ISSN: 2595-5942

Análise de ameaças e vulnerabilidades em sistemas de casas inteligentes baseados em IoT

Felipe Aires Joaquim
Fatec Mogi das Cruzes
felipe.joaquim@fatec.sp.gov.br

Matheus Rodrigues Bispo
Fatec Mogi das Cruzes
matheus.bispo01@fatec.sp.gov.br

Luciano Gonçalves de Carvalho
Fatec Mogi das Cruzes
luciano.carvalho@fatec.sp.gov.br

Resumo
Este artigo analisa as vulnerabilidades de segurança em dispositivos de casas inteligentes, cujo risco aumentou com a maior conectividade doméstica e o crescimento de ciberataques. A pesquisa foi realizada por meio de uma revisão bibliográfica sistemática, na qual foram selecionados estudos recentes sobre IoT e segurança residencial. A análise permitiu identificar padrões recorrentes de falhas e agrupar as vulnerabilidades em três categorias principais: problemas de software e firmware, ausência de atualizações e configurações inadequadas de rede. Esses fatores expõem os usuários a ameaças como invasões remotas, sequestro de dispositivos e monitoramento indevido. Com base nesses achados, o estudo propõe duas medidas de mitigação: a segmentação da rede *Wi-Fi* para isolar dispositivos IoT e o uso de um hub de segurança dedicado com *firewalhjunuiii* para centralizar o controle. Embora eficazes, essas soluções apresentam desafios como complexidade de implementação, custos adicionais e possível ponto único de falha. Conclui-se que a segurança em casas inteligentes depende de uma postura proativa do usuário, incluindo atualizações constantes e adoção de práticas robustas de proteção.

Palavras-chave: Cibersegurança; IoT; Segurança; Tecnologia.

Abstract

This article analyzes security vulnerabilities in smart home devices, a risk that has increased with greater domestic connectivity and the rise of cyberattacks. The study was conducted through a systematic literature review, in which recent academic papers on IoT and residential cybersecurity were selected. The analysis identified recurring patterns of failures and grouped vulnerabilities into three main categories: software and firmware weaknesses, lack of updates, and insecure network configurations. These factors expose users to threats, such as remote intrusions, device hijacking, and unauthorized monitoring. Based on these findings, the study proposes two mitigation strategies: Wi-Fi network segmentation to isolate IoT devices and the use of a dedicated security hub with an integrated firewall. Although effective,

these measures present challenges, such as implementation complexity, additional costs, and the possibility of creating a single point of failure. The study concludes that smart home security depends on a proactive user posture, including regular updates and the adoption of robust protection practices.

Keywords: Cybersecurity; IoT; Security; Technology.

I. INTRODUÇÃO

Com o aumento de dispositivos conectados à internet, torna-se evidente que a tecnologia passou a assumir um papel central nas atividades domésticas, automatizando tarefas e oferecendo maior praticidade ao cotidiano. A evolução da automação residencial possibilitou a popularização de dispositivos inteligentes, como lâmpadas, tomadas, sensores, assistentes de voz e robôs de limpeza, que operam com mínima intervenção humana. Essa expansão foi impulsionada pelo avanço da Internet das Coisas (IoT), que permite que diversos equipamentos se comuniquem entre si e com a nuvem, criando ecossistemas domésticos cada vez mais integrados.

Entretanto, o crescimento desse cenário trouxe implicações relevantes para a segurança digital. À medida que mais dispositivos passam a depender de conectividade contínua, aumenta também a superfície de ataque explorável por agentes mal-intencionados. Vulnerabilidades como firmware desatualizado, senhas fracas, portas de rede expostas e falhas de projeto tornam-se pontos de entrada para ameaças como invasões remotas, sequestro de dispositivos, monitoramento indevido e disseminação de malwares. Em ambientes onde diversos serviços estão vinculados a uma única conta principal, a violação de um único dispositivo pode comprometer e-mails, redes sociais e até dados financeiros do usuário.

