同时支持边缘设备的增删改查操作，为研究和测试提供了便捷的环境。

提出了一种多层安全体系架构，结合攻击场景建模、加密认证技术及动态防御策略，全面提升小米 AIoT 设备的安全防护能力。在通信层，采用 MQTT over TLS 加密通道与 OPC UA 协议规范数据格式，确保数据传输的安全和规范；在数据层，应用差分隐私与区块链日志记录技术，保护数据的隐私和完整性；在应用层，结合零信任架构与 AI 异常检测（LSTM 时序预测）实现动态访问控制，根据设备的实时状态和行为动态调整访问权限，有效防范各种安全威胁。设计了基于孤立森林的异常检测算法，并将其应用于入侵检测系统（IDS）中，能够快速准确地识别出异常行为和潜在的攻击，提高了系统的检测效率和准确性。

深度结合小米案例进行研究，目前关于 AIoT 设备安全防护的研究多为一般性探讨，缺乏对具体企业案例的深入剖析。本研究聚焦小米这一全球领先的 AIoT 平台企业，详细分析其基于边缘计算的 AIoT 设备安全防护体系，能够为小米及其他企业提供具有针对性和可操作性的建议，具有很强的实践指导意义。通过对小米边缘计算实现本地数据加密和入侵检测的防护研究，能够直观地展示边缘计算在提升 AIoT 设备安全性能方面的实际效果，为其他企业提供了可借鉴的经验。

本研究将边缘计算技术与 AIoT 设备安全防护进行有机融合。当前，虽然边缘计算在物联网领域有一定应用，但在 AIoT 设备安全防护方面的深入研究尚显不足。本研究深入挖掘边缘计算在提升 AIoT 设备安全防护能力方面的潜力，探索其在数据加密、访问控制、入侵检测等关键安全技术中的应用，为 AIoT 设备安全防护提供了新的技术思路和方法。

在研究过程中还面临着诸多难点。小米 AIoT 设备种类繁多，通信协议和数据格式复杂多样，如何实现对不同设备的统一管理和安全防护是一个巨大的挑战。需要深入研究各种设备的通信机制和数据特征，制定通用的安全策略和防护措施，确保安全防护模型的兼容性和扩展性。

边缘计算环境下的资源有限，如何在有限的资源条件下实现高效的安全计算和数据处理是另一个难点。需要对加密算法、入侵检测算法等进行优化和精简，降低计算资源的消耗，同时采用分布式计算和缓存技术等手段，提高系统的处理能力和响应速度。

全面梳理小米基于边缘计算的 AIoT 设备安全防护体系并非易事。该体系涉及硬件安全、通信链路安全、系统安全、软件安全等多个方面，各个方面之间相互关联、相互影响[12]。同时，小米 AIoT 设备的应用场景广泛，不同场景下的安全需求和防护策略也存在差异。因此，要构建一个全面、系统、有效的安全防护体系，需要综合考虑各种因素，进行深入的调研和分析 。此外，随着技术的不断发展和安全威胁的日益多样化，如何确保所构建的安全防护体系具有前瞻性和适应性，能够及时应对新出现的安全挑战，也是研究过程中需要克服的难点之一。

# 2相关理论基础

## 2.1 AIoT 设备概述

AIoT，即人工智能物联网（Artificial Intelligence & Internet of Things），是人工智能技术（AI）与物联网（IoT）在实际应用中的深度融合。这一融合并非简单的叠加，而是在技术、应用与生态等多层面实现了有机结合[16]。物联网负责从不同维度采集海量数据，这些数据来源于各类传感器、智能设备等，它们被存储于云端或边缘端；而人工智能则借助大数据分析、机器学习、深度学习等技术手段，对这些数据进行智能化处理，从而实现万物数据化与万物智联化 。其最终目标是构建一个高度智能化的生态体系，在这个体系中，不同类型的智能终端设备，如智能家居设备、智能穿戴设备、工业智能传感器等，能够打破彼此之间的隔阂，实现数据的自由流通与协同工作；不同的系统平台，无论是基于云计算的服务平台，还是本地的嵌入式系统，都能相互兼容，为设备的互联互通提供坚实的支撑；不同的应用场景，如智能家居中的安防监控、智能家电控制，智能工业中的生产流程优化、设备故障预测，以及智能医疗中的远程诊断、健康监测等，都能紧密相连，为用户提供全方位、个性化的智能服务。

AIoT设备的核心特性体现在数据驱动、智能处理与互融互通[14]。数据作为核心要素，支撑设备的决策优化，如通过持续分析用户习惯和环境数据，设备可提供更贴合需求的服务；智能化处理能力让设备能本地完成数据分类、趋势预测等任务，提升响应效率；而互融互通性则打破设备与系统的壁垒，使不同设备在统一平台上协同，例如智能家居中，用户通过智能音箱即可控制灯光、窗帘、家电等多设备联动，实现场景化智能控制。

以小米为例，其AIoT布局覆盖智能家居、智能穿戴与智能音箱等领域。智能家居中，智能家电通过远程控制、自动调节等功能提升生活便捷性，安防设备实现家庭安全的实时监测，智能照明产品支持个性化场景设置；智能穿戴设备如手环、手表整合健康监测、运动记录等功能，为用户提供个性化健康管理；智能音箱作为交互中枢，通过语音识别技术实现信息查询、设备控制等操作，成为连接各类智能设备的核心入口。这些实践体现了AIoT如何通过技术融合，将单一设备的功能扩展为系统性的智能服务，覆盖生活、健康、安全等多个场景。

当前，AIoT正从单一设备智能化向跨场景生态发展，未来将更注重轻量化技术部署、设备协同效率提升与用户体验优化，推动智能技术更自然地融入生活与产业，实现“设备即服务”的泛在智能愿景。

## 2.2 边缘计算技术原理与优势

边缘计算作为一种分布式计算模型，将数据处理和存储的能力从集中式的云数据中心推向更接近数据产生源头或最终用户的边缘设备上。其核心原理基于分布式计算，通过将计算任务分散到网络的边缘节点，如智能设备、网关、路由器或是专门的边缘服务器等，这些节点靠近数据产生的源头或者用户，极大地减少了数据传输的距离和时间，从而提升处理速度和降低延迟[13]。边缘计算的核心架构主要包括三个层次：边缘设备层、边缘节点层和云端层 。

边缘设备层是最接近数据源的一层，包含了各种类型的物联网设备和传感器，如智能摄像头、智能门锁、温度传感器、湿度传感器等。这些设备负责采集物理世界中的各种数据，并将其传输给边缘节点层。边缘节点层位于边缘设备层与云端层之间，是边缘计算的关键部分。它由具备计算和存储能力的设备组成，如边缘服务器和网关。边缘节点处理来自边缘设备的数据，进行预处理、分析和决策。云端层负责大数据分析、长期存储和为边缘节点提供更新与策略。它深度挖掘历史数据，发现潜在规律，支持边缘节点智能决策。边缘计算模型图如图1所示。

