aurum
Revista Multidisciplinar

ISSN: 3085-7783

ANÁLISE DE VULNERABILIDADES EM CASAS INTELIGENTES: PROPOSTA DO MODELO DE SEGURANÇA IOT RESIDENCIAL EM CAMADAS (MSIOT-RC)

VULNERABILITY ANALYSIS IN SMART HOMES: PROPOSAL FOR A LAYERED RESIDENTIAL IOT SECURITY MODEL (MSIOT-RC)

https://doi.org/10.63330/armv2n7-002

Submetido em: 09/07/2026 e Publicado em: 16/07/2026

ARM: e261930

Júlia Afonso Isaac
Mestre em Engenharia Informática – Especialidade em Gestão de Redes de Computadores e Sistemas de Comunicação
E-mail: juliamakete@gmail.com
ORCID: https://orcid.org/0009-0007-1000-8531

Resumo

Este trabalho apresenta uma análise aprofundada das vulnerabilidades de segurança presentes em sistemas de casas inteligentes baseados na Internet das Coisas (IoT). A pesquisa fundamenta-se na crescente adoção de tecnologias residenciais conectadas e nos riscos cibernéticos associados à exposição de dados sensíveis de rotina, hábitos e comportamentos dos utilizadores. Com base em revisão sistemática da literatura e em testes práticos de penetração, foi desenvolvido um protótipo funcional de casa inteligente utilizando a plataforma ESP32, integrando sensores, atuadores e um aplicativo de controle. As vulnerabilidades foram identificadas por meio de ferramentas especializadas Nmap, Wireshark, Aircrack-ng, hping3 e Bandit — abrangendo as camadas de aplicação, rede e hardware. Como contribuição original, propõe-se o Modelo de Segurança IoT Residencial em Camadas (MSIoT-RC), uma arquitetura de proteção multidimensional que integra autenticação reforçada com bcrypt, tokens temporários com HMAC-SHA256, isolamento de rede e fortalecimento físico. Os resultados demonstram elevação significativa do nível de segurança em todas as dimensões analisadas, validando a eficácia das medidas propostas.

Palavras-chave: Casa Inteligente; ESP32; Internet das Coisas; Segurança da Informação; Vulnerabilidades.

Abstract

This paper presents an in-depth analysis of security vulnerabilities in smart home systems based on the Internet of Things (IoT). The research is grounded in the growing adoption of connected residential technologies and the cyber risks associated with exposing sensitive routine, habit, and behavior data. Based

on a systematic literature review and practical penetration testing, a functional smart home prototype was developed using the ESP32 platform, integrating sensors, actuators, and a control application. Vulnerabilities were identified using specialized tools — Nmap, Wireshark, Aircrack-ng, hping3, and Bandit covering application, network, and hardware layers. As an original contribution, the IoT Residential Security Layered Model (MSIoT-RC) is proposed, a multidimensional protection architecture that integrates enhanced authentication with bcrypt, temporary tokens with HMAC-SHA256, network isolation, and physical hardening. Results demonstrate a significant increase in security levels across all analyzed dimensions, validating the effectiveness of the proposed measures.

Keywords: ESP32; Information Security; Internet of Things; Smart Home; Vulnerabilities.

1 INTRODUÇÃO

A quarta revolução industrial, caracterizada pela convergência entre tecnologias digitais, físicas e biológicas, tem redefinido a forma como os seres humanos interagem com o ambiente construído. Nesse contexto, a Internet das Coisas (IoT[1]) emerge como um dos pilares estruturais dessa transformação, conectando objetos do cotidiano à infraestrutura global de comunicações e possibilitando níveis sem precedentes de automação, monitoramento e controle remoto. Conforme dados da Statista (2024), estima-se que existam mais de 15 bilhões de dispositivos IoT ativos mundialmente, com projeção de crescimento para 29 bilhões até 2030.

Dentre as aplicações mais promissoras da IoT, as casas inteligentes (smart homes) destacam-se como um segmento de alta adesão popular, oferecendo conveniência, eficiência energética e segurança residencial. No entanto, a expansão acelerada dessas tecnologias não tem sido acompanhada por padrões robustos de segurança cibernética, tornando os dispositivos residenciais alvos privilegiados para agentes mal-intencionados.

A presente pesquisa fundamenta-se na hipótese de que a maioria dos sistemas de casas inteligentes disponíveis no mercado consumidor apresenta vulnerabilidades críticas em múltiplas camadas aplicação, rede e hardware que podem ser exploradas por atacantes com diferentes níveis de sofisticação. Para testar essa hipótese, desenvolveu-se um protótipo funcional de casa inteligente baseado na plataforma ESP32[2], submetendo-o a uma bateria de testes de penetração com ferramentas reconhecidas internacionalmente.