Nesse contexto, surge um problema de pesquisa central: quais são as vulnerabilidades predominantes em sistemas de casas inteligentes baseados em IoT, e quais mecanismos de segurança podem reduzir de forma eficaz os riscos associados ao seu uso no ambiente doméstico?

Diante dessa questão, o objetivo deste estudo é identificar e analisar as principais ameaças e vulnerabilidades presentes em dispositivos de automação residencial, além de avaliar práticas de mitigação capazes de aumentar a segurança digital nesse tipo de ecossistema. A partir de uma revisão bibliográfica sistemática, busca-se compreender como essas falhas se manifestam, quais fatores contribuem

para sua exploração e quais estratégias podem ser adotadas para fortalecer a proteção dos usuários em ambientes conectados.

Para responder a esse problema, este estudo conduz uma revisão bibliográfica sistemática focada nas principais vulnerabilidades e estratégias de mitigação para ambientes domésticos inteligentes.

2. FUNDAMENTAÇÃO TEÓRICA

2.1. Automação Residencial

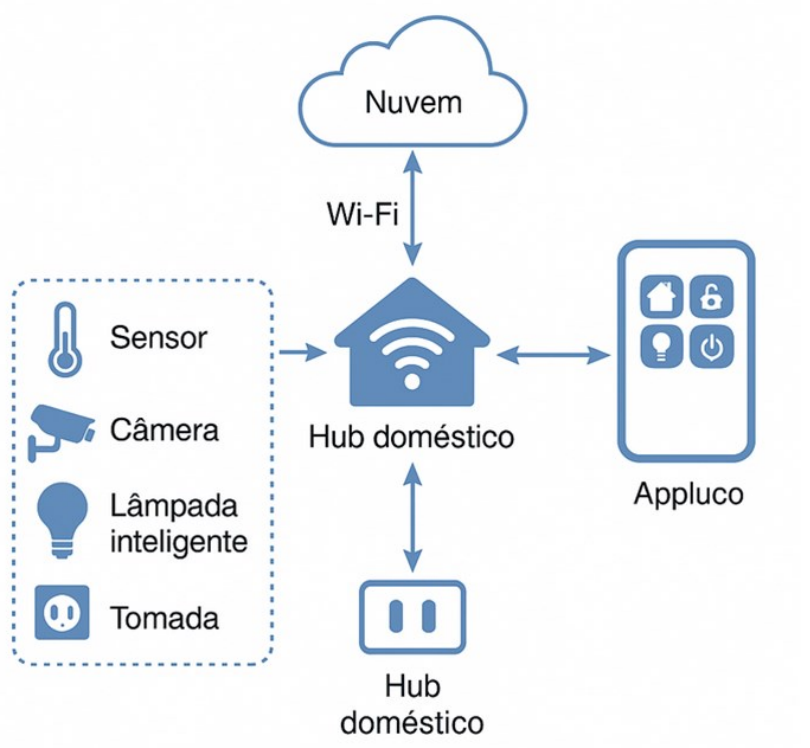
Com o desenvolvimento da tecnologia, percebe-se que o aumento do acesso à internet e o crescimento dos dispositivos tecnológicos têm sido incorporados ao contexto residencial de forma constante, agilizando atividades cotidianas e auxiliando pessoas idosas a realizarem tarefas com mais autonomia. Segundo Rocha e Anhesine (2020), o crescimento populacional tende à estagnação em 2047, o que reforça a necessidade de tecnologias que apoiem a vida diária. Assim, a automação residencial torna-se uma solução que busca melhorar qualidade de vida, conforto e segurança.

A automação residencial consiste em um conjunto de dispositivos conectados entre si por meio de um controlador, no qual esses dispositivos possuem acesso à internet e são controlados automaticamente ou podem ser controlados remotamente pelo usuário, portanto, segundo Simplício, Lima e Silva (2018), torna-se possível controlar, gerenciar e obter informações de uma residência equipada com produtos automatizados. Alguns exemplos de automação residencial atualmente em uso são: controle de iluminação, sensores de presença, portas automáticas, integração ambiental com telefones celulares e rega automática.