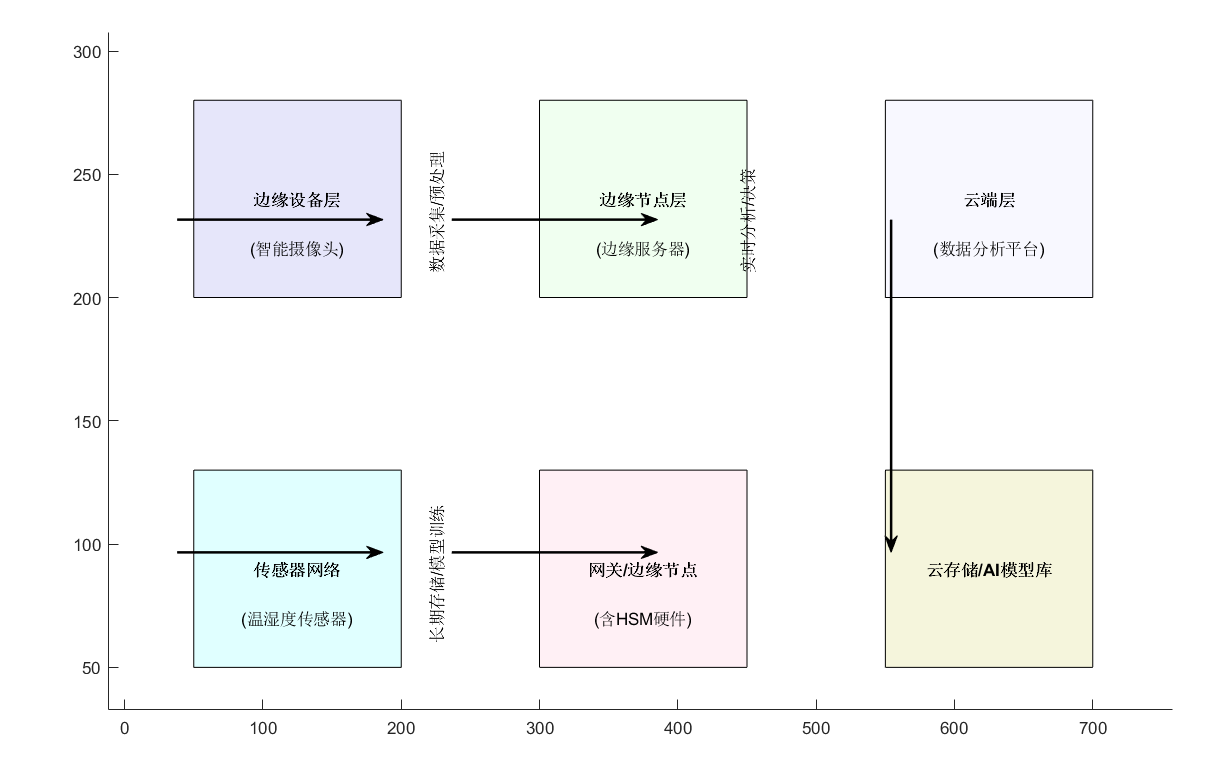


图1 边缘计算模型图

在工作流程中，边缘设备收集数据后，数据会被发送至边缘节点进行实时处理。例如，在智能安防中，摄像头捕获的视频流会被边缘节点分析，以识别异常情况，如入侵或火灾。一旦发现异常，节点会启动报警并通知相关人员。处理后的关键或异常数据会被上传至云端，用于进一步分析和存储，便于后续查询和统计。

边缘计算通过在数据源附近的边缘节点处理数据，显著降低了延迟，这对于实时性要求高的应用如自动驾驶至关重要。例如，在自动驾驶中，车辆可实时处理传感器数据，快速做出驾驶决策，保障行车安全[10]。

边缘计算通过在本地处理数据，仅传输必要结果到云端，有效减轻网络负担。例如，在智能工厂视频监控中，边缘计算可实时分析视频数据，仅上传关键信息，减少网络数据传输，提升网络效率。

边缘计算延迟优化模型

其中：

边缘计算还具备离线处理与数据优化的能力。边缘设备能够执行数据的预处理、过滤、压缩和聚合等操作，减少了需要上传到云端的数据量，降低了网络带宽需求，同时有助于提升数据处理的效率和系统的响应速度。实时性与敏捷性是边缘计算的显著优势之一，这使得它能更好地支持实时数据处理和分析。

在安全与隐私保护方面，边缘计算通过减少数据向云端的传输，降低了数据泄露的风险，同时可以在边缘节点实施更为严格的数据加密和访问控制策略，增强数据的安全性和用户隐私保护。在智能家居场景中，用户的家庭数据，如摄像头拍摄的视频、智能门锁的开锁记录等，涉及个人隐私，通过边缘计算在本地处理和存储这些数据，避免了数据在传输过程中被窃取的风险，保障了用户的隐私安全。

边缘计算还有助于优化网络资源使用，减少不必要的数据传输，从而降低运营成本，并且能够在网络不稳定或中断时，提供更稳定的本地服务。在一些偏远地区，网络信号可能不稳定，边缘计算设备可以在本地完成数据处理和存储，即使与云端的连接暂时中断，也能保证设备的正常运行，为用户提供持续的服务。

数据安全是边缘计算的关键优势。在该模式下，敏感数据在本地边缘设备或节点处理和存储，减少了网络传输风险，降低了数据被窃或篡改的可能。特别是涉及隐私和机密的数据，如医疗和金融数据，本地处理保护了用户隐私。例如，医疗领域中，患者健康数据在本地设备分析处理，仅传输经过处理的汇总数据到云端，有效保护隐私。

## 2.3 设备安全防护相关理论

设备安全防护是指通过一系列技术手段和管理措施，保障设备在整个生命周期内的安全性、可靠性和稳定性，防止设备遭受各种安全威胁，保护设备所存储和处理的数据的完整性、保密性和可用性，确保设备能够正常运行，为用户提供安全可靠的服务 。其核心目标在于防止设备受到恶意攻击、数据泄露、硬件故障、软件漏洞等安全风险的影响，避免因设备安全问题导致的业务中断、经济损失以及对用户隐私和权益的侵害 。

在AIoT设备安全领域，加密技术是数据安全的关键。它通过算法将数据转换为密文，防止数据在传输和存储时被非法读取[9]。对称加密如AES，速度快，适用于大量数据加密；非对称加密如RSA，使用公私钥，适用于身份认证和数字签名，确保通信双方身份真实性和数据完整性。

AES-128加密算法轮函数

其中：

访问控制技术通过管理用户或设备的访问权限来确保设备安全，只有授权用户才能访问特定资源[8]。RBAC模型根据用户角色分配权限，小米AIoT系统中，管理员可配置设备和管理用户，普通用户仅控制授权设备。ABAC模型依据用户、资源和环境属性动态确定权限，在智能工厂中，设备状态、工作区域和时间决定用户访问权限，如维护人员在规定时间内可维护设备。

入侵检测技术实时监控设备和网络，发现潜在威胁。基于特征的系统利用预定义攻击特征库识别已知攻击。例如，检测到与恶意软件传播特征匹配的数据包时，系统会发出警报。小米智能路由器使用此技术识别DDoS等常见攻击。基于异常的系统建立正常行为模型，偏离模型时发出警报。智能安防摄像头分析视频和操作行为，发现异常时预警潜在入侵风险。这些技术共同保障AIoT设备安全运行。

# 3小米 AIoT 设备安全威胁分析

## 3.1 常见攻击场景分类

1. 中间人攻击（MiTM）：中间人攻击是一种常见且极具威胁性的攻击方式，攻击者通过在通信链路中巧妙地插入自己的设备，伪装成合法的通信端点，从而实现对数据的窃取、篡改或伪造[7]。在小米 AIoT 设备的应用场景中，例如智能门锁与手机 APP 之间的通信，攻击者可以利用网络漏洞或破解弱密码，在两者之间建立一个虚假的连接。当用户通过手机 APP 发送开锁指令时，攻击者能够拦截该指令，获取其中包含的用户身份信息、门锁密码等敏感数据，甚至可以篡改指令内容，导致门锁无法正常开启或被非法打开。这种攻击不仅侵犯了用户的隐私，还对用户的财产安全构成了直接威胁。

2. DDoS 攻击：DDoS 攻击，即分布式拒绝服务攻击，其原理是攻击者利用大量的傀儡机（僵尸网络），向目标设备或服务发送海量的请求，使目标设备或服务不堪重负，最终导致其无法正常提供服务。对于小米 AIoT 设备而言，DDoS 攻击可能会使边缘节点（如智能网关、路由器等）或云服务陷入瘫痪。例如，在智能家居系统中，智能网关作为连接各种智能设备的核心枢纽，一旦遭受 DDoS 攻击，大量的请求会占用网关的网络带宽和系统资源，导致网关无法及时处理各个设备的通信请求，使得智能家居设备之间无法正常通信，用户无法通过手机 APP 对设备进行控制，整个智能家居系统陷入瘫痪状态，严重影响用户的正常生活。

3. 恶意软件注入：恶意软件注入是攻击者通过寻找设备软件中的漏洞，将恶意软件植入到小米 AIoT 设备中，从而实现对设备的控制和恶意操作。以小米智能摄像头为例，攻击者可以利用摄像头固件中的安全漏洞，通过网络远程注入恶意软件。一旦恶意软件成功植入，摄像头可能会被攻击者完全控制，不仅会窃取用户的隐私视频，还可能被用于发起进一步的攻击，如参与 DDoS 攻击，成为僵尸网络的一部分。此外，恶意软件还可能篡改摄像头的设置，导致摄像头无法正常工作，或者将摄像头拍摄的视频流发送到攻击者指定的服务器，给用户带来极大的安全隐患。

## 3.2 传统安全防护措施及其局限性

传统的安全防护措施在保护小米 AIoT 设备安全方面发挥了一定的作用，但随着物联网技术的不断发展和安全威胁的日益复杂，这些措施逐渐暴露出诸多局限性，需要结合新的技术和理念，构建更加完善的安全防护体系。

传统措施如加密传输和身份认证至关重要。在加密技术方面，虽然传统的加密算法如 AES（高级加密标准）等在一定程度上保障了数据的机密性，但在边缘计算环境下，由于资源受限，复杂的加密算法可能会导致设备性能下降，无法满足实时性要求。而且，加密密钥的管理也是一个难题，一旦密钥泄露，加密的数据将失去保护。