Como principal contribuição original, este trabalho propõe o Modelo de Segurança IoT Residencial em Camadas (MSIoT-RC[3]), uma arquitetura conceitual e prática de proteção multidimensional que integra

1 Internet das Coisas (Internet of Things)
2 Espressif Systems 32 microcontrolador com Wi-Fi e Bluetooth integrados
3 Modelo de Segurança Internet das Coisas Residencial em Camadas

mecanismos de defesa em cinco níveis hierárquicos: perímetro físico, rede e comunicação, dispositivo embarcado, aplicação e gestão de políticas de segurança. O modelo foi validado experimentalmente, demonstrando elevação substancial do nível de maturidade de segurança do protótipo analisado.

O artigo está estruturado da seguinte forma: a Seção 2 apresenta a revisão da literatura; a Seção 3 descreve os materiais e métodos; a Seção 4 expõe os resultados dos testes; a Seção 5 detalha o modelo MSIoT-RC proposto; a Seção 6 discute as implicações dos achados; e a Seção 7 sintetiza as conclusões e sugestões para trabalhos futuros.

2 REVISÃO DA LITERATURA

2.1 INTERNET DAS COISAS (IOT)

A Internet das Coisas (Internet of Things IoT) constitui uma extensão paradigmática da Internet tradicional, caracterizada pela interconexão de objetos físicos dotados de capacidade computacional, sensores e atuadores que lhes permitem coletar, processar e trocar dados através de redes de comunicação. Conforme Atzori, Iera e Morabito (2010), a IoT representa a convergência de três visões complementares: a orientada a objetos (identificação e rastreamento), a orientada a Internet (conectividade e serviços) e a semântica (interoperabilidade e processamento inteligente de dados).

A arquitetura funcional da IoT pode ser decomposta em três estratos interdependentes: (i) a camada de percepção, responsável pela captura de dados do ambiente físico através de sensores e identificadores; (ii) a camada de rede, que viabiliza a transmissão dos dados coletados mediante protocolos de comunicação; e (iii) a camada de aplicação, onde os dados processados geram valor através de interfaces, serviços e atuadores (Xu, He e Li, 2014).

A aplicação da IoT transcende fronteiras setoriais, abrangendo transportes inteligentes, agricultura de precisão, saúde conectada, cidades inteligentes e automação residencial. Segundo o World Economic Forum (2023), o impacto econômico estimado da IoT deve ultrapassar US$ 14 trilhões na economia global até 2030, evidenciando a relevância estratégica dessa tecnologia.

2.2 CASAS INTELIGENTES

O conceito de casa inteligente (smart home) remonta às visões futuristas do final do século XX, mas sua materialização em escala comercial ocorreu nas últimas duas décadas, impulsionada pela miniaturização de componentes eletrônicos, pela popularização de redes sem fio de alta velocidade e pela proliferação de assistentes virtuais. Uma casa inteligente pode ser definida como uma residência equipada com dispositivos computacionais e tecnologias de informação que antecipam e respondem às necessidades dos ocupantes, promovendo conforto, conveniência, segurança e entretenimento (Harper, 2003).

O ecossistema de uma casa inteligente tipicamente compreende: (a) sensores (temperatura, umidade, movimento, luminosidade); (b) atuadores (lâmpadas, fechaduras, termostatos, motores); (c) controladores centrais (hubs, microcontroladores como ESP32 e Raspberry Pi); e (d) interfaces de usuário (aplicativos móveis, painéis táteis, comandos de voz). A integração desses componentes viabiliza cenários como iluminação adaptativa, controle climático automatizado, vigilância residencial remota e gestão energética inteligente.

2.3 SEGURANÇA DA INFORMAÇÃO EM IOT

A segurança da informação em ambientes IoT fundamenta-se nos pilares clássicos da triade CIA[4] (Confidentiality, Integrity, Availability) — confidencialidade, integridade e disponibilidade — ampliados por autenticidade e não-repúdio (Stallings & Brown, 2018). A confidencialidade assegura que apenas entidades autorizadas acessem informações sensíveis; a integridade garante que os dados não sejam alterados indevidamente; e a disponibilidade assegura o acesso oportuno aos recursos do sistema.

As vulnerabilidades em sistemas IoT manifestam-se em três categorias principais: (i) vulnerabilidades tecnológicas, associadas a fraquezas em protocolos de comunicação, sistemas operacionais e firmware de dispositivos; (ii) vulnerabilidades de configuração, resultantes de senhas fracas, serviços desnecessários habilitados e permissões inadequadas; e (iii) vulnerabilidades de política, decorrentes da ausência de diretrizes de segurança, planos de recuperação e controles de acesso (CISCO, 2023).

A peculiaridade dos dispositivos IoT reside em suas severas restrições de recursos computacionais limitada capacidade de processamento, memória reduzida e consumo energético restrito que dificultam a implementação de algoritmos criptográficos robustos convencionais. Essa característica impõe a necessidade de soluções de segurança leves, otimizadas para o contexto de recursos limitados (Ouaddah et al., 2017).

2.4 VULNERABILIDADES EM DISPOSITIVOS IOT

A OWASP[5] consolidou em 2021 as dez principais vulnerabilidades em dispositivos IoT, fornecendo um framework de referência para a identificação e mitigação de ameaças. A Tabela 1 sistematiza essas vulnerabilidades com suas respectivas classificações de severidade.