A Figura 1 ilustra a estrutura básica de um sistema de automação residencial, evidenciando a comunicação entre sensores, atuadores, o hub doméstico e o aplicativo móvel conectado à nuvem.

ISSN: 2595-5942

Figura 1 – Estrutura de um Sistema de Automação Residencial



Fonte: Elaborado pelos autores (2025)

Apesar dos benefícios, a automação residencial ainda enfrenta desafios, como alto custo, falta de padronização de protocolos e dificuldades na implementação em estruturas pré-existentes. Este cenário revela um contraste entre autores: enquanto Simplício et al. (2018) destacam o potencial social e econômico, Teixeira e Cosmo (2022) reforçam que a adoção depende de soluções acessíveis, indicando que a evolução da automação ainda é desigual em diferentes faixas socioeconômicas. Essa divergência mostra que a automação não é apenas uma questão técnica, mas também estrutural e social.

2.2. IoT Aplicado à Automação Residencial

Com o avanço tecnológico, mais dispositivos passam a se conectar à internet, formando ecossistemas capazes de coletar e analisar dados sem intervenção humana. Segundo Carrion e Quaresma (2019), a Internet das Coisas engloba uma diversidade de tecnologias e serviços que formam um ecossistema amplo e interdependente. Massola e Pinto (2018) complementam afirmando que a IoT

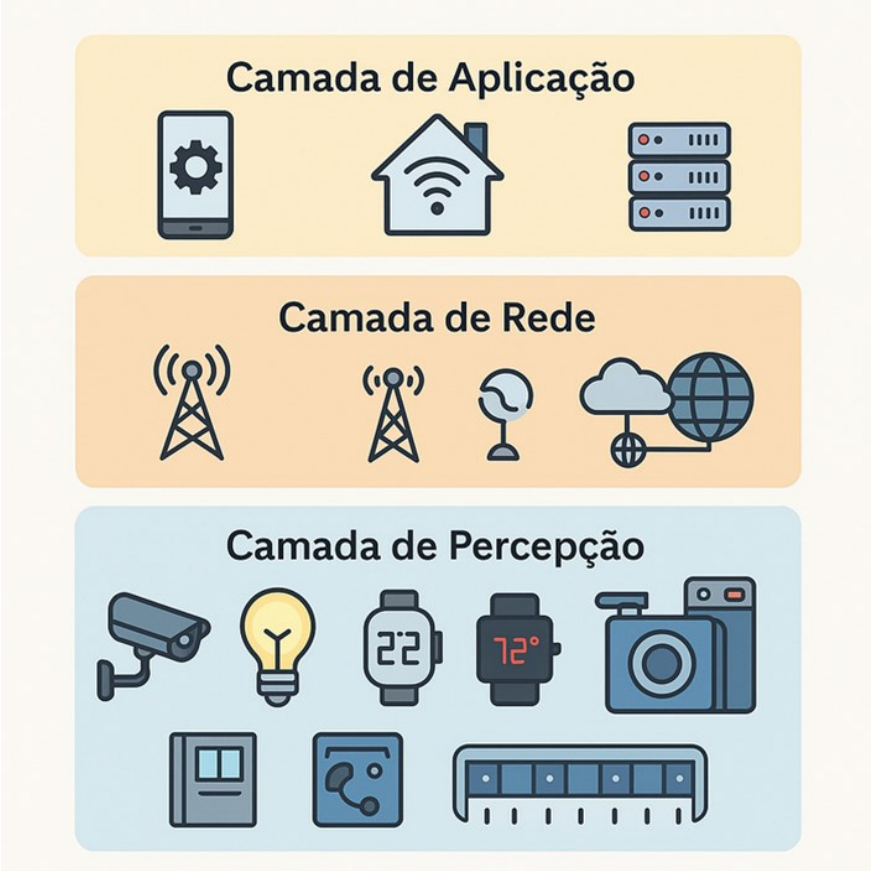
ISSN: 2595-5942

funciona como uma estrutura de rede composta por objetos capazes de sensoriamento, comunicação e processamento.