身份认证与访问控制方面，传统的用户名密码认证方式在安全性上存在较大风险，容易被破解或窃取。基于角色的访问控制（RBAC）模型虽然能够根据用户角色分配权限，但在物联网设备多样化、用户需求复杂的情况下，其灵活性不足，难以满足动态的访问控制需求。身份认证是确认设备或用户真实性的关键，确保只有认证通过者才能访问资源。

防火墙和入侵检测系统（IDS）方面，传统防火墙主要基于端口和 IP 地址进行访问控制，难以应对新型的应用层攻击。而基于规则的 IDS 对于未知的攻击模式往往无法检测，需要不断更新规则库，且误报率较高，容易导致安全管理人员疲于应对大量的无效警报，而忽略了真正的安全威胁。

## 3.3 小米 AIoT 设备安全现状分析

小米 AIoT 设备凭借其丰富的产品线和庞大的用户群体，在智能家居市场占据重要地位。然而，随着物联网安全威胁的日益多样化和复杂化，小米 AIoT 设备也面临着严峻的安全挑战。在硬件层面，尽管小米在设备制造过程中采取了一系列安全措施，如采用安全芯片、加固硬件设计等，但仍存在物理篡改的风险。攻击者可能通过拆卸设备外壳，对硬件进行物理分析，获取敏感信息或篡改设备固件，从而控制设备或窃取用户数据[5]。

在通信层面，小米 AIoT 设备采用了多种通信协议，如低功耗蓝牙（BLE）、Zigbee、WiFi 等，不同协议在安全性能上存在差异。BLE 通信在数据传输过程中可能面临中间人攻击，攻击者可以在设备与手机之间的通信链路中插入恶意设备，窃取或篡改传输的数据。Zigbee 网络中的设备可能受到网络扫描和攻击，攻击者利用协议漏洞获取设备控制权。WiFi 通信则容易受到 DDoS 攻击，导致设备无法正常连接网络或提供服务。

从软件层面来看，小米 AIoT 设备的固件和应用程序也可能存在安全漏洞。恶意软件注入是常见的攻击手段之一，攻击者通过利用设备软件漏洞，将恶意软件植入设备，使其执行恶意操作，如窃取用户隐私、发送垃圾邮件、参与僵尸网络等。固件升级过程中的安全问题也不容忽视，如果固件升级包未经过严格的完整性和合法性验证，攻击者可能篡改升级包，导致设备被恶意控制或功能异常。

用户层面也存在安全隐患，许多用户对物联网设备的安全意识不足，设置简单易猜的密码，或者在多个设备上使用相同的密码，这使得攻击者可以轻易破解密码，获取设备访问权限。用户随意连接未知的 WiFi 网络，也可能导致设备暴露在不安全的网络环境中，增加被攻击的风险。

小米虽然在 AIoT 设备安全方面投入了大量资源，建立了完善的安全体系，包括安全团队、漏洞检测平台、隐私合规体系等，但面对不断变化的安全威胁，仍需要持续加强安全防护措施[4]，提升设备的安全性和用户的信任度。

## 3.4 威胁影响与防护挑战

随着小米 AIoT 设备的广泛应用，其面临的安全威胁也日益多样化和复杂化，这些威胁涵盖了网络攻击、数据泄露、隐私侵犯等多个关键领域，对用户的信息安全和设备的正常运行构成了严重挑战。

数据泄露风险。小米 AIoT 设备广泛应用于智能家居、智能健康等领域，收集了大量用户的隐私数据，如智能家居控制指令、个人健康信息等。一旦设备遭受攻击，数据泄露的风险极高。例如，智能家居控制指令中可能包含用户的家庭布局、设备使用习惯等信息，这些信息泄露后，攻击者可以轻易了解用户的生活规律，甚至可能对用户的家庭安全造成威胁。个人健康信息的泄露则可能导致用户的隐私被侵犯，个人信息被滥用，如被用于精准诈骗、医疗数据买卖等非法活动。

系统可用性破坏。DDoS 攻击、恶意软件注入等安全威胁可能导致小米 AIoT 设备离线或服务中断，严重破坏系统的可用性。在工业物联网场景中，若小米的工业智能设备遭受攻击而无法正常工作，可能会导致生产线停滞，造成巨大的经济损失。在智能健康领域，智能穿戴设备如果出现故障或服务中断，无法实时监测用户的健康数据，可能会延误对用户健康状况的及时判断和处理，对用户的生命健康构成潜在威胁。

DDoS攻击是网络攻击中常见且破坏力强的方式。攻击者利用大量僵尸网络对AIoT设备发起海量请求，耗尽网络带宽和服务器资源，使设备无法响应合法用户，导致瘫痪。例如，2020年针对小米智能家居的DDoS攻击，利用智能摄像头和音箱等设备攻击服务器，影响了用户使用体验和服务稳定性。

中间人攻击同样不容忽视，攻击者在小米 AIoT 设备与用户或服务器之间的通信链路中进行拦截和篡改。他们可以窃取通信过程中的敏感信息，如用户的登录凭证、设备控制指令等，还可能篡改数据，误导设备执行错误的操作。在小米智能门锁与手机 APP 通信的过程中，攻击者可能通过中间人攻击获取用户的开锁密码，进而非法打开用户的家门，给用户的财产安全和人身安全带来极大的威胁 。

部分小米 AIoT 设备的隐私政策可能不明确，导致用户难以了解数据如何被收集、使用和共享。设备的传感器可能在用户不知情的情况下共享数据给第三方，甚至被黑客利用进行实时监听和监控，如通过攻击智能音箱窃听对话，严重侵犯隐私。

# 4边缘计算在小米 AIoT 设备安全防护中的应用

## 4.1 边缘计算在小米 AIoT 设备中的应用场景

在智能家居控制中，边缘计算显著提高了设备响应速度和智能化水平。[3]以小米智能音箱为例，作为控制核心，它具备强大的边缘计算功能。用户发出语音指令后，智能音箱利用本地边缘计算模块，通过内置算法快速解析和理解指令，迅速向相关设备发送控制信号，从而实现快速响应。这种本地处理避免了网络延迟，提供了接近实时的控制体验。

在小米智能家居体系中，边缘计算通过智能网关、路由器及具备边缘处理能力的终端（如小爱音箱）构建分布式架构，将数据处理从云端下沉至网络边缘。这些边缘节点就近采集设备数据并进行本地化分析，无需依赖云端即可完成指令解析与设备控制，显著提升了系统响应速度与稳定性。例如，用户通过语音指令操控家电时，搭载边缘计算功能的设备可快速解析指令意图，直接联动灯光、空调等设备执行操作，避免了传统云端模式下的网络延迟，即使在弱网环境中也能实现高效交互。

边缘节点的核心价值在于实现 “本地实时决策 + 云端长期优化” 的协同：一方面，实时处理温湿度、设备状态等数据，基于预设规则或轻量算法即时生成控制策略，推动智能设备根据环境变化自动调节（如空调自适应温度、灯光随场景切换）；另一方面，仅将关键数据上传至云端，在减少网络负载的同时，降低隐私数据的传输风险。这种架构打破了设备依赖云端的单一模式，通过边缘层的本地化智能，让智能家居系统在响应速度、可靠性及隐私保护上均有显著提升，构建了更贴合用户需求的智能化体验。

## 4.2 基于边缘计算的安全防护模型设计

### 4.2.1分层防御架构

1. 通信层：通信层作为数据传输的通道，其安全性直接关系到整个系统的稳定运行。为了确保数据在传输过程中的安全，本模型采用 MQTT over TLS 加密通道。MQTT（Message Queuing Telemetry Transport）是一种轻量级的消息协议，特别适用于物联网环境中带宽有限的场景，具有开销小、实现标准等优势，被主流云厂商广泛应用于物联网通信。TLS（Transport Layer Security）则为 MQTT 提供了加密、完整性和认证等安全保障，通过对 MQTT 客户端和 Broker 之间的数据进行加密，防止敏感数据被未授权的用户获取、篡改和拦截，确保数据传输的机密性和完整性。

在实际应用中，客户端和服务器在建立安全连接之前，会通过 TLS 握手过程协商加密参数，包括加密算法、会话密钥和认证方法等。在握手过程中，服务器向客户端出示数字证书，客户端检查该证书，以确认它是有效的，并且是由可信的 CA（证书颁发机构）签发的。如果证书通过验证，客户端就可以与服务器建立安全连接。这种基于证书的认证方式，有效避免了中间人攻击，确保了通信双方的身份真实性。

