

智能家居运维服务平台设计

肖翔元, 肖 健, 胡 静, 李 行

天津大学智能与计算学部, 天津

收稿日期: 2024年11月1日; 录用日期: 2024年12月19日; 发布日期: 2024年12月31日

摘 要

针对物联网智能家居平台的运行维护挑战, 本文深入研究了网络系统、安全系统与应用接口服务的设计策略。在网络系统层面, 提出一套实时性、可靠性和安全性广域网方案。在安全系统方面, 提出了包含网络安全、主机安全、应用安全及数据安全在内的多层次防护体系, 全面提升了平台的安全性。在应用接口服务方面, 提出了一种便捷使用, 可快速开发的服务系统。通过结合以上三方面, 构建出一套完整、高效的智能家居运维服务平台架构。

关键词

智能家居, 维护服务, 网络系统, 安全系统

Design of Intelligent Home Maintenance Service Platform

Xiangyuan Xiao, Jian Xiao, Jing Hu, Hang Li

College of Intelligence and Computing, Tianjin University, Tianjin

Received: Nov. 1st, 2024; accepted: Dec. 19th, 2024; published: Dec. 31st, 2024

Abstract

Aimed at the operation and maintenance challenges of the IoT smart home platform, this paper conducts an in-depth study of the design strategies of the network system, security system, and application interface service. At the network system level, a real-time, reliable, and secure wide area network solution is proposed. Regarding the security system, a multi-level protection system encompassing network security, host security, application security, and data security is put forward, comprehensively enhancing the security of the platform. In the aspect of application interface service, a service system that is convenient to use and enables rapid development is proposed. By integrating the above three aspects, a complete and efficient intelligent home operation and maintenance service platform architecture is constructed.

Keywords

Smart Home, Maintenance Services, Network Systems, Security System

Copyright © 2024 by author(s) and Hans Publishers Inc.

This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

<http://creativecommons.org/licenses/by/4.0/>



Open Access

1. 引言

传统的家居建设缺乏智能互联的功能，各个家居设备之间无法进行有效的通信和协作。用户需要手动操作每个设备，无法实现自动化控制和智能化管理。物联网智能家居平台具有以下优势：一方面，智能家居平台采用模块化设计，当某个设备出现故障时，通常不会影响到其他设备的正常运行。这种故障隔离机制保证了智能家居平台的稳定性和可靠性。另一方面，智能家居平台通过统一的系统或应用程序，将家中的各种智能设备连接起来，实现集中控制，降低了管理的难度。

智能家居平台是一个集成了物联网、云计算、大数据、人工智能等先进技术的综合性系统。该平台通过物联网技术将家庭中的各种智能设备和传感器连接起来，形成一个智能网络。这些设备包括但不限于智能灯光、恒温器、安防系统、家电控制等，它们能够相互通信、交换信息，并通过云端平台进行集中管理和控制。其核心在于其能够实现设备的互联互通、数据的实时采集与分析，以及基于人工智能的自动化决策与控制[1]。通过该平台，用户可以远程监控和控制家中的设备，实现家庭环境的智能化调节和管理，从而提升生活的便捷性、舒适度和安全性。