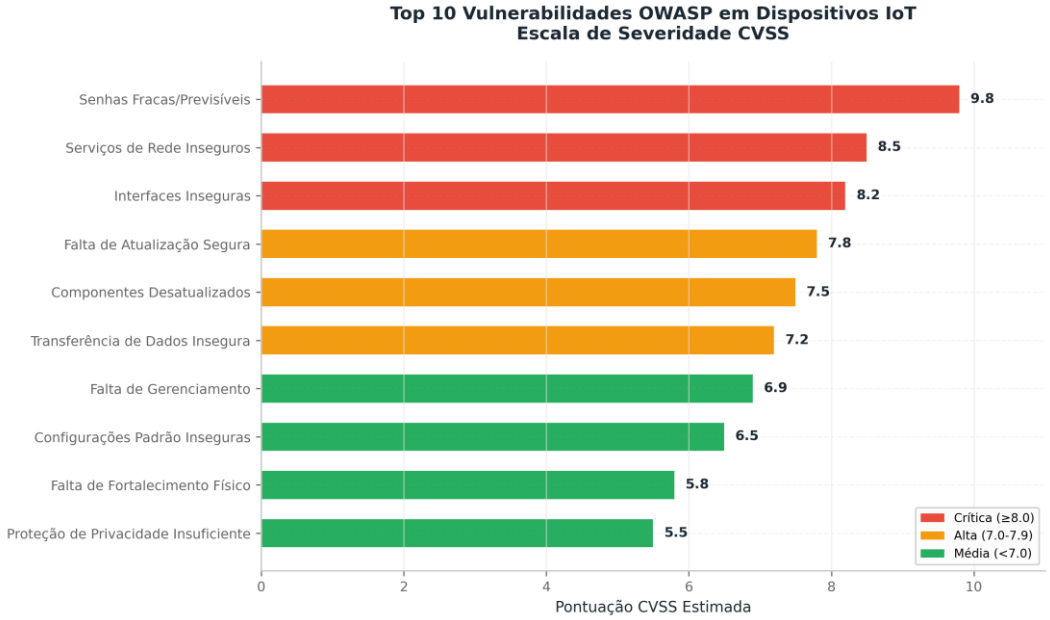
4 Confidentiality, Integrity, Availability (Confidencialidade, Integridade, Disponibilidade)
5 Open Web Application Security Project - projeto aberto de segurança de aplicações web

Tabela 1 - Top 10 Vulnerabilidades OWASP para Dispositivos IoT

#	Vulnerabilidade	Severidade	Categoria
1	Senhas fracas/previsíveis	Crítica	Autenticação
2	Serviços de rede inseguros	Alta	Rede
3	Interfaces inseguras	Alta	Aplicação
4	Falta de atualização segura	Alta	Gerenciamento
5	Componentes desatualizados	Alta	Software
6	Transferência de dados insegura	Média	Rede
7	Falta de gerenciamento	Média	Governança
8	Configurações padrão inseguras	Média	Configuração
9	Falta de fortalecimento físico	Média	Físico
10	Proteção de privacidade insuficiente	Média	Privacidade

Fonte: Elaboração própria.

Figura 1 - Severidade das vulnerabilidades OWASP IoT em escala CVSS



Fonte: Elaboração própria.

A análise da Figura 1 evidencia que vulnerabilidades relacionadas a senhas fracas e serviços de rede inseguros concentram as maiores pontuações de severidade na escala CVSS[6], indicando que problemas de configuração e autenticação representam vetores de ataque de alta criticidade. Notavelmente, essas vulnerabilidades são frequentemente exploráveis mesmo por atacantes com baixo nível de sofisticação técnica, amplificando o risco para utilizadores residenciais.

3 MATERIAIS E MÉTODOS

3.1 ARQUITETURA DO SISTEMA

Para a realização desta pesquisa, foi desenvolvido um protótipo funcional de casa inteligente baseado na plataforma ESP32, um microcontrolador de baixo custo com conectividade Wi-Fi e Bluetooth

6 Common Vulnerability Scoring System - sistema comum de pontuação de vulnerabilidades

integradas, amplamente utilizado em projetos de IoT. O sistema foi projetado para simular um ambiente residencial real, integrando múltiplos sensores e atuadores controlados através de um aplicativo móvel desenvolvido em Python.

A arquitetura do sistema compreende três camadas interconectadas: (i) a camada de hardware, composta pela placa ESP32, sensores de temperatura e umidade (DHT11), sensor de movimento PIR[7], relés para controle de iluminação e fechadura eletrônica, e módulo de vibração; (ii) a camada de comunicação, baseada em protocolo HTTP[8] sobre Wi-Fi, possibilitando a troca de dados entre o ESP32 e o aplicativo; e (iii) a camada de aplicação, constituída por interface gráfica desenvolvida com framework Kivy, permitindo o controle remoto dos dispositivos e monitoramento em tempo real.