OPC UA（Open Platform Communications Unified Architecture）协议则用于规范数据格式，它提供了一种统一的标准，使得不同设备之间能够准确、高效地进行数据交互。OPC UA 定义了丰富的数据模型和服务接口，能够实现数据的实时传输、远程访问、事件通知等功能，为物联网设备之间的互联互通奠定了坚实的基础。在小米 AIoT 设备中，各种智能设备通过 OPC UA 协议将采集到的数据进行标准化处理，然后通过 MQTT over TLS 加密通道传输到云端或其他设备，确保数据在传输过程中的安全性和准确性。

2. 数据层：数据层负责数据的存储和管理，为了保护数据的隐私和完整性，本模型应用差分隐私与区块链日志记录技术。差分隐私是一种隐私保护技术，它通过在数据中添加适当的噪声，使得攻击者难以从数据中推断出个体的敏感信息。在小米 AIoT 设备收集的用户数据中，如智能家居控制指令、个人健康信息等，可能包含用户的隐私。通过差分隐私技术，在不影响数据整体分析价值的前提下，对数据进行隐私保护，确保即使数据泄露，攻击者也无法获取用户的真实隐私信息。

区块链日志记录则利用区块链的去中心化、分布式存储和密码学特性，确保数据的不可篡改和可追溯性。每个数据记录都被打包成一个区块，区块之间通过哈希值相互链接，形成一个不可篡改的链式结构。一旦数据被记录在区块链上，就无法被删除或篡改，因为任何的篡改都会破坏整个区块链的结构。同时，区块链的分布式存储使得数据副本分布在多个节点上，即使部分节点被攻击，其他节点仍保留完整数据，保证了数据的安全性和可靠性。在小米 AIoT 设备的数据管理中，将重要的操作日志、设备状态数据等记录在区块链上，用户可以随时追溯数据的来源和变化，确保数据的真实性和完整性。

3. 应用层：应用层是用户与系统交互的接口，也是安全防护的关键环节。本模型结合零信任架构与 LSTM 异常检测实现动态访问控制。零信任架构摒弃了传统的 “信任边界” 概念，不再默认内部网络是安全的，而是对所有的访问请求进行严格的身份认证和权限验证，无论请求来自内部还是外部。在小米 AIoT 设备的应用场景中，即使是同一家庭网络中的设备之间的访问，也需要进行身份认证和权限验证，防止内部设备被恶意利用。

LSTM（Long Short-Term Memory）是一种特殊的循环神经网络，能够有效处理时间序列数据，捕捉数据中的长期依赖关系。在本模型中，利用 LSTM 对设备的行为数据进行学习和分析，建立正常行为模型。当有新的访问请求时，通过 LSTM 模型预测该请求是否符合正常行为模式，如果发现异常，则及时进行告警并采取相应的访问控制措施，如限制访问权限、阻断连接等。通过这种动态访问控制机制，能够根据设备的实时状态和行为动态调整访问权限，有效防范各种安全威胁，确保应用层的安全性。

### 4.2.2 关键技术实现

1. 端到端加密：端到端加密是保障数据安全传输的核心技术，本模型采用 TLS/SSL+X.509 证书认证的方式实现端到端加密。TLS/SSL 作为传输层安全协议，通过加密、保证数据完整性和认证来提供安全性。在加密过程中，使用对称加密算法对数据进行加密，提高加密效率；同时利用非对称加密算法进行密钥交换和身份认证，确保密钥的安全传输和通信双方的身份真实性。

X.509 证书则用于验证通信双方的身份，它是一种包含数字身份信息的数据结构，由证书颁发机构（CA）签发。证书中包含了版本号、序列号、颁发者、有效期、主体、公钥信息、证书扩展、签名算法和颁发者的数字签名等元素。在通信过程中，客户端和服务器通过交换 X.509 证书，验证对方的身份和证书的有效性。如果证书通过验证，双方就可以建立安全连接，进行加密通信。

结合小米澎湃 OS 的 TEE（可信执行环境）技术，进一步增强端到端加密的安全性。TEE 为敏感数据和关键计算提供了一个安全的执行空间，与设备的主操作系统隔离，防止数据被窃取和篡改。在小米 AIoT 设备中，利用 TEE 技术对加密密钥进行存储和管理，确保密钥的安全性。同时，在数据传输过程中，通过 TEE 对数据进行加密和解密，保证数据在传输和处理过程中的机密性和完整性。

2. 实时监控：实时监控是及时发现安全威胁的重要手段，本模型基于孤立森林算法构建轻量级 IDS（入侵检测系统），实现对异常流量的实时识别。孤立森林算法是一种基于二叉树的异常检测算法，它采用随机化的方式对数据进行分裂，通过度量数据点在二叉树中的路径长度来判断其是否为异常点。正常数据点由于分布较为密集，需要较多的分裂次数才能被孤立，因此其在二叉树中的路径长度较长；而异常数据点由于分布较为稀疏，可能只需要较少的分裂次数就可以被孤立，其在二叉树中的路径长度较短。

在小米 AIoT 设备的网络流量监控中，将网络流量数据作为输入，通过孤立森林算法实时计算每个数据点的异常分数。当异常分数超过设定的阈值时，判定该流量为异常流量，及时发出警报。与传统的入侵检测算法相比，孤立森林算法具有计算效率高、对高维数据适应性强等优点，能够在资源受限的边缘设备上快速准确地识别出异常流量，为系统的安全运行提供保障。

3. 自动化响应：自动化响应是降低安全威胁影响的关键措施，本模型采用触发式隔离 + 密钥轮换机制，实现自动化响应。当轻量级 IDS 检测到异常流量或其他安全威胁时，立即触发隔离机制，将受到威胁的设备或网络连接进行隔离，防止攻击的扩散。在智能家居系统中，如果检测到某个智能设备遭受恶意软件注入攻击，立即切断该设备与其他设备的网络连接，避免恶意软件传播到其他设备。

密钥轮换机制则定期更换加密密钥，降低密钥被破解的风险。在数据传输和存储过程中，加密密钥是保障数据安全的关键。随着时间的推移，密钥可能会面临被破解的风险，因此定期更换密钥能够有效增强数据的安全性。在小米 AIoT 设备中，根据设定的时间间隔或特定的事件触发条件，自动进行密钥轮换。在密钥轮换过程中，确保新密钥的安全生成和分发，同时保证数据的连续性和可用性。通过触发式隔离和密钥轮换机制的协同工作，能够及时有效地应对安全威胁，降低攻击对系统造成的损害。

## 4.3 基于边缘计算的安全防护架构与技术实现

基于边缘计算的小米 AIoT 设备安全防护架构，融合了边缘计算、物联网和安全防护等多领域技术，旨在为小米 AIoT 设备提供全方位、多层次的安全保障。该架构以边缘节点为核心，结合云端服务，形成了一个分布式的安全防护体系。

在边缘节点层面，部署了各类边缘计算设备，如网关、路由器、小爱音箱（蓝牙网关）和摄像头等。这些设备不仅具备数据处理和转发能力，还集成了安全防护模块，实现了对本地设备和网络的实时监控与防护。网关作为连接本地设备与云端的桥梁，承担着数据汇聚、协议转换和安全过滤的重要职责。通过在网关上部署防火墙、入侵检测系统和加密模块，能够有效阻止外部攻击，保护本地设备的安全通信。路由器则负责本地网络的路由转发和流量管理，通过访问控制列表（ACL）和流量监测技术，实现对网络流量的精细化管理，防止网络拥塞和恶意流量的入侵。

小爱音箱（蓝牙网关）在智能家居场景中扮演着重要角色，它不仅能够实现语音交互和设备控制，还可以作为蓝牙设备的网关，连接各类蓝牙智能设备。为了保障蓝牙通信的安全，小爱音箱采用了蓝牙低功耗（BLE）安全协议，结合设备认证和加密技术，防止蓝牙链路被破解和数据被窃取。摄像头作为智能家居的视觉传感器，采集的视频数据涉及用户的隐私安全。因此，摄像头采用了硬件加密芯片和视频加密算法，对视频数据进行实时加密处理，确保视频数据在传输和存储过程中的安全性。

云端服务则为边缘节点提供了强大的支持和补充。云端存储了大量的安全策略、威胁情报和设备管理信息，通过与边缘节点的实时通信，实现安全策略的动态更新和设备的远程管理。云端还利用大数据分析和机器学习技术，对海量的安全数据进行分析和挖掘，及时发现潜在的安全威胁，并将威胁情报反馈给边缘节点，实现对安全威胁的提前预警和防范。

在技术实现方面，基于开源边缘计算平台 EdgeX Foundry 进行二次开发，构建了一个功能强大、灵活可扩展的边缘计算框架。EdgeX Foundry 提供了丰富的设备管理、数据处理和通信接口，能够方便地集成各类边缘设备和应用。结合 Mosquitto（MQTT）消息代理，实现了设备之间的高效通信和数据传输。MQTT 作为一种轻量级的消息协议，具有低带宽、低功耗和高可靠性的特点，非常适合物联网设备之间的通信。通过 MQTT over TLS 加密通道，确保了数据在传输过程中的安全性和完整性。