2. 总体框架设计

物联网智能家居平台比传统智能家居模型更加高效、便捷、实用，在系统维护、升级和管理等方面有较大优势[2]。物联网智能家居平台总体框架的设计不仅影响智能家居平台的当前功能和性能，还关系到其未来的可扩展性和长期维护。因此，精心设计总体框架是确保智能家居平台成功和可持续发展的关键。良好的平台设计方案应当满足一些特定的需求。首先，一个好的总体框架确保系统能够稳定运行，减少故障和错误。合理的架构设计有助于识别和解决潜在的系统瓶颈，设计时需要考虑系统的容错能力，以保证在某些组件发生故障时，平台仍能正常运行。其次，智能家居系统通常需要处理大量数据，包括传感器数据和用户请求，优化总体框架可以提高数据处理效率，确保系统响应迅速。通过合理的架构设计，可以有效地管理系统资源，如计算能力和存储空间，避免资源浪费[3]。同时，良好的框架设计通常采用模块化的方法，使得系统能够方便地添加新功能或支持新设备，而无需大规模重构。设计时需要考虑平台的兼容性，以便与各种智能设备和技术标准对接，满足不断变化的市场需求[4]。用户体验也是总体框架设计的重要考虑因素。用户界面的设计直接影响用户如何与平台互动，一个直观和易用的界面可以提升用户满意度。安全性和隐私保护在智能家居平台设计中显得愈发重要，框架设计中需要包含数据加密和访问控制机制，以保护用户数据不被未经授权访问。同时设计时要遵守隐私法规，确保用户数据的合法和透明处理。最后，一个好的总体框架设计有助于简化系统的维护和管理，减少维护成本，设计时应包含监控和日志功能，以便快速定位和解决问题[5]。

本文探讨了智能家居产品链服务平台在网络系统设计、安全系统设计及主机应用安全三方面的构建。在网络设计方面，强调通讯网络的重要性，确保通讯的实时、可靠、安全和可扩展。安全系统设计方面，

构建了全面的防护体系,进一步增强平台安全性。同时,强化主机和应用的安全管理,保障系统和数据的机密性、完整性和可用性。

2.1. 网络系统

通讯网络是整个智能家居产品链服务平台服务系统的关键部分,通过它可以把分布在不同地理位置的各种系统连接起来,最有效地利用各种资源,保证整个系统高效、可靠地运行完成各种关键业务处理工作。智能家居产品链服务平台的通讯网络设计以用户需求为核心,注重安全性、实时性、可靠性和可扩展性[6]。网络采用快速交换式以太网和 DDN 专线,确保高效传输和稳定性。系统支持多数据中心和云端部署,利用云服务的弹性计算和安全特性,实现数据资产的存储与备份。网络管理采用 IBM Nways Workgroup Manager,实现设备的全面监控和维护,降低成本并提高效率。整体设计兼顾技术先进性与标准化,保障网络的开放性、灵活性和互连性。

网络设计的出发点是用户的需求有以下的设计目标:性能目标,实时性,成熟性、先进性,可靠性、安全性,可扩充性、灵活性。为了达到这些设计目标根据以往的经验我们提出以下设计原则:

用户的实际和潜在需求:对于智能家居产品链服务平台来说内部专用网最重要的是安全性和实时性,而外部公务网要求是可靠性和较高的传输带宽[7]。除此之外还考虑了用户将来的潜在需求如网络规模扩大的需求、网络技术升级的需求、多厂家网络设备互连的需求等。

不同厂家设备的互连性:开放系统的好处之一就是具有好的互连性。不同的网络厂家在产品和技术上都有着一些不同的优势,因此一个网络系统由不同厂家设备组成是完全有可能的。所以网络设备的选择要考虑其互连性。

网络的可伸缩和易管理性:网络的规模和应用不断扩大网络的设计要充分考虑其可伸缩性,一方面是网络结构的灵活性、易扩展性,另一方面是网络技术的升级性。

2.2. 安全系统

网络体系结构安全性是指在规划和配置网络信息系统期间根据特定安全要求部署其他安全设备。其他安全机制通过安全设置,安全部署,规划和设计来实现网络架构。在信息系统建设计划的初始阶段,应当适当选择网络设备,根据服务系统的实际需要,确定设备的基本技术参数,满足建设目标,网络设备服务的处理能力必须满足最大的业务需求。

首先,明确网络安全防护策略,规划、部署网络数据流检测和控制的安全设备,具体可根据需要部署入侵监测/防御系统、网络防病毒系统、抗 DDoS 系统等。其次,还应部署网络安全审计系统,制定网络和系统审计安全策略,具体措施包括设置操作系统日志及审计措施、设计应用程序日志及审计措施等[8]。为了允许远程用户安全地访问网络,可以设计远程安全访问系统来规划网络远程访问的安全性,并部署 IPSec 和 SSLVPN 等安全通信设备。