Essa comunicação entre atuadores, controladores e dispositivos sensores é fundamental para automatizar ambientes residenciais, permitindo conforto, agilidade e eficiência. A Figura 2 apresenta a arquitetura em camadas da IoT, evidenciando as interações entre percepção, rede e aplicação.

Contudo, embora os autores concordem sobre o potencial da IoT, divergem quanto aos desafios: enquanto Carrion e Quaresma (2019) enfatizam sua complexidade tecnológica, Massola e Pinto (2018) chamam atenção para limitações técnicas necessárias para seu funcionamento, como sensoriamento e conectividade estável. Essa comparação evidencia que a IoT, além de ser o núcleo funcional da automação, também representa um ponto crítico para vulnerabilidades quando mal projetada.

Figura 2 – Arquitetura em Camadas da Internet das Coisas (IoT)



Fonte: Elaborado pelos autores (2025)

2.3. Segurança da Informação

A segurança da informação parte do princípio da proteção de dados ou um conjunto de determinadas informações do indivíduo. Com o objetivo de garantir a preservação dos seus respectivos valores, atuando digitalmente ou não, busca impedir a manipulação de tais dados por pessoas maliciosas e que não devem possuir acesso autorizado a esses dados de maneira alguma. Dessa forma, alguns valores são empregados nos ideais da segurança da informação como atributos de confidencialidade, integridade e disponibilidade.

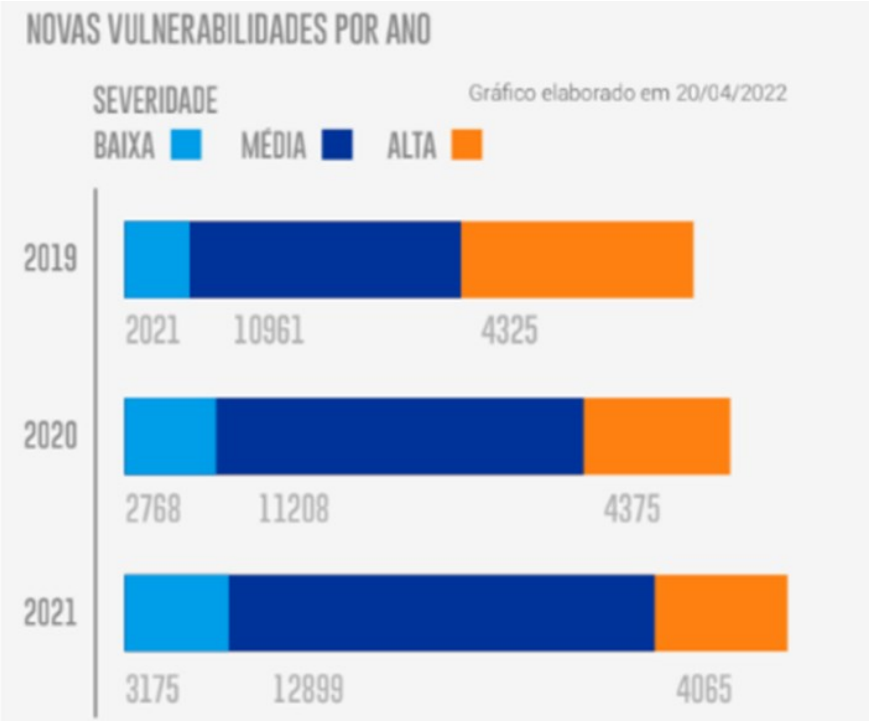
Devido ao avanço tecnológico, nota-se a importância da segurança da informação nas grandes organizações. Em sistemas de casas inteligentes também não é diferente, seguindo-se o princípio de que os dados devem ser mantidos em segurança. A maior causa de perda de dados é dada por ataques cibernéticos, onde seu único objetivo é o roubo, violação e sequestro de informações sigilosas armazenadas.