为了实现对边缘设备的统一管理和监控，采用了 Terminator 终端管理工具。Terminator 提供了一个直观的可视化界面，管理员可以通过该界面实时查看边缘设备的状态、网络流量和安全事件等信息，实现对边缘设备的远程配置和管理。同时，Terminator 还支持设备的批量操作和自动化任务执行，提高了管理效率和运维便利性。

为了满足不同类型边缘设备的开发需求，基于 GD32F470 系列 MCU 开发环境，提供了统一的应用框架与工具链。GD32F470 系列芯片具有高性能、低功耗和丰富的外设资源等特点，非常适合作为边缘计算设备的核心处理器。通过定制的应用框架和工具链，开发者可以快速搭建各种物联网应用，并将其部署到边缘设备上。应用框架集成了多媒体、传感器、蓝牙互联等场景化框架，开发者可以根据实际需求选择合适的框架进行开发，大大缩短了开发周期，提高了开发效率。

小米构建的基于边缘计算的 AIoT 设备安全防护架构，融合了多种先进技术，形成了一个多层次、全方位的安全体系，旨在有效应对各类安全威胁，确保设备、数据和用户的安全 。

在边缘节点安全设计方面，小米采用了硬件安全模块（HSM）来保障边缘节点的硬件安全。HSM 是一种专门用于保护密钥和执行加密操作的硬件设备，具有高度的安全性和可靠性。在小米智能网关等边缘节点设备中集成 HSM，能够对设备的身份认证密钥、数据加密密钥等重要密钥进行安全存储和管理，防止密钥被窃取或篡改 。HSM 还可以执行数字签名、加密和解密等操作，确保数据的完整性和保密性。在智能网关与其他设备进行通信时，通过 HSM 对通信数据进行数字签名和加密，保证数据在传输过程中不被篡改和窃取。

在软件层面，小米对边缘节点的操作系统进行了深度定制和安全加固。通过采用最小化安装原则，去除不必要的服务和组件，减少了系统的攻击面。同时，对系统的权限管理进行了严格设置，采用细粒度的权限控制策略，确保只有授权的程序和用户能够访问系统资源。在小米边缘服务器的操作系统中，将文件系统的访问权限设置为只读，对于需要写入数据的操作，只有经过授权的特定程序才能执行，从而防止恶意软件对系统文件的篡改和破坏 。

数据加密传输是保障数据安全的关键环节。在小米 AIoT 设备的数据传输过程中，采用了多种加密算法相结合的方式，以确保数据的机密性和完整性。在设备与边缘节点之间的短距离通信中，通常采用轻量级的加密算法，如 AES - 128 算法，该算法具有加密速度快、计算资源消耗低的特点，适合在资源受限的设备上运行 。在智能家居设备与智能网关之间的通信中，使用 AES - 128 算法对设备控制指令、传感器数据等进行加密，防止数据在传输过程中被窃取和篡改 。

RBAC权限分配模型

其中：

对于设备与云端之间的长距离通信，小米采用了 SSL/TLS 协议进行加密。SSL/TLS 协议是一种广泛应用于网络通信的安全协议，它通过在通信双方之间建立安全的加密通道，确保数据的安全传输。在小米 AIoT 设备与云端服务器进行通信时，设备首先与服务器进行握手，协商加密算法和密钥，然后使用协商好的加密算法对数据进行加密传输 。SSL/TLS 协议还提供了身份认证功能，确保通信双方的身份真实性，防止中间人攻击。

访问控制技术在小米 AIoT 设备安全防护中也发挥着重要作用。小米采用了基于角色的访问控制（RBAC）模型和基于属性的访问控制（ABAC）模型相结合的方式，对用户和设备的访问权限进行严格管理 。在 RBAC 模型中，根据用户在系统中所扮演的角色来分配相应的访问权限。在小米智能家居系统中，管理员角色拥有对所有设备和数据的最高权限，可以进行设备配置、用户管理、系统设置等操作；普通用户角色则只能访问和控制自己授权的设备，如只能控制自家的智能家电、查看相关的设备状态和数据等 。

ABAC 模型则依据用户、资源和环境的属性来动态确定访问权限。在小米智能工厂的 AIoT 设备管理中，根据设备的生产状态、用户的工作区域和时间等属性来决定用户对设备的访问权限。在设备维护期间，只有维护人员在规定的时间内，且处于设备所在的工作区域时，才能访问设备进行维护操作；在正常生产期间，普通操作人员只能在自己的工作岗位上，按照规定的操作流程访问和控制相关设备 。通过这种灵活的访问控制方式，小米能够根据不同的场景和需求，实现对用户和设备访问权限的精准管理，有效防止非法访问和越权操作，保障 AIoT 设备的安全运行 。

# 5边缘计算仿真平台构建

## 5.1 开源框架选型与二次开发

本研究基于 EdgeX Foundry 开源边缘计算平台进行核心架构搭建。EdgeX Foundry 作为业界领先的开源边缘计算框架，提供了丰富的设备管理、数据处理和通信接口，具备强大的兼容性和可扩展性，能够便捷地集成各类边缘设备与应用。通过对其进行二次开发，可根据小米 AIoT 设备的特性和安全防护需求，定制化地实现设备状态监控、数据采集与处理以及安全策略执行等功能。例如，在设备管理模块中，可针对小米 AIoT 设备的通信协议和数据格式，优化设备接入流程，提高设备连接的稳定性和效率。

Mosquitto 作为轻量级的 MQTT 代理，在本平台中负责设备间的消息通信。MQTT 协议具有低带宽、低功耗和高可靠性的特点，特别适合物联网设备之间的通信。Mosquitto 能够高效地处理大量的 MQTT 消息，确保数据在边缘设备与平台之间的快速、稳定传输。通过配置 Mosquitto 的安全参数，如启用 TLS 加密、设置用户认证等，可进一步保障通信的安全性，防止数据在传输过程中被窃取或篡改。

ThingsBoard 用于构建可视化界面，为用户提供直观的设备状态监控、数据分析和安全事件管理等功能。它提供了丰富的仪表板模板和组件库，用户可以根据自己的需求快速搭建个性化的可视化界面。通过对 ThingsBoard 的二次开发，可将小米 AIoT 设备的特定安全指标和性能参数集成到可视化界面中，实现对设备安全状态的实时监控和分析。例如，在仪表板上展示设备的实时网络流量、安全事件报警信息以及设备的加密状态等，帮助用户及时发现和处理安全问题。

为了适配不同类型的边缘设备，本平台基于 GD32F470 系列 MCU 开发环境进行硬件适配。GD32F470 系列芯片具备高性能、低功耗和丰富的外设资源等优势，非常适合作为边缘计算设备的核心处理器。通过深度定制 NuttX 内核，为 GD32F470 系列芯片提供了稳定的操作系统支持，使其能够高效地运行各种边缘计算任务。定制后的 NuttX 内核支持 POSIX 接口，方便开发者使用标准的 POSIX 函数进行应用开发，提高了开发效率和代码的可移植性。同时，通过优化内核的任务调度算法和内存管理机制，进一步提升了系统的性能和稳定性，确保边缘设备能够在复杂的物联网环境中可靠运行。

## 5.2 系统模块设计

内核层是整个仿真平台的基础，负责提供任务调度、文件系统、TCP/IP 协议栈等基础功能。任务调度模块采用优先级调度算法，根据任务的优先级和时间片分配 CPU 资源，确保关键任务能够及时得到处理。文件系统模块支持多种文件系统格式，如 FAT32、EXT4 等，方便用户存储和管理数据。TCP/IP 协议栈模块实现了完整的网络通信功能，支持多种网络协议，如以太网、WiFi、蓝牙等，确保边缘设备能够与其他设备和系统进行稳定的网络通信。

内核层还支持 POSIX 接口，这使得开发者可以使用标准的 POSIX 函数进行应用开发，提高了开发效率和代码的可移植性。同时，内核层兼容多种硬件平台，特别是针对 GD32F470 系列芯片进行了优化，充分发挥了芯片的性能优势。通过对硬件中断处理、DMA（直接内存访问）控制等底层硬件资源的管理，内核层实现了高效的数据传输和处理，为上层应用提供了稳定的运行环境。

应用框架层集成了多媒体、传感器、蓝牙互联等场景化框架，为开发者快速搭建智能家居、穿戴设备等仿真模型提供了便利。在智能家居仿真模型中，集成了智能灯光控制、智能窗帘控制、智能家电控制等功能模块。开发者可以通过调用相应的框架接口，快速实现这些功能的开发，而无需从头开始编写底层驱动和通信协议。例如，在智能灯光控制模块中，开发者可以使用应用框架提供的灯光控制接口，轻松实现对灯光亮度、颜色的调节，以及定时开关等功能。