其次,为确保系统的可用性,应当设计网络线路和网络重要设备冗余措施,采用不同电信运营商的通信线路,相互备份确保网络畅通,制定网络系统和数据的备份策略,具体措施包括设计网络冗余线路、部署网络冗余路由和交换设备、部署负载均衡系统、部署系统和数据备份等。

网络体系结构安全性设计着重于从规划阶段开始,综合考虑安全设备部署、安全策略制定和网络架构规划,以确保信息系统的安全性[9]。关键措施包括合理选择网络设备、划分安全区域、规划 IP 地址和设计冗余措施。同时,网络安全设计采用防火墙、入侵检测和 VPN 等技术,严格控制信息出入口,监控网络运行状况,防止黑客入侵和病毒传播。此外,还需定期使用漏洞扫描工具,加强数据备份和访问控制管理,确保数据的安全性和完整性。

2.3. 应用终端与开放接口

应用终端系统是智能家居产品链服务平台和外部用户交互的重要渠道，应该充分体现产品交互的友好型同时兼顾系统的权威性。终端系统作为传感器，负责上传下载数据及响应用户需求。尤其在前后端分离的趋势下，前端获取页面模板和接口数据，完成渲染，与用户交互，智能家居产品链服务平台各终端系统实行前后端分离的开发模式。未来适应当下用户的产品使用情况以及智能家居产品链服务平台的用户群体，智能家居产品链服务平台的终端系统重点在传统的 PC 端以及移动小程序端。

开放平台是指软件系统通过公开其应用程序编程接口(API)或函数(function)来使外部的程序可以增加该软件系统的功能或使用该软件系统的资源，而不需要更改该软件系统的源代码。在智能家居产品链服务平台中，开放平台作为智能家居产品链服务平台的一个重要组成部分，基于智能家居产品链服务平台的服务中台封装成一系列计算机易识别的数据接口开放出去，供第三方开发者使用。有效地加速了智能家居产品链服务平台整体数据以及模型业务输出的能力和效率。

3. 平台详细设计

3.1. 网络系统详细设计

智能家居产品链服务平台服务系统网络是一个多级网络系统，该网络系统的网络中心采用以太网交换机下联各部数据中心。路由器的广域网端口通过专线并采用 PSTN 备份与省政府网络中心相连通过 PSTN 或 DDN，实现与各区政府的广域网连接。外部公务网采用电信局的虚拟主机方式，通过 DDN 专线及 PSTN 备份方式连入互联网，实现基于互联网上的访问阅读和下载。为了确保安全保密，两网在物理上是完全自成体系的，涉及两网的数据交换，由网络中心统一管理实施。必要时可在两套网络之间增加防火墙。建议在第二阶段网络建设完成后，在行署中心配备网管系统。

3.1.1. 网络的升级

在广域网方面，限于国内现有的通讯线路采用的仍然是路由器方式。将来随着网络线路的改良技术的发展，在广域网方面也可以采用交换式技术，建立传输速率更高的多媒体网络，从而提高广域网络的功能及性能，建立包括远程部门系统在内的广泛的虚拟网络。