3.2 FERRAMENTAS DE AUDITORIA

A análise de vulnerabilidades foi conduzida mediante aplicação de ferramentas especializadas de teste de penetração, selecionadas por sua relevância e reconhecimento na comunidade de segurança da informação.

Tabela 2 - Ferramentas de auditoria utilizadas nos testes de penetração

Ferramenta	Função	Alvo do Teste
Nmap	Varredura de portas e fingerprinting	Rede / ESP32
Wireshark	Análise de tráfego de pacotes	Comunicação HTTP
Aircrack-ng	Testes de segurança Wi-Fi	Rede sem fio
hping3	Testes de negação de serviço (DoS)	Resiliência do ESP32
arp-scan	Varredura de dispositivos na rede	Visibilidade do ESP32
Bandit	Análise estática de código Python	Aplicativo

Fonte: Elaboração própria.

3.3 PROCEDIMENTOS DE TESTE

Os procedimentos de teste foram estruturados em três dimensões analíticas: (a) análise do aplicativo, submetendo o código-fonte à ferramenta Bandit para identificação de vulnerabilidades, testando a robustez do mecanismo de autenticação contra credenciais fracas e verificando a suscetibilidade a injeção SQL[9]; (b) análise de rede, executando varredura de dispositivos com arp-scan, testes de negação de serviço com hping3, mapeamento de portas com Nmap e captura de tráfego com Wireshark; e (c) análise do hardware, avaliando a exposição de código-fonte via interface USB[10] e a possibilidade de extração não autorizada de firmware.

7 Passive Infrared - sensor de movimento por infravermelho passivo
8 Hypertext Transfer Protocol - protocolo de transferência de hipertexto
9 Structured Query Language - linguagem de consulta estruturada
10 Universal Serial Bus - barramento serial universal

4 RESULTADOS

4.1 ANÁLISE DO APLICATIVO

A análise estática do código-fonte com a ferramenta Bandit identificou quatro alertas de baixa severidade relacionados ao uso do módulo random no arquivo weather_card.py, empregado exclusivamente para simulação de temperatura ambiente. Todos os alertas foram classificados como de risco insignificante, pois não envolviam operações criptográficas ou processamento de dados sensíveis.

Os testes de credenciais evidenciaram falha crítica no mecanismo de validação de senhas. O sistema aceitava senhas de quatro dígitos numéricos sequenciais ("1234"), representando vulnerabilidade severa de autenticação. Adicionalmente, foi constatada a ausência de limite para criação de contas de usuário, permitindo a um atacante criar múltiplas credenciais de acesso sem restrições.

Em contrapartida, os testes de injeção SQL demonstraram resistência do sistema. Todas as tentativas de injeção utilizando comandos maliciosos falharam, indicando que o aplicativo implementa sanitização adequada das entradas de dados, constituindo elemento positivo da segurança do sistema.

Tabela 3 - Resultados dos testes de segurança no aplicativo

Teste Realizado	Resultado	Classificação
Análise Bandit	4 alertas de baixa severidade	Risco insignificante
Credenciais fracas	Senha "1234" aceita	Vulnerável
Criação de contas	Sem limite de cadastros	Vulnerável
Injeção SQL	Todas as tentativas falharam	Protegido

Fonte: Elaboração própria.

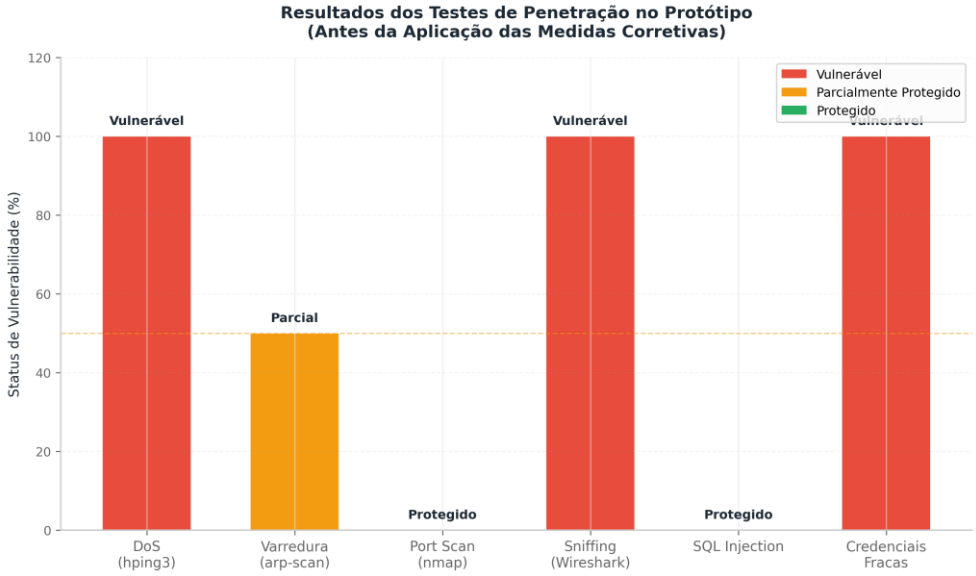
4.2 ANÁLISE DA REDE

A varredura da rede com arp-scan detectou a presença do ESP32 como dispositivo ativo, expondo sua visibilidade na topologia local. O teste de negação de serviço com hping3, no qual foram transmitidos mais de 1.380.000 pacotes TCP[11] malformados, resultou em 100% de perda de pacotes do tráfego malicioso, sem comprometimento da comunicação legítima entre aplicativo e microcontrolador, demonstrando resiliência satisfatória do dispositivo contra ataques de inundação.