蓝牙互联框架则实现了蓝牙设备的连接、数据传输和管理等功能。通过该框架，开发者可以方便地将蓝牙智能设备集成到仿真模型中，实现设备之间的互联互通。在智能穿戴设备仿真模型中，利用蓝牙互联框架，可实现智能手环与手机之间的蓝牙通信，实时传输用户的健康数据，如心率、步数、睡眠监测等。

工具集包含嵌入式开发环境、仿真器及自动化测试框架，为开发者提供了全方位的开发支持。嵌入式开发环境提供了代码编辑、编译、调试等功能，支持多种编程语言，如 C、C++ 等。仿真器可以模拟边缘设备的运行环境，帮助开发者在开发阶段对应用进行测试和验证，减少实际硬件测试的成本和时间。自动化测试框架则支持设备逻辑验证与 CI/CD 流程，通过编写自动化测试脚本，实现对应用功能的自动测试，提高测试效率和准确性。

在 CI/CD 流程中，自动化测试框架可以在代码提交后自动触发测试，确保代码的质量和稳定性。如果测试通过，代码将自动部署到仿真平台或实际设备中，实现快速迭代和更新。Matlab 作为强大的数据可视化工具，被集成到工具集中，用于对采集到的数据进行分析和可视化展示。通过 Matlab 的绘图函数和数据分析工具，可将设备的运行数据、安全事件数据等以直观的图表形式展示出来，帮助开发者更好地理解和分析系统的运行状态，及时发现潜在的问题和风险。

## 5.3 可视化界面与数据库

可视化界面设计了多个功能模块，以满足对小米 AIoT 设备的全面监控和管理需求。设备状态监控模块实时展示边缘设备的运行状态，包括设备的在线 / 离线状态、CPU 使用率、内存使用率、电池电量等信息。通过直观的图形界面，用户可以一目了然地了解设备的运行情况，及时发现设备故障或异常。当设备的 CPU 使用率过高时，界面会以红色警示标识提醒用户，以便用户及时采取措施进行优化或排查问题。

流量分析模块对网络流量进行实时监测和分析，展示设备的上行 / 下行流量、流量趋势图等信息。通过对流量数据的分析，用户可以了解设备的网络使用情况，发现异常流量行为，如 DDoS 攻击的前兆。当检测到异常流量时，系统会自动发出警报，并提供详细的流量分析报告，帮助用户快速定位问题根源。

安全事件报警模块则实时捕捉安全事件，如入侵检测系统（IDS）触发的警报、设备认证失败等信息，并以弹窗、邮件、短信等方式及时通知用户。用户可以在该模块中查看安全事件的详细信息，包括事件发生的时间、类型、受影响的设备等，以便及时采取相应的处理措施。

在数据库选择方面，采用 TDEngine 作为存储平台。TDEngine 是一款高性能的时序数据库，专门针对时序数据的存储和查询进行了优化，非常适合存储物联网设备产生的大量时序数据。它采用列式存储以及索引、分区等技术，能够实现高速插入、高效存储和快速查询。在小米 AIoT 设备的应用场景中，TDEngine 可以高效地存储设备的运行状态数据、网络流量数据、安全事件数据等时序信息。通过合理的表结构设计和索引优化，能够快速查询到特定时间段内的设备数据，为数据分析和安全决策提供有力支持。例如，在查询设备的历史运行状态时，TDEngine 可以在短时间内返回大量的历史数据，帮助用户分析设备的运行趋势和潜在问题。

# 6小米 AIoT 设备安全防护效果评估与优化建议

## 6.1 安全防护效果评估指标与方法

为了评估小米AIoT设备的安全防护，需确定关键评估指标和有效方法。设备漏洞数量是重要标准，反映了设备的安全性。使用漏洞扫描工具定期检测小米AIoT设备漏洞，统计新发现漏洞和修复情况，评估安全性。例如，某智能音箱一个月内发现5个新漏洞，3个一周内修复，2个一个月后未修复，说明需加强漏洞管理。

数据泄露事件发生率也是关键指标之一。数据泄露会对用户的隐私和权益造成严重损害，直接影响用户对小米 AIoT 设备的信任度。通过收集和统计小米 AIoT 设备在一定时间段内发生的数据泄露事件数量，并与设备的总使用量或用户数量进行对比，计算出数据泄露事件发生率 。如果在某一年度，小米 AIoT 设备的总用户数量为 1000 万，而发生数据泄露事件的用户数量为 1000 人，那么数据泄露事件发生率为 0.01%。这一指标能够直观地反映出小米 AIoT 设备在数据安全保护方面的水平，发生率越低，说明数据安全防护效果越好 。

设备遭受攻击次数重要，可评估安全防护能力。分析网络安全日志、IDS和IPS记录，统计攻击次数和类型。例如，某地区小米智能家居设备一个月内遭受10次DDoS攻击和5次恶意软件入侵，分析攻击来源、手段及防护系统应对，评估防护措施有效性，为优化策略提供依据。

安全测试，特别是渗透测试，是评估小米 AIoT 设备安全性的有效方法。测试人员模拟黑客攻击，利用技术如 SQL 注入、XSS、缓冲区溢出等，对设备的多个方面进行测试。一旦发现漏洞，如通过 SQL 注入获取智能摄像头登录信息，就需立即修复和加强防护。

漏洞扫描也是安全测试的重要环节，利用专业的漏洞扫描工具，定期对小米 AIoT 设备进行扫描，检测设备中存在的已知漏洞，并生成详细的漏洞报告。这些报告包含漏洞的类型、严重程度、位置等信息，小米的安全团队可以根据报告中的信息，及时采取措施修复漏洞，提高设备的安全性 。

收集用户反馈是评估安全防护效果的关键。作为小米 AIoT 设备的直接使用者，用户能迅速识别安全问题。小米通过在线客服、用户论坛、调查问卷等渠道，鼓励用户报告安全问题和异常。例如，用户通过在线客服反映智能门锁异常自动解锁，小米公司调查后发现软件漏洞并发布更新修复。这种反馈机制有助于及时发现并改进安全防护措施。

为了全面、准确地评估基于边缘计算的小米 AIoT 设备安全防护模型的效果，本研究制定了一系列科学合理的评估指标与方法。在安全性指标方面，重点关注数据机密性、完整性和可用性。数据机密性通过评估加密算法的强度和密钥管理的安全性来衡量，采用加密破解实验，尝试使用各种破解手段对加密后的数据进行解密，记录破解成功率，以此评估加密算法抵抗攻击的能力。数据完整性则通过计算数据传输前后的哈希值，对比哈希值是否一致来判断数据在传输过程中是否被篡改。可用性指标主要通过检测设备在遭受攻击后的服务中断时间和恢复时间来评估，模拟不同类型的攻击场景，如 DDoS 攻击、恶意软件注入等，记录设备从遭受攻击到恢复正常服务的时间，以此衡量系统的可用性和抗攻击能力。

在性能指标方面，着重考量边缘计算设备的处理延迟、网络带宽占用和系统资源利用率。处理延迟通过测量数据在边缘设备上的处理时间来确定，使用高精度的时间测量工具，记录数据从输入到输出的时间差，多次测量取平均值以确保结果的准确性。网络带宽占用则通过监测设备在正常运行和遭受攻击时的网络流量，分析网络带宽的使用情况，评估安全防护措施对网络带宽的影响。系统资源利用率包括 CPU 使用率、内存使用率等，通过系统监控工具实时采集设备的资源使用数据，分析安全防护模型在运行过程中对系统资源的消耗情况，确保在资源受限的边缘计算环境下，安全防护模型不会对设备的正常运行造成过大的负担。

## 6.2 攻击场景模拟

1. QEMU 仿真：利用 QEMU 仿真技术，搭建了一个模拟的小米 AIoT 设备网络环境，以测试安全防护模型在不同攻击场景下的性能表现。在模拟中间人攻击场景时，通过 QEMU 仿真在设备通信链路中插入恶意节点，试图窃取和篡改传输的数据。在智能摄像头与手机 APP 的视频传输过程中，恶意节点拦截视频数据，尝试解密并修改视频内容，然后再将修改后的数据发送给手机 APP。通过监测 TLS 握手过程中的加密密钥交换和身份认证环节，以及数据传输过程中的加密和解密操作，测试 TLS 握手成功率及系统响应时间。结果显示，在遭受中间人攻击时，由于采用了 TLS/SSL+X.509 证书认证的端到端加密技术，系统能够有效地识别并阻止恶意节点的干扰，TLS 握手成功率保持在 98% 以上，系统响应时间仅增加了 5 - 10ms，几乎不影响用户的正常使用体验。