3.1.2. 网络拓扑

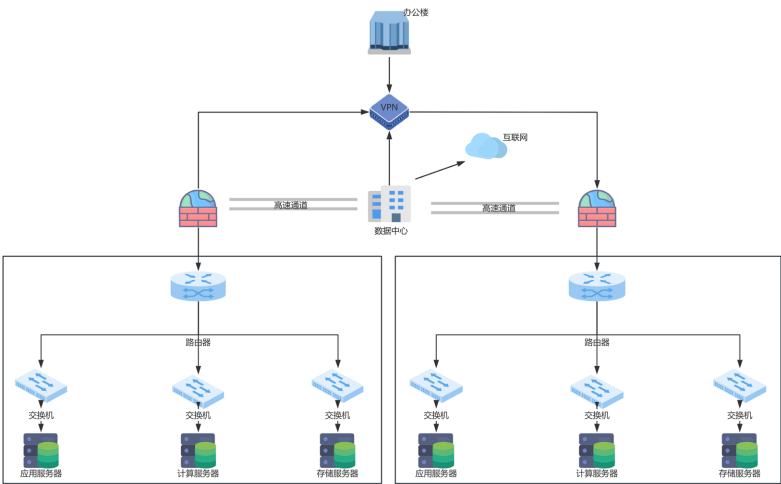


Figure 1. Network topology structure
图 1. 网络拓扑结构图

智能家居产品链服务平台系统采用多数据中心 + 云端的网络部署方式,网络拓扑结构如图 1 所示,同时结合当前各大云服务商的优势,充分引入云服务特性,构建成混合云部署。云端充分采用弹性计算特征以及防攻击特性,重点部署应用服务以及外网用户接入,自建数据中心存储重要数据资产同时构建多数据中心互相备份,确保重要数据资产不丢失。

3.2. 安全系统详细设计

智能家居安全体系旨在通过设计恰当的安全措施,确保合理部署网络设备,结合安全技术手段,确保智能家居系统的网络架构安全、数据传输安全及用户隐私保护,实现全面的安全防护和高效的管理策略,从而保障智能家居环境的稳定运行和用户信息的安全[10]。本次设计的智能家居安全系统包括网络安全、主机安全和数据安全三个方面。

3.2.1. 网络安全

网络安全是指对网络中所有的设备进行检测、分析和评估,发现并报告系统内存在的弱点和漏洞,评估安全风险,建议补救措施,并有效地防止黑客入侵和病毒扩散,监控整个网络的运行状况[11]。网络安全系统分为生产环境与试验环境两个部分,利用软件隔离。生产环境包括高性能的服务器、存储设备、网络设备和安全设备等,负责处理日常的业务交易、数据存取和客户服务等关键任务。实验环境是一个模拟的生产环境,用于测试新的应用程序、安全补丁、配置更改等。实验环境需要适当的安全措施来防止未经授权的访问和数据泄露,对于安全性的要求低于生产环境。针对生产环境,我们制定如下入侵检测方案,如图 2 所示。

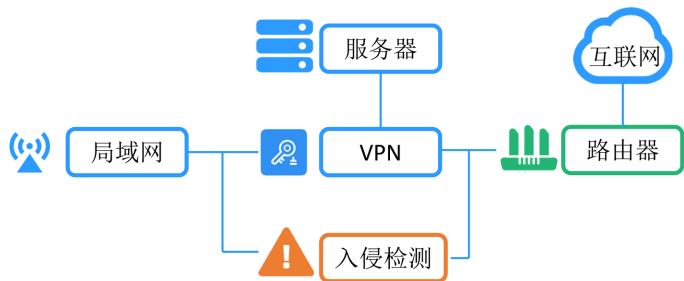


Figure 2. Intrusion detection scheme frame diagram
图 2. 入侵检测方案框架图

防火墙:采用了一台服务器作为双重防火墙,将 Internet 与内部网络分隔开。这道防火墙对进入网络的数据进行了严格的筛选,只允许特定的、必要的服务如网页浏览、文件传输等通过,并阻止了外部非法访问。同时,需要定期对防火墙的访问记录进行检查,并对防火墙的管理权限进行了严格限制,以确保系统的安全稳定运行。

VPN 系统:考虑到内部设备与用户外部通信需求,我们部署了 VPN 系统,该系统在公网上构建加密隧道,利用加密、认证、封装及密钥交换技术,确保合法用户安全访问企业私有数据。此方案不仅替代了传统专线,还实现了移动用户与远程 LAN 的安全连接,同时支持对整个 VPN 网络的安全策略进行集中管理和配置,为内部通信提供了全面安全保障。

防病毒软件:采用网络防病毒软件,构建机房全方位防毒体系,覆盖所有服务器与计算机。网络中心设立病毒防护中心,统一管理局域网设备,制定防毒策略,自动扫描查杀病毒。此系统集中监控病毒入侵、防护状态及软件运作,便于集中管理、设置与维护,及时报警病毒爆发,汇总分析日志信息。针对新病毒,迅速部署补丁与工具,有效预防,确保安全无虞。