O Gráfico 1, apresentado por Prates et al. (2022), demonstra o crescimento de vulnerabilidades identificadas ao longo dos anos, especialmente durante a pandemia de COVID-19. Esse contexto reforça que a segurança da informação, antes associada ao ambiente corporativo, tornou-se indispensável em casas inteligentes, onde falhas simples podem resultar em invasões, sequestros de dados e monitoramentos indevidos.

A literatura converge ao reconhecer a importância dos princípios de segurança, mas diverge quanto às causas das falhas. Enquanto Prates et al. (2022) associam o aumento de incidentes ao trabalho remoto e à maior conectividade, autores como Sen (2018) apontam fatores econômicos e comportamentais como elementos igualmente críticos. Essa diversidade de interpretações reforça que a segurança em casas inteligentes é multifatorial.

ISSN: 2595-5942

Gráfico 1 – Novas Vulnerabilidades por ano



Fonte: PRATES *et al*. (2022, p. 02)

A partir dos dados apresentados pelo Gráfico 1, observa-se que o aumento das vulnerabilidades não representa apenas um crescimento quantitativo, mas também qualitativo, refletindo a sofisticação dos ataques direcionados a dispositivos conectados. Durante o período da pandemia, a maior dependência de redes domésticas ampliou a exposição de aparelhos IoT, exigindo uma evolução proporcional das práticas de proteção. Nesse contexto, medidas como redução da exposição de portas e serviços, manutenção frequente de firmware, habilitação de autenticação multifator e segmentação da rede doméstica passaram a ser fundamentais para mitigar riscos.

Em casas inteligentes, onde sensores, câmeras, hubs e assistentes virtuais operam de forma integrada, qualquer dispositivo desatualizado pode se tornar o elo mais fraco de toda a arquitetura. Além disso, como esses equipamentos permanecem conectados continuamente, a janela de oportunidade para ataques se mantém aberta durante todo o tempo. Dessa forma, a literatura converge ao demonstrar que práticas básicas de segurança como atualizações, senhas robustas e isolamento da rede deixam de ser recomendações opcionais e se tornam requisitos essenciais para preservar a integridade dos dados e a privacidade do usuário.

ISSN: 2595-5942

2.3.1 Vulnerabilidades de Dispositivos Conectados à Rede

Com o fluxo contínuo de dados na internet, dispositivos domésticos tornam-se alvos potenciais de ataques. Falhas de projeto, firmware desatualizado e configurações inseguras ampliam a superfície de ataque e podem expor informações do usuário. Lima e Panham (2019) destacam que muitos projetistas não dominam protocolos de segurança, contribuindo para a fragilidade dos sistemas.

A conectividade contínua das casas inteligentes 24 horas por dia intensifica esses riscos, uma vez que dispositivos vulneráveis permanecem constantemente acessíveis a ataques remotos. A falta de atualizações de firmware cria ciclos de vulnerabilidade prolongados.

A Tabela 1 evidencia como ataques cibernéticos a dispositivos IoT seguem um ciclo que vai da exploração inicial ao roubo de dados. Esse modelo, embora amplamente aceito, também é criticado por simplificar cenários mais complexos, como ataques distribuídos, engenharia social ou exploração de ecossistemas integrados. Essa observação crítica alinha o referencial teórico com a necessidade de análises mais profundas na literatura.

Tabela 1 – Etapas de um ataque cibernético em dispositivos IoT

Etapa	Descrição
1. Exploração de vulnerabilidade	O atacante identifica e explora falhas existentes em firmware, aplicativos ou configurações inseguras do dispositivo IoT.
2. Invasão	Após explorar a brecha, o invasor obtém acesso ao dispositivo, podendo modificar parâmetros, instalar códigos maliciosos ou criar portas de acesso remoto.
3. Controle remoto	O atacante passa a manipular o dispositivo comprometido, executando comandos, monitorando atividades ou conectando-o a uma botnet.
4. Roubo de dados	Os dados armazenados ou transmitidos pelo dispositivo são interceptados e extraídos, podendo incluir informações sensíveis do usuário.