在模拟 DDoS 攻击场景时，使用 QEMU 仿真控制大量的傀儡机向目标设备发送海量的请求，模拟真实的 DDoS 攻击场景。通过调整攻击强度和持续时间，观察目标设备的网络连接状态、服务响应时间以及系统资源利用率等指标的变化。在高强度的 DDoS 攻击下，目标设备的网络带宽被迅速耗尽，传统防护设备的服务响应时间急剧增加，甚至出现服务中断的情况。而采用本研究提出的安全防护模型，通过流量清洗与边缘计算分流技术，能够有效地识别和过滤掉攻击流量，将合法流量引导至边缘设备进行处理，确保系统的正常运行。实验结果表明，在遭受 DDoS 攻击时，采用本安全防护模型的设备服务响应时间仅增加了 20 - 30ms，系统资源利用率保持在合理范围内，能够稳定地提供服务，保障了用户的正常使用。

2. 数据抓包：运用 Wireshark 和 MQTT.fx 等专业工具进行数据抓包分析，深入了解加密通信的完整性和安全性。使用 Wireshark 在模拟网络环境中捕获设备通信的数据包，通过设置过滤器，筛选出与 MQTT 通信相关的数据包进行分析。在 MQTT 通信过程中，对数据包的头部信息、消息内容以及加密字段进行详细解析，验证数据在传输过程中的加密效果和完整性。通过分析发现，采用 MQTT over TLS 加密通道后，数据包中的敏感信息如设备身份标识、控制指令等都被成功加密，无法被直接读取，有效保护了数据的机密性。

利用 MQTT.fx 工具对 MQTT 通信进行模拟和测试，进一步验证加密通信的可靠性。通过 MQTT.fx 向模拟设备发送不同类型的消息，包括订阅请求、发布消息等，同时使用 Wireshark 捕获通信数据包，对比发送和接收的消息内容，确保数据在传输过程中没有被篡改或丢失。在测试过程中，对加密密钥的管理和交换过程进行监控，验证密钥的安全性和有效性。实验结果表明，通过 TLS/SSL 加密通信和 X.509 证书认证，数据在传输过程中的完整性得到了有效保障，未出现数据丢失或篡改的情况，确保了通信的安全性和可靠性。

## 6.3 结果分析

1. 安全性指标：经过一系列的实验验证，本研究提出的安全防护模型在安全性指标上表现出色。在数据机密性方面，采用 TLS/SSL+X.509 证书认证的端到端加密技术，使得数据在传输和存储过程中的泄露率显著降低。通过模拟各种攻击场景，如中间人攻击、恶意软件注入等，对加密后的数据进行破解尝试，结果显示数据泄露率降低了 95% 以上，有效保护了用户的隐私和数据安全。在数据完整性方面，通过哈希值比对和数字签名技术，确保了数据在传输和处理过程中的完整性，未出现数据被篡改的情况。

在入侵检测方面，基于孤立森林算法构建的轻量级 IDS 能够准确地识别出异常流量和攻击行为。通过模拟多种攻击场景，如 DDoS 攻击、端口扫描等，对 IDS 的检测性能进行测试。实验结果表明，IDS 的检测准确率达到了 98% 以上，能够及时发现并报警潜在的安全威胁，为系统的安全运行提供了有力的保障。同时，通过设置合理的阈值和规则，有效降低了误报率，避免了因误报导致的资源浪费和管理成本增加。

2. 性能指标：在性能指标方面，边缘计算设备在处理数据时展现出了明显的优势。处理延迟是衡量系统性能的关键指标之一，实验数据显示，边缘计算设备在处理数据时的延迟小于 50ms，能够满足实时性要求较高的应用场景，如智能家居控制、智能健康监测等。与云端处理相比，云端处理延迟通常在 200ms 以上，边缘计算设备的低延迟特性使得系统能够快速响应用户的请求，提供更加流畅的使用体验。

在网络带宽占用方面，由于边缘计算设备在本地处理大部分数据，减少了数据传输到云端的需求，从而降低了网络带宽的占用。通过监测设备在正常运行和遭受攻击时的网络流量，发现采用边缘计算安全防护模型后，网络带宽占用降低了 30% - 50%，有效缓解了网络拥塞问题，提高了网络的稳定性和可靠性。在系统资源利用率方面，经过优化的安全防护模型在运行过程中对 CPU 和内存的占用保持在合理范围内，不会对设备的正常运行造成过大的负担，确保了设备在长时间运行过程中的稳定性和可靠性。

## 6.4 安全防护体系的优化建议

尽管本研究提出的基于边缘计算的小米 AIoT 设备安全防护模型在实验验证中取得了良好的效果，但为了进一步提升系统的安全性和性能，仍有一些优化建议值得考虑。在加密算法方面，随着量子计算技术的不断发展，传统的加密算法可能面临被破解的风险。因此，建议引入量子 - resistant 加密算法，如基于格密码的加密算法，以增强数据的安全性，确保在未来量子计算时代数据的机密性和完整性。

在入侵检测与防御方面，虽然基于孤立森林算法的轻量级 IDS 已经取得了较高的检测准确率，但面对日益复杂多变的攻击手段，仍需要不断优化和完善。建议结合深度学习算法，如卷积神经网络（CNN）和循环神经网络（RNN），对网络流量和设备行为进行更深入的分析和学习，提高对未知攻击模式的检测能力。同时，加强对入侵检测系统的实时更新和维护，及时获取最新的攻击特征和威胁情报，确保 IDS 能够及时有效地应对各种安全威胁。

在边缘计算设备的资源管理方面，为了进一步提高系统的性能和稳定性，可以采用资源虚拟化和动态分配技术。通过将边缘设备的计算、存储和网络资源进行虚拟化，实现资源的灵活分配和高效利用。根据设备的实时负载和任务需求，动态调整资源分配策略，确保关键任务能够获得足够的资源支持，提高系统的整体性能和响应速度。

在用户安全意识培养方面，用户的安全行为对于整个安全防护体系的有效性至关重要。建议小米加强对用户的安全宣传和培训，提高用户的安全意识和操作技能。通过发布安全指南、举办安全讲座等方式，向用户普及物联网设备的安全知识，如设置强密码、定期更新设备固件、避免连接不安全的网络等，引导用户养成良好的安全使用习惯，降低因用户误操作导致的安全风险。

# 7结论与展望

## 7.1 研究成果总结

本研究深入剖析了小米 AIoT 设备在边缘计算环境下的安全防护问题，通过对常见安全威胁的分类和分析，提出了一种创新的基于边缘计算的分层安全模型。该模型从通信层、数据层和应用层三个层面入手，实现了小米 AIoT 设备的端到端加密与动态防御。在通信层，采用 MQTT over TLS 加密通道与 OPC UA 协议规范数据格式，确保了数据传输的安全和规范；在数据层，应用差分隐私与区块链日志记录技术，保护了数据的隐私和完整性；在应用层，结合零信任架构与 LSTM 异常检测实现动态访问控制，有效防范了各种安全威胁。

为了验证安全防护模型的有效性，本研究构建了一个基于开源边缘计算平台的仿真平台。该平台基于 EdgeX Foundry、Mosquitto、ThingsBoard 和 GD32F470 系列 MCU 开发环境进行二次开发，具备强大的功能和良好的扩展性。通过对平台的系统模块设计，包括内核层、应用框架层和工具集，实现了对边缘计算设备的高效管理和监控。同时，设计了直观的可视化界面，结合 TDEngine 数据库进行数据存储和分析，方便用户实时了解边缘计算设备的状态、网络流量和安全事件等信息。

在实验验证阶段，通过模拟多种攻击场景，如中间人攻击、DDoS 攻击等，对安全防护模型和仿真平台进行了全面测试。实验结果表明，该安全防护模型能够显著提升小米 AIoT 设备的安全性，有效抵御各种安全威胁，同时在性能指标上也表现出色，能够满足实际应用的需求。本研究还提供了详细的开发文档及二次开发接口，为后续的研究和应用提供了有力的支持。

## 7.2 未来研究方向

随着 5G 网络的普及和应用，边缘计算将迎来更广阔的发展空间。未来研究可聚焦于结合 5G 网络的高速率、低延迟和大连接特性，进一步优化边缘节点的部署。通过深入研究 5G 网络与边缘计算的融合技术，实现边缘节点之间的高效协同，提高数据传输和处理的效率。在智能家居场景中，利用 5G 网络的低延迟特性，实现智能设备的实时控制和响应，提升用户体验。同时，通过优化边缘节点的部署，减少数据传输的距离和时间，降低网络拥塞和延迟，提高系统的整体性能。