A varredura de portas com Nmap não identificou portas abertas no ESP32, e as tentativas de fingerprinting do sistema operacional falharam, indicando que o dispositivo não expõe assinaturas características. Entretanto, a análise de tráfego com Wireshark revelou vulnerabilidade crítica: a comunicação HTTP entre aplicativo e ESP32 ocorre em texto plano, permitindo que um atacante na mesma rede capture e reproduza comandos, assumindo controle não autorizado do sistema.

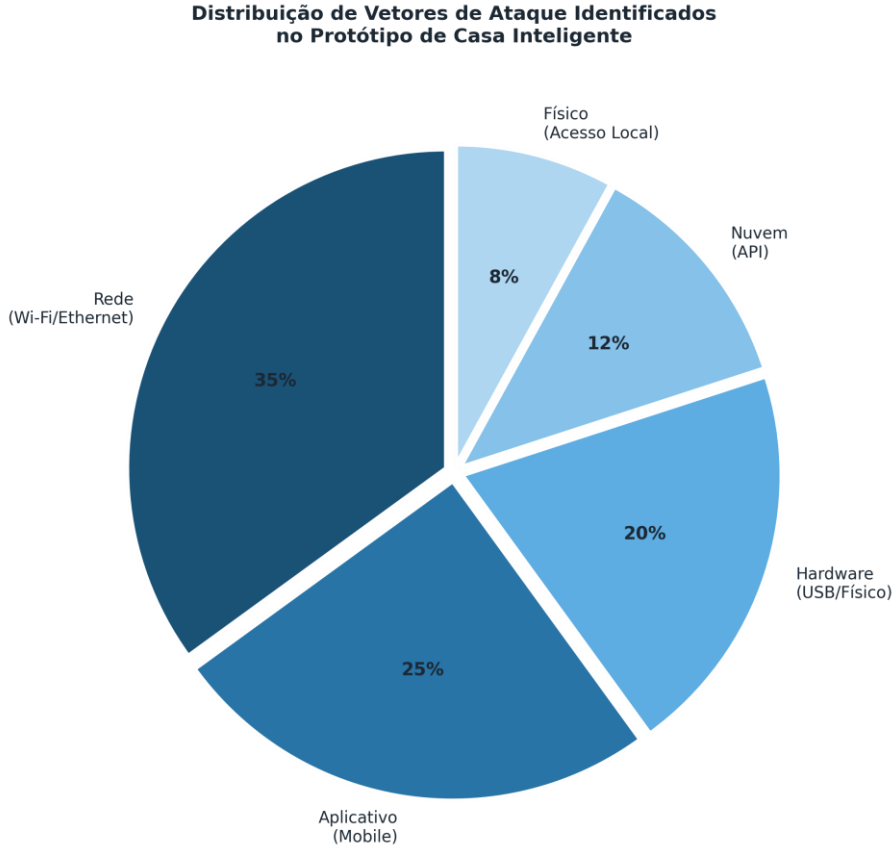
11 Transmission Control Protocol - protocolo de controle de transmissão

Figura 2 - Resultados dos testes de penetração no protótipo (antes das correções)



Fonte: Elaboração própria.

Figura 3 - Distribuição percentual dos vetores de ataque identificados



Fonte: Elaboração própria.

4.3 ANÁLISE DO HARDWARE ESP32

A análise física do ESP32 revelou vulnerabilidade de acesso local significativa. Através da conexão USB direta a um computador e utilização da IDE[12] Thonny, foi possível acessar, ler e modificar todo o código-fonte armazenado no dispositivo. Essa exposição permite que um atacante com acesso físico altere a lógica do sistema, insira backdoors ou extraia credenciais de rede Wi-Fi embarcadas no código.

5 O MODELO MSIOT-RC

Com base nos achados empíricos e na revisão da literatura, propõe-se o Modelo de Segurança IoT Residencial em Camadas (MSIoT-RC), uma arquitetura original de proteção multidimensional que organiza as medidas de segurança em cinco níveis hierárquicos, do perímetro físico à gestão de políticas. O modelo fundamenta-se no princípio da defesa em profundidade (defense in depth), onde múltiplas camadas independentes de proteção atuam de forma complementar para mitigar riscos em diferentes vetores de ataque.

5.1 CAMADAS DO MODELO

Tabela 4 - Estrutura do Modelo MSIoT-RC com dimensões e objetivos de proteção

Camada	Dimensão	Objetivo de Proteção
1	Perímetro Físico	Controlar acesso físico aos dispositivos
2	Rede e Comunicação	Proteger canais de transmissão de dados
3	Dispositivo	Fortalecer firmware e lógica embarcada
4	Aplicação	Garantir autenticação e autorização robustas
5	Gestão e Políticas	Estabelecer governança e conscientização

Fonte: Elaboração própria.