ISSN: 2595-5942

Fonte: Elaborado pelos autores (2025)

2.3.2 Segurança de Redes

Quando se fala de aplicações IoT, os sistemas de redes têm um papel muito importante, o que torna a segurança de redes um fator de extrema importância. Isto porque, se um ataque de rede feito por um hacker for bem-sucedido, ele poderá não apenas roubar dados importantes, como também danificar dispositivos ligados à rede atacada.

Apesar de a internet possuir protocolos de segurança como o TCP/IP para tentar evitar esses ataques, estes possuem vulnerabilidades que são exploradas por hackers mal-intencionados. Para fortalecer a proteção, é preciso considerar os pilares da segurança de redes. Segundo Chahar (2022), os fatores que devem ser levados em conta são confidencialidade, integridade, autenticação e não-repúdio.

Sendo assim, para garantir a segurança das redes é necessário conhecer as vulnerabilidades relacionadas a elas, a fim de ter medidas de proteção para possíveis ataques. Além disso, embora exista consenso na literatura sobre a importância desses pilares, há divergências sobre quais camadas da rede apresentam maior risco: alguns autores enfatizam falhas de aplicação, enquanto outros destacam vulnerabilidades decorrentes de configurações inadequadas de roteadores e portas expostas. Essa variedade de interpretações mostra que a proteção de redes em ambientes IoT exige uma abordagem integrada, que considere tanto aspectos técnicos quanto configurações adotadas pelo usuário.

2.4. Cybersecurity

A segurança cibernética (cybersecurity) consiste em um conjunto de padrões, normas e práticas que tem como objetivo garantir um ambiente totalmente seguro. Ambientes seguros são compostos por dispositivos, sistemas e pessoas. Este termo vem ganhando cada vez mais destaque devido à crescente expansão do uso da internet ocorrida nos últimos anos.

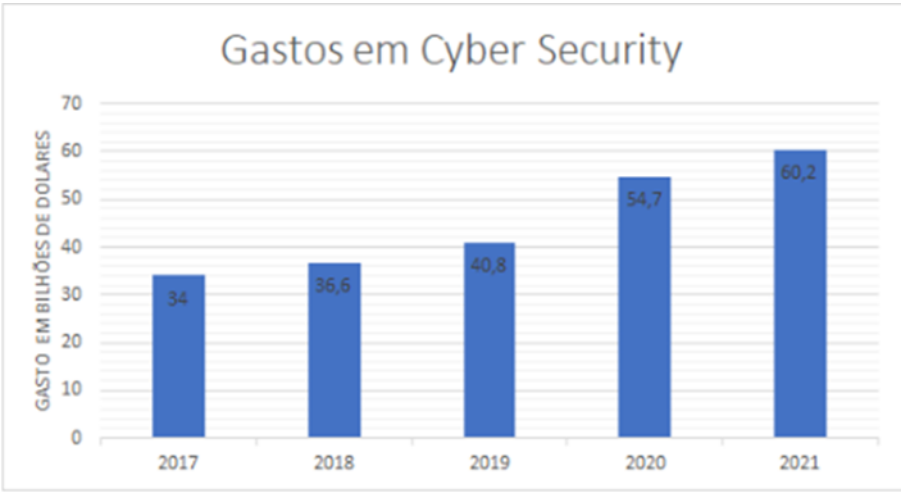
Um grande exemplo dessa expansão foi durante a pandemia da COVID-19 onde foi possível observar um aumento no uso de sites ou aplicativos de compra online e o uso de ferramentas de vídeo chamada para trabalho ou estudo. Diante

dessa realidade, houve também um aumento de ataques cibernéticos cuja finalidade seria prejudicar empresas e pessoas por meio da coleta de dados sensíveis.

De acordo com o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), o ano de 2019 registrou um aumento de 29% no total de notificações de segurança, alcançando 875.327 incidentes reportados. O destaque principal foi o crescimento de 90% nas notificações sobre computadores envolvidos em ataques de negação de serviço (DoS), que somaram 301.308 casos - o maior número da série histórica. A maior parte desses ataques de negação de serviço distribuídos (DDoS) foi originada por botnets de dispositivos de IoT, como Mirai e Bashlite, que exploram vulnerabilidades em equipamentos como roteadores e DVRs.