3.2.2. 主机安全

智能家主机安全是指保护连接到网络的计算机或其他设备免受未经授权的访问、恶意软件的攻击和其他安全威胁的保障措施。主机安全是网络安全的基础，对于维护整个网络系统的稳定和安全至关重要[12]。

BIOS 安全：BIOS 作为主机最基础的安全防护之一，扮演着至关重要的角色。

其关键在于设置密码和配置启动顺序，从而有效地加固系统的物理与逻辑访问控制。首先必须为 BIOS 设置一个足够复杂的密码，以抵抗可能的暴力破解尝试。除了设置密码外，调整 BIOS 的启动顺序同样重要。U 盘作为一种常用的数据传输介质，同时也成为了恶意攻击者植入病毒或木马的首选途径。因此，禁止从 U 盘启动可以有效阻断这类威胁，减少系统被非法侵入的风险。

默认账号管理：Linux 开源系统广泛用于网络系统中，通常会预装一些默认的账号。然而，这些默认账号中的很多，在实际部署和运行环境中可能并不需要，甚至可能成为潜在的安全风险点。因此，强烈推荐禁止或删除所有那些被操作系统本身启动但并不需要的默认账号。

端口与服务：在规划网络架构时，管理员应当详细审查所有网络设备和服务器上运行的服务及其对应的端口。利用安全扫描工具定期对网络环境进行全面扫描，以发现未授权的服务和开放的端口。其次，应根据扫描结果制定相应的禁用计划，并在维护窗口内执行禁用操作。同时，还应更新防火墙和安全组规则，以阻止外部流量访问这些被禁用的服务和端口。

3.2.3. 数据安全

多用户、高可靠性需求、频繁更新与大文件处理，显著增加了数据库构建与维护的复杂度，同时也暴露了潜在的安全隐患，让攻击者能利用隐蔽漏洞进行非法侵入。因此，深入探讨并优化网络数据库的安全设计与实现至关重要，旨在为用户筑起坚实的技术防线[13]。此系统以认证服务器为核心，分层架构各司其职，贯穿其中的是角色导向的数据库访问控制，辅以精细的安全策略与组件，确保访问机制严密可控。表示层作为用户交互窗口，数据访问层负责认证、加密等核心逻辑，而数据层则专注于数据存储、封装与高效调用的实现。

系统表示层：网络数据库安全访问系统的表示层作为前端交互界面，负责用户登录信息的接收、初步验证及提交。它通过窗体展示用户信息，包括用户名、角色等，并处理用户登录请求。用户需通过身份验证后方可登录，系统据此分配角色并创建 Cookie 存储角色信息以避免重复验证。登录后，用户基于分配的角色访问不同界面进行数据库操作。系统还采取防范措施对抗 SQL 注入攻击，通过参数集确保用户输入被安全处理，并在出现异常时隐藏 SQL 错误信息，仅向用户提供友好提示，以保护系统安全。

系统数据访问层：数据访问涉及加密解密、认证与授权。系统加密连接字符串、用户密码及用户输入信息，通过加密方法加密并传递至后端服务器。后端采用哈希算法结合随机数填充进行加密处理。权限撤销由管理员执行，通过调用存储过程删除角色对应的操作权限及认证数据库中的相关记录。

数据层：数据备份和数据恢复的设计决定关键业务数据的安全性与可恢复性。

备份架构图如图 3 所示。备份策略包括本机和特定服务器备份。本机可以利用热插拔硬盘进行定期的备份文件复制，并设定备份文件的存储周期以管理存储空间，结合全备份、增量备份及跟踪备份等多种模式，以最大化备份效率与数据完整性。对于如 WEB、邮件、FTP 及防病毒等特定服务器，系统还规定了需手动导出的重要资料类别，并通过相应工具自动完成备份过程。