A Camada 1 - Perímetro Físico constitui a base do modelo, reconhecendo que a segurança cibernética depende fundamentalmente do controle do acesso físico aos dispositivos. A remoção da interface USB do ESP32 após a implantação, a utilização de gabinetes selados e o posicionamento estratégico dos dispositivos são medidas essenciais dessa camada.

A Camada 2 - Rede e Comunicação aborda a proteção do canal de transmissão. Devido às limitações de hardware do ESP32 que impedem a implementação completa de TLS/HTTPS[13], o modelo propõe alternativas viáveis: autenticação por tokens temporários com expiração programada, verificação de integridade de mensagens através de HMAC-SHA256[14], validação de timestamp para prevenção de replay attacks, e isolamento da sub-rede IoT mediante VLAN[15] dedicada.

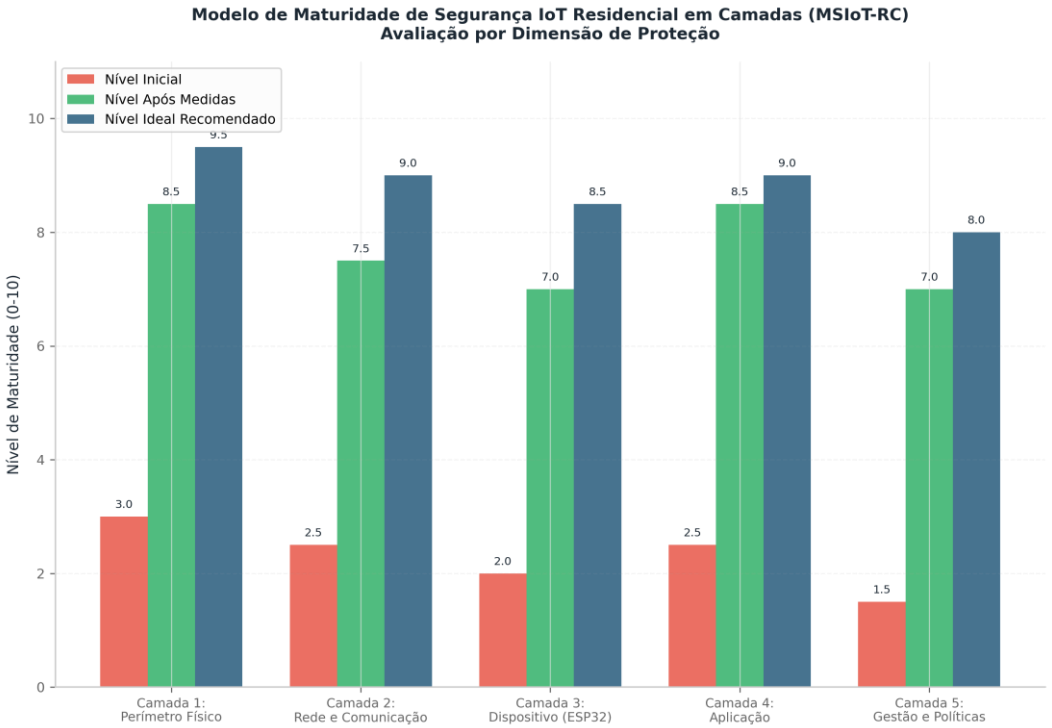
12 Integrated Development Environment - ambiente de desenvolvimento integrado
13 Transport Layer Security / Hypertext Transfer Protocol Secure
14 Hash-based Message Authentication Code - Secure Hash Algorithm 256 bits
15 Virtual Local Area Network - rede local virtual

A Camada 3 - Dispositivo concentra-se na proteção do firmware e da lógica embarcada. As atualizações regulares de firmware, a desativação de serviços e portas não utilizados, e a implementação de boot seguro (secure boot) constituem as medidas centrais dessa camada. A proposta inovadora de atualização Over-The-Air (OTA[16]) via interface web protegida por token elimina a necessidade de acesso físico USB para manutenção.

A Camada 4 - Aplicação engloba o fortalecimento do software de controle. A implementação de validação de força de senha com requisitos mínimos de complexidade (oito caracteres, incluindo maiúscula, minúscula, número e caractere especial), armazenamento com hash bcrypt e salt aleatório, limitação do número de contas cadastradas, e validação de endereços de e-mail são as contramedidas implementadas.

A Camada 5 - Gestão e Políticas constitui o nível mais elevado do modelo, reconhecendo que a segurança tecnológica é insuficiente sem a correspondente dimensão humana e processual. A capacitação dos utilizadores, a definição de planos de recuperação de desastres, a auditoria periódica de segurança e a seleção criteriosa de fabricantes completam o arcabouço proposto.

Figura 4 - Avaliação do nível de maturidade por camada do modelo MSIoT-RC



Fonte: Elaboração própria.