Dentro desta realidade, a proteção digital se tornou uma ferramenta importante para a segurança de dados sensíveis de empresas e pessoas que fazem o uso diário de dispositivos ligados a redes ou serviços via internet, como a computação na nuvem. Com esse objetivo em mente, as organizações vêm cada vez mais investindo em recursos de segurança, como mostra o gráfico a seguir os investimentos feitos em cybersecurity de 2017 a 2021 em todo o mundo.

Gráfico 2 – Gastos em Cyber Security no mundo de 2017 a 2021



Fonte: Adaptado do Statista (2022)

Porém, apenas os investimentos no setor não garantem a segurança desses dados. Segundo Sen (2018), a fragilidade da segurança digital está ligada a fatores técnicos, problemas econômicos, legais e comportamentais que são enfrentados por

usuários e organizações. A fim de garantir um ambiente seguro, é necessário adotar as medidas necessárias de proteção adequadas. Da mesma forma, é crucial que as pessoas que fazem uso da tecnologia tenham o conhecimento sobre a importância dessas medidas.

Embora os dados apresentem um aumento considerável nos investimentos globais em segurança cibernética, a literatura indica que essas iniciativas nem sempre se traduzem em redução efetiva dos ataques. Isso ocorre porque grande parte das vulnerabilidades exploradas em ambientes IoT decorre de práticas inadequadas de configuração, dispositivos desatualizados e falta de capacitação dos usuários. Assim, observa-se um descompasso entre o avanço das soluções tecnológicas e a capacidade dos usuários de aplicá-las corretamente, tornando o fator humano um ponto crítico para a proteção de casas inteligentes.

3. MÉTODO

A presente pesquisa teve como objetivo analisar as principais ameaças e vulnerabilidades presentes em sistemas de casas inteligentes baseados em IoT. Para isso, adotou-se uma abordagem exploratória com base em uma revisão bibliográfica sistemática, permitindo identificar o estado da arte sobre segurança em dispositivos conectados no ambiente doméstico.

A busca por materiais foi realizada entre agosto e setembro de 2025 em bases de dados amplamente utilizadas na área de tecnologia e ciência da computação, incluindo Google Acadêmico, ResearchGate, SciELO, e a Biblioteca Digital de Teses e Dissertações da USP. Para complementar os dados estatísticos relacionados ao crescimento de ataques cibernéticos e investimentos em segurança, utilizou-se ainda o portal Statista.

Os principais termos de busca empregados foram: “automação residencial”, “IoT aplicado à automação residencial”, “segurança da informação”, “vulnerabilidades em IoT”, “segurança de redes”, “cibersegurança”, “ataques cibernéticos” e “dispositivos inteligentes”. Os termos foram combinados com operadores booleanos (AND/OR), resultando em um conjunto inicial de 97 estudos identificados.

A seleção dos materiais seguiu critérios previamente definidos. Foram incluídos estudos que: abordassem diretamente dispositivos IoT ou automação residencial; apresentassem dados, análises ou discussões sobre vulnerabilidades, ataques ou

segurança; estivessem publicados entre 2018 e 2025; fossem artigos científicos, relatórios técnicos, revisões ou documentos oficiais.

Assim como na etapa de inclusão, critérios também foram aplicados para a exclusão de materiais que não atendiam aos requisitos metodológicos do estudo. Foram excluídos: trabalhos duplicados; documentos sem texto completo disponível; artigos que tratavam de IoT apenas no contexto industrial; materiais sem abordagem clara da segurança da informação ou de vulnerabilidades.

Após a triagem dos títulos e resumos, 54 estudos permaneceram para avaliação completa. Destes, 32 foram excluídos por não atenderem aos critérios temáticos ou metodológicos. Assim, o corpus final da revisão foi composto por 22 estudos, que fundamentaram as análises e discussões apresentadas neste artigo.