在数据恢复方面，当主数据服务器遭遇数据损坏时，系统支持从最近的备份记录中恢复数据至原服务器。若数据服务器本身也受损，则可通过备份服务器中的数据进行恢复。此外，系统还采用了硬盘作为备份介质，以应对数据服务器与备份服务器同时损毁的极端情况，确保数据的最终可恢复性。

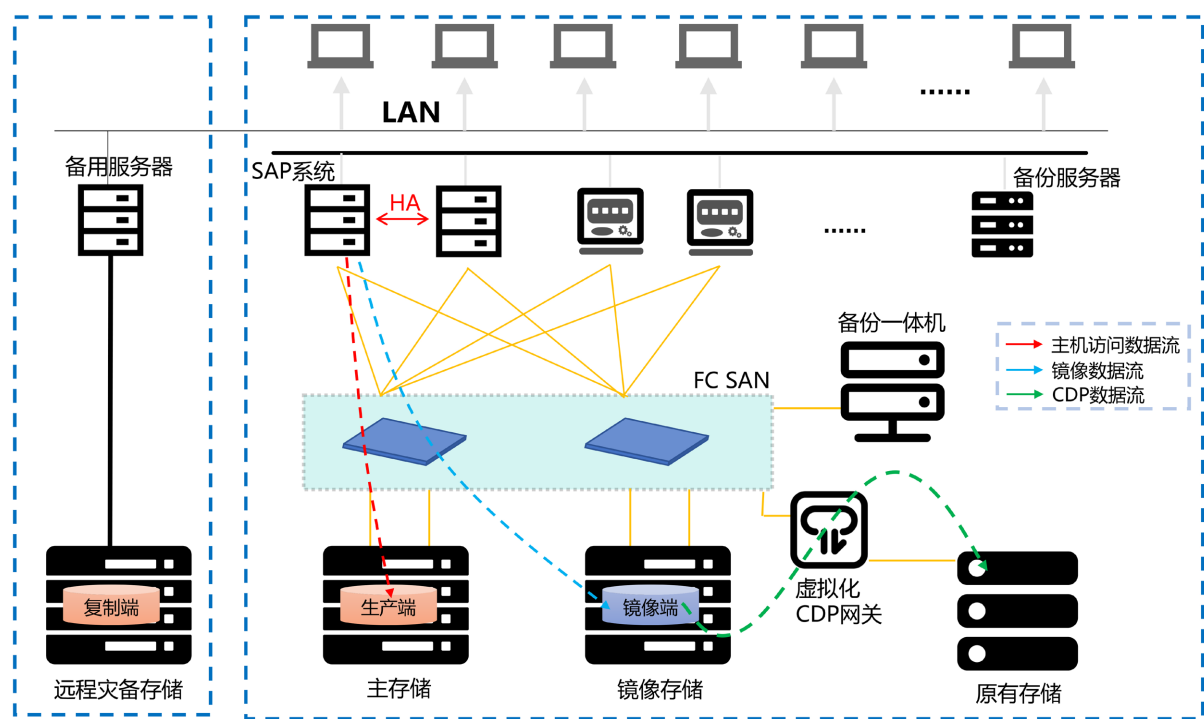


Figure 3. Backup architecture diagram
图 3. 备份架构图

3.3. 应用终端与开放接口详细设计

3.3.1. 应用终端系统设计

智能家居产品链服务平台精心构建了应用终端系统，旨在成为用户与平台间高效、友好的交互桥梁。该系统不仅强调用户界面的友好性，还兼顾了系统的权威性和稳定性。通过前后端分离的开发模式，前端负责页面渲染与用户互动，后端则专注于数据处理，确保数据传输的高效与安全。针对用户习惯，平台重点发展 PC 端 WEB 门户与移动小程序端，PC 端以数据可视化为核心，优化用户体验；而移动小程序端则利用微信的高普及率，快速响应用户需求，提供便捷的服务体验。