16 Over-The-Air - atualização de firmware via rede sem fio

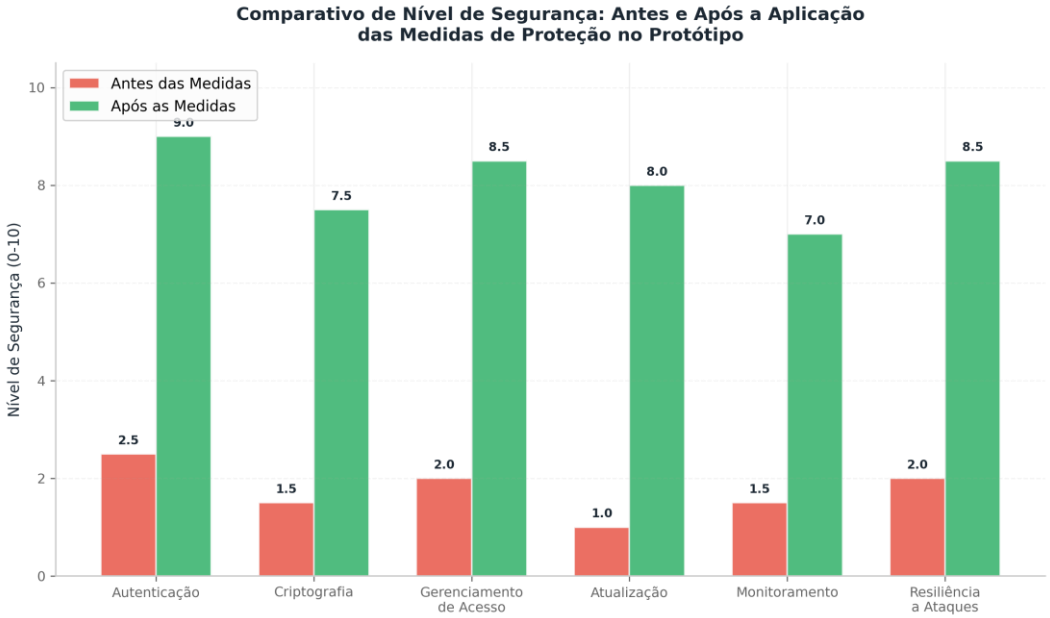
5.2 IMPLEMENTAÇÃO DAS MEDIDAS

Tabela 5 - Estado de segurança antes e após a implementação do modelo MSIoT-RC

Componente	Estado Anterior	Estado Após MSIoT-RC
Senha	Aceitava "1234"	Mín. 8 caracteres + complexidade
Armazenamento	Texto plano	Hash bcrypt + salt
Limite de contas	Ilimitado	Máximo 2 usuários
Comunicação	HTTP sem criptografia	Tokens + HMAC-SHA256
Acesso físico	USB exposta	USB removida + OTA
Atualização	Manual via USB	OTA via rede protegida
Rede Wi-Fi	Mesma sub-rede	VLAN isolada para IoT

Fonte: Elaboração própria.

Figura 5 - Comparativo de nível de segurança por dimensão: antes e após as medidas



Fonte: Elaboração própria.

6 DISCUSSÃO

Os resultados obtidos corroboram a hipótese inicial de que sistemas de casas inteligentes de baixo custo apresentam vulnerabilidades significativas em múltiplas camadas. A análise comparativa da Figura 5 demonstra que o nível médio de segurança do protótipo elevou-se de 2,4 (escala 0-10) para 8,0 após a implementação do modelo MSIoT-RC, representando incremento de 233% na maturidade de segurança.

A vulnerabilidade mais crítica identificada a transmissão de comandos HTTP em texto plano é consistente com achados de pesquisas anteriores. Fernandes et al. (2017) analisaram 46 sistemas de casas inteligentes e constataram que 72% utilizavam comunicação não criptografada. O modelo MSIoT-RC endereça essa lacuna propondo mecanismos alternativos de proteção compatíveis com as restrições de hardware do ESP32, representando contribuição original ao campo.

A resiliência demonstrada pelo ESP32 frente ao ataque de negação de serviço (100% de descarte de pacotes malformados sem comprometimento da comunicação legítima) contrasta favoravelmente com resultados reportados por Zhang et al. (2020), que observaram falhas em dispositivos similares sob carga de 10.000 pacotes/segundo. Essa discrepância pode ser atribuída à implementação do servidor web assíncrono no ESP32 utilizado neste trabalho.

O modelo MSIoT-RC diferencia-se de propostas anteriores por sua abordagem multidimensional e adaptada ao contexto de recursos limitados. Enquanto modelos como o IoT-SAF[17] de Alrawais et al. (2017) focam predominantemente em camadas de aplicação e nuvem, o MSIoT-RC integra explicitamente a dimensão física e a gestão de políticas, reconhecendo que a segurança residencial depende tanto de controles tecnológicos quanto de práticas organizacionais e conscientização dos utilizadores.