A análise dos estudos selecionados ocorreu por meio de categorização temática, permitindo identificar padrões recorrentes, tais como: falhas de software e firmware, ausência de atualizações, vulnerabilidades de rede, uso de senhas fracas, exposição de portas, e riscos gerados pela integração entre múltiplos dispositivos inteligentes. Essa análise qualitativa possibilitou sintetizar as principais ameaças relacionadas às casas inteligentes, bem como compreender suas causas e impactos sobre privacidade, integridade e disponibilidade dos dados.

Com base nas vulnerabilidades mais frequentes identificadas na revisão, foram avaliadas soluções presentes na literatura como segmentação de rede, adoção de hubs de segurança e autenticação multifator, examinando não apenas seus benefícios, mas também limitações e desafios de implementação em residências comuns. Esse processo permitiu propor recomendações alinhadas ao perfil dos riscos levantados, garantindo coerência entre os achados da revisão e as estratégias apresentadas no estudo.

4. ANÁLISE E RESULTADOS

A análise dos 22 estudos selecionados demonstrou que, embora os dispositivos de casas inteligentes ofereçam praticidade e automação, eles também apresentam vulnerabilidades significativas associadas ao software embarcado, ao firmware desatualizado e às configurações inadequadas de rede. A maior parte dos trabalhos revisados destacou que falhas de implementação, ausência de atualizações e uso de senhas fracas são fatores centrais que ampliam a superfície

de ataque dos dispositivos IoT, confirmando a tendência observada por Lima e Panham (2019) e Sen (2018). A elevação dos ataques durante a pandemia da COVID-19, também apresentada por Prates et al. (2022), reforça a necessidade de mecanismos de proteção adaptados ao ambiente doméstico conectado.

Com base nessas vulnerabilidades predominantes, duas estratégias foram identificadas como recorrentes na literatura e viáveis para o contexto residencial: a segmentação da rede doméstica e a adoção de um hub de segurança dedicado com firewall integrado. Ambas aparecem como recomendações frequentes nos estudos analisados, especialmente naqueles que abordam ataques decorrentes da exploração de dispositivos mal configurados ou inseridos em redes domésticas pouco protegidas.

Solução 1: Segmentação da Rede Wi-Fi Doméstica

Uma medida eficaz descrita em diversos estudos consiste em criar uma rede exclusiva para dispositivos IoT, por meio de redes de convidados ou VLANs. A literatura aponta que o isolamento dos dispositivos reduz significativamente o potencial de movimentação lateral de um invasor dentro da rede doméstica, uma vez que equipamentos sensíveis (como computadores e smartphones) permanecem protegidos na rede principal.

A Tabela 2 apresenta uma comparação entre redes convencionais e redes segmentadas, destacando ganhos de segurança, capacidade de monitoramento e limitações práticas.

Tabela 2 – Comparação entre rede convencional e rede segmentada para dispositivos IoT

Aspecto	**Rede Convencional**	**Rede Segmentada (com rede IoT dedicada)**
Topologia	Todos os dispositivos conectam-se ao mesmo roteador e compartilham a mesma rede local.	Criação de uma rede separada (VLAN ou rede de convidados) exclusivamente para dispositivos IoT.
Segurança	Maior exposição: um dispositivo comprometido	Reduz a superfície de ataque, isolando dispositivos IoT e

	pode servir de porta de entrada para outros da rede.	protegendo os que armazenam dados sensíveis.
Gerenciamento	Controle simplificado, mas sem monitoramento segmentado de tráfego.	Permite monitoramento e controle específicos por segmento, facilitando detecção de anomalias.
Complexidade de configuração	Instalação rápida e intuitiva, adequada para usuários leigos.	Requer conhecimento intermediário de rede para configuração de sub-redes ou VLANs.
Custo adicional	Nenhum custo adicional além do roteador principal.	Pode exigir roteadores avançados ou equipamentos com suporte a múltiplas redes.

Fonte: Elaborado pelos autores (2025)

Análise de Risco da Solução 1:

- **Complexidade de Implementação