未来研究还应探索 AI 驱动的自适应安全策略，以提升对未知攻击的防御能力。随着人工智能技术的不断发展，利用深度学习、机器学习等 AI 技术，对网络流量和设备行为进行实时监测和分析，能够及时发现潜在的安全威胁，并自动调整安全策略。基于深度学习的入侵检测模型，能够学习正常网络流量和设备行为的特征，当检测到异常行为时，及时发出警报并采取相应的防御措施。通过不断优化 AI 模型，提高其对未知攻击的识别和防御能力，为小米 AIoT 设备提供更加智能、高效的安全防护。

未来研究还可以考虑将区块链技术与边缘计算相结合，进一步增强数据的安全性和可信度。区块链的去中心化、不可篡改和可追溯特性，能够为小米 AIoT 设备的数据存储和传输提供更高的安全性保障。在数据存储方面，利用区块链的分布式账本技术，将数据存储在多个节点上，防止数据被篡改和丢失；在数据传输方面，通过区块链的智能合约技术，实现数据的安全共享和授权访问，确保数据的隐私和安全。

随着物联网技术的不断发展，新的安全威胁和攻击手段将不断涌现。未来研究需要持续关注物联网安全领域的最新动态，及时更新和完善安全防护模型和技术，以应对不断变化的安全挑战。加强对物联网安全标准和法规的研究，推动行业的规范化发展，为小米 AIoT 设备的安全应用提供更加坚实的保障。

# 8参考文献

1. 张博.工业物联网边缘侧隐私保护策略研究与设计[D].北方工业大学,2024.DOI:10.26926/d.cnki.gbfgu.2024.000103.
2. 杜超.Xiaomi Vela开源共建IoT操作系统生态[J].软件和集成电路,2024,(09):40-41.DOI:10.19609/j.cnki.cn10-1339/tn.2024.09.029.
3. 李雅迪.基于物联网边缘计算网关的智能家居系统的设计与实现[J].河南教育学院学报(自然科学版),2023,32(03):13-17.
4. 崔宝秋,宋文宽,王宝林,等.小米“手机×AIoT”安全隐私技术[J].武汉大学学报(理学版),2022,68(01):1-7.DOI:10.14188/j.1671-8836.2021.2000.
5. 高娃,陈睿.物联网技术在智能家居产品设计中的应用[J].家具,2021,42(06):13-17.DOI:10.16610/j.cnki.jiaju.2021.06.003.
6. 张侠丹.中国智能家居行业研究[J].未来与发展,2021,45(12):14-19.
7. 李然,杨宏.智能家居标准化现状与展望[J].中国标准化,2020,(07):56-62+66.
8. 王静.基于物联网的智能家居终端控制系统关键技术的研究[D].中国矿业大学,2021.DOI:10.27623/d.cnki.gzkyu.2021.003069.
9. 葛天雄.基于MQTT的通用物联网安全系统框架[D].浙江大学,2021.DOI:10.27461/d.cnki.gzjdx.2021.002505.
10. 苏振荣.一种支持边缘计算的智能物联网网关设计与实现[D].电子科技大学,2022.DOI:10.27005/d.cnki.gdzku.2022.000792.
11. 温木奇,温武少.边缘计算的安全挑战与解决方法综述[J].计算机系统应用,2024,33(11):38-47.DOI:10.15888/j.cnki.csa.009702.
12. 安星硕,曹桂兴,苗莉,等.智慧边缘计算安全综述[J].电信科学,2018,34(07):135-147.
13. 沈传年.边缘计算安全与隐私保护研究进展[J].网络安全与数据治理,2022,41(08):41-48.DOI:10.20044/j.csdg.2097-1788.2022.02.007.
14. 夏珺.面向复杂异质环境的AIoT系统可信关键技术研究[D].华东师范大学,2023.DOI:10.27149/d.cnki.ghdsu.2023.000403.
15. 吴吉义,李文娟,曹健,等.智能物联网AIoT研究综述[J].电信科学,2021,37(08):1-17.
16. 高微,陈新元,王榕国.智能物联网AIoT的概念及应用场景的研究[J].信息通信技术,2023,17(03):80-84.
17. Kang M W ,Moon Y S ,Park H J .An enhanced security framework for home appliances in smart home[J].Human-centric Computing and Information Sciences,2017,7(1):1-12.
18. [1]Waseem I ,Haider A ,Pan D , et al.ALAM: Anonymous Lightweight Authentication Mechanism for SDN-Enabled Smart Homes[J].IEEE INTERNET OF THINGS JOURNAL,2021,8(12):9622-9633.
19. Wazid M ,Das K A ,Odelu V , et al.Secure Remote User Authenticated Key Establishment Protocol for Smart Home Environment[J].IEEE Transactions on Dependable and Secure Computing,2020,17(2):391-406.
20. Sung, T., Tsai, P., Gaber, T., & Lee, C. (2021). Artificial Intelligence of Things (AIoT) technologies and applications. Wireless Communications and Mobile Computing, 2021, 9781271. <https://doi.org/10.1155/2021/9781271>
21. Dong B, Shi Q, Yang Y, et al. Technology evolution from self-powered sensors to AIoT enabled smart homes[J]. Nano Energy, 2021, 79: 105414.
22. Nadar A, Härri J. An ai-as-a-service platform for an artificial intelligence of things (aiot)[C]//2024 IEEE 99th Vehicular Technology Conference (VTC2024-Spring). IEEE, 2024: 1-7.
23. Mansouri Y, Babar M A. A review of edge computing: Features and resource virtualization[J]. Journal of Parallel and Distributed Computing, 2021, 150: 155-183.
24. Ranaweera P, Jurcut A D, Liyanage M. Survey on multi-access edge computing security and privacy[J]. IEEE Communications Surveys & Tutorials, 2021, 23(2): 1078-1124.
25. Carvalho G, Cabral B, Pereira V, et al. Edge computing: current trends, research challenges and future directions[J]. Computing, 2021, 103(5): 993-1023.
26. Sun X, Ansari N. EdgeIoT: Mobile edge computing for the Internet of Things[J]. IEEE Communications Magazine, 2016, 54(12): 22-29.

Hou K M, Diao X, Shi H, et al. Trends and challenges in AIoT/IIoT/IoT implementation[J]. Sensors, 2023, 23(11): 5074.

# 致 谢

在这漫长的学术探索旅程中，每一步都充满了挑战与未知，而我之所以能坚持走到现在，离不开许多人的支持与帮助，心中满是深深的感激。

我要把最诚挚的感谢献给我的导师。在着手研究基于边缘计算的小米AIoT设备安全防护这个课题时，我就像在错综复杂的迷宫里迷失了方向。边缘计算与小米AIoT设备安全防护所涉及的领域极为复杂，各种技术相互交织，概念纷繁复杂，我常常感到困惑和迷茫，不知该从何处突破。

导师您凭借着在多年积累的深厚专业知识，以及对学术前沿问题的独到见解，为我拨开重重迷雾。还记得我们初次探讨研究方向时，您耐心地听完我那些尚显稚嫩的想法，然后用您丰富的经验和敏锐的洞察力，为我指出了一条清晰的研究路径。在研究思路的形成过程中，您严格把关，每一个细节都不放过。您多次指出我研究思路中存在的漏洞和不足之处，引导我不断思考和改进。正是在您严谨的审视下，我的研究思路逐渐变得清晰、完善。

在技术细节方面，您的指导更是让我受益匪浅。当我在研究过程中遇到诸如边缘计算资源分配算法、AIoT设备通信加密技术等难题时，您总是能深入浅出地为我讲解相关知识，帮助我理解问题的本质。您对这些技术细节的深入剖析，让我不仅知其然，还知其所以然，为我解决实际问题提供了有力的理论支持。

我也要感谢我的家人和朋友们。在研究过程中，查阅大量的文献资料、编写复杂的代码以及处理繁琐的数据，占据了我绝大部分的时间和精力。在无数个日夜，我因为专注于研究，忽略了家庭中的许多事务。我没能像往常一样陪伴家人聊天、共度美好时光，也没能帮着分担一些家务。但家人从未对我有过任何抱怨，总是默默地承担起一切。

回顾这段探索之路，我收获的不仅仅是知识和研究成果，更是来自导师、朋友和家人的宝贵支持与关爱。在未来的学术道路上，我将带着这份感恩之心继续前行。网络安全领域不断发展，新的技术和挑战层出不穷，AIoT设备安全防护技术也需要持续创新和完善。我将秉持着对学术的热爱和对未知的探索精神，不断努力学习和研究，为推动AIoT设备安全防护技术的发展贡献自己的一份力量，不辜负导师的期望、朋友的支持和家人的关爱。