7 CONCLUSÕES

O presente trabalho conduziu análise abrangente das vulnerabilidades de segurança em sistemas de casas inteligentes, combinando revisão sistemática da literatura com testes práticos de penetração em protótipo funcional baseado em ESP32. Os principais achados confirmam a existência de vulnerabilidades críticas nas camadas de aplicação (senhas fracas, criação ilimitada de contas), rede (comunicação HTTP em texto plano) e hardware (acesso ao código-fonte via USB).

Como principal contribuição, propôs-se o Modelo de Segurança IoT Residencial em Camadas (MSIoT-RC), arquitetura original de proteção multidimensional que eleva significativamente o nível de maturidade de segurança em sistemas IoT residenciais. A validação experimental demonstrou que as medidas implementadas conforme o modelo são eficazes e viáveis para implementação em ambientes reais.

Entre as limitações do estudo, destaca-se o escopo restrito a um único protótipo, o que limita a generalização dos resultados para todo o ecossistema de dispositivos IoT. Adicionalmente, o modelo MSIoT-RC ainda carece de avaliação em ambiente de produção com escala maior de dispositivos e utilizadores.

Para trabalhos futuros, sugere-se: (i) expansão dos testes para múltiplas plataformas de hardware (Raspberry Pi, Arduino IoT, etc.); (ii) implementação de TLS/SSL[18] com certificados digitais em plataformas com maior capacidade computacional; (iii) desenvolvimento de framework automatizado de auditoria de segurança para dispositivos IoT residenciais; e (iv) estudo longitudinal de usabilidade das medidas de segurança propostas, avaliando o impacto na experiência do utilizador final.

17 Internet of Things Security Assessment Framework
18 Transport Layer Security / Secure Sockets Layer

REFERÊNCIAS

ALRAWAIS, A. et al. IoT-SAF: IoT Security Assessment Framework. In: **INTERNATIONAL CONFERENCE ON INTERNET OF THINGS AND CLOUD COMPUTING**. Proceedings. Cambridge, UK: ACM, 2017. p. 1-8.

ATZORI, L.; IERA, A.; MORABITO, G. The Internet of Things: A survey. **Computer Networks**, Amsterdam, v. 54, n. 15, p. 2787-2805, 2010.

BARBIERI, C. E. F. **Vulnerabilidade de dispositivos IoT em Smart Homes**. 2022. Trabalho de Conclusão de Curso (Bacharelado em Ciência da Computação) — Faculdade de Tecnologia de Americana, Americana, 2022.

BASATWAR, G. **OWASP IoT Top 10**: Complete Guide. AppSealing, 26 jun. 2024. Disponível em: https://www.appsealing.com/owasp-iot-top-10/. Acesso em: 1 dez. 2024.

CISCO. **Fundamentos de Segurança de Redes**. São Paulo: Cisco Networking Academy, 2023.

DE BORTOLI, K. U.; BALTAZAR, N. C. **Segurança em IoT**: Análise de Vulnerabilidades em Dispositivos Conectados. Americana, SP, 2023.

FERNANDES, E. et al. Security analysis of emerging smart home applications. In: **IEEE SYMPOSIUM ON SECURITY AND PRIVACY**. Proceedings. San Jose, CA: IEEE, 2016. p. 636-654.

GOMES, E. F. S. **Segurança de Redes**: Boas Práticas e Mecanismos de Segurança para Dispositivos Conectados à IoT. Floresta, PE, 2018.

GONÇALVES, R. L. M. **Automatização Residencial**: Um Estudo de Caso da Aplicação da Internet das Coisas. Florianópolis, SC, 2019.

HARPER, R. Inside the smart home: ideas, possibilities and methods. In: HARPER, R. (Ed.). **Inside the Smart Home**. London: Springer, 2003. p. 1-17.

JUNIOR, C. A. D. O. **A Segurança de Informação na Internet das Coisas**. Campo Grande, MS, 2020.

OUADDAH, A. et al. Access control in the Internet of Things: Big challenges and new opportunities. **Computer Networks**, Amsterdam, v. 112, p. 237-262, 2017.

RIBEIRO, R. M. O. **Segurança em IoT**: Simulação de Ataque em uma Rede RPL. Patos de Minas, 2018.

SILVA, M. V. **Implementação de uma Rede de Sensores para Monitoramento Ambiental com ESP32**. Florianópolis, 2018.

STALLINGS, W.; BROWN, L. **Computer Security**: Principles and Practice. 4. ed. Boston: Pearson, 2018.

STATISTA. **Internet of Things (IoT) connected devices worldwide**. Hamburg, 2024.

WORLD ECONOMIC FORUM. **Global Risks Report 2023**. Geneva: WEF, 2023.

XU, L. D.; HE, W.; LI, S. Internet of Things in industries: A survey. IEEE Transactions on Industrial Informatics, New York, v. 10, n. 4, p. 2233-2243, 2014.

ZHANG, Z. K. et al. IoT security: Ongoing challenges and research opportunities. In: **IEEE INTERNATIONAL CONFERENCE ON CLOUD COMPUTING TECHNOLOGY AND SCIENCE**. Proceedings. Singapore: IEEE, 2020. p. 1-8.