3.3.2. 开放平台设计

智能家居产品链服务平台开放平台，作为连接平台与第三方开发者的桥梁，通过开放 API 接口，促进资源共享与功能拓展。该平台基于服务中台的数据封装，为开发者提供了一系列标准化的数据接口，加速了智能家居产品的创新与迭代。开放平台内置的服务接入网关，是核心功能之一，它负责处理外部系统的服务请求，通过严格的限流、熔断机制，保障系统稳定运行；同时，实施服务计费与访问安全控制，确保平台的经济性与安全性。此外，平台支持分布式扩展，以应对大并发场景下的挑战，为智能家居产品的未来发展奠定坚实基础。

4. 总结

本文深入探讨了物联网智能家居平台的运维服务，从网络系统、安全系统与终端应用和接口三个方面进行了讨论与设计预想。网络系统设计基于快速交换式以太网和 DDN 专线，确保了通讯的实时性、可靠性和安全性。安全系统则实施了包括网络安全、主机安全、应用安全及数据安全在内的多层次防护体系，通过防火墙、入侵检测系统、虚拟专用网络系统及公开密钥身份认证等手段，全面提升了平台的安全

全性。在应用终端与开放接口的设计, 强调了前后端分离模式的重要性, 并介绍了开放平台的 API 接口设计, 以及如何通过服务接入网关实现服务请求的处理和安全控制。总体而言, 本文提供了一个全面的视角, 展示了如何通过精心设计的网络和安全系统, 以及用户友好的终端系统, 来提升智能家居平台的性能和用户体验。

基金项目

本研究由国家重点研发计划项目资助, 项目编号 2021YFF0901200。

参考文献

- [1] 王一炜, 郑仁思, 宋嘉欣. 物联网趋势下的智能家居产品设计策略[J]. 轻纺工业与技术, 2021, 50(9): 103-104.
- [2] 郭涛, 韩建亭, 杨晓玲. 智能家居管理系统分析与技术架构[J]. 电信科学, 2015, 31(11): 110-115.
- [3] Guo, T., Han, J.T. and Yang, X.L. (2015) Architecture and Key Capabilities of Management System of Smart Home. *Telecommunications Science*, **31**, 110-115.
- [4] 严萍, 张兴敢, 柏业超, 杜仲林. 基于物联网技术的智能家居系统[J]. 南京大学学报(自然科学版), 2012, 48(1): 26-32.
- [5] Yan, P., Zhang, X.G., Bai, Y.-C. and Du, Z.L. (2012) Smart Home Based on Internet of Things. *Journal of Nanjing University (Natural Sciences)*, **48**, 26-32.
- [6] 朱峰. 基于智能家居环境下信息监测系统的设计开发[J]. 电子通信与计算机科学, 2022, 4(3): 121-122.
- [7] 秦浩, 刘凌旗, 栾添, 等. 2021 年世界网信前沿技术领域发展综述[J]. 中国电子科学研究院学报, 2022, 17(4): 354-361.
- [8] 蒋志伟, 王伟, 刘姗, 等. 基于 ARM 的智能家居系统的设计与实现[J]. 现代电子技术, 2023, 46(4): 177-181.
- [9] 苗志强. 物联网智能家居家庭网关系统设计与实现[D]: [硕士学位论文]. 西安: 长安大学, 2015.
- [10] 何文丰. 一种多层结构型智能家居系统的设计与实现[D]: [硕士学位论文]. 厦门: 厦门大学, 2023.
- [11] Ma, G., Chen, L., Wang, Y., Fan, J., Liu, J. and Tian, L. (2023) Design and Implementation of Smart Home System Based on STM32 Microcomputer. *International Journal of Advanced Network, Monitoring and Controls*, **8**, 11-19. <https://doi.org/10.2478/ijanmc-2023-0072>
- [12] 姚金山. 智能家居系统的设计与实现[D]: [硕士学位论文]. 哈尔滨: 哈尔滨理工大学, 2017.
- [13] 刘兵. 智能家居系统互联互通的设计与实现[D]: [硕士学位论文]. 北京: 北京邮电大学, 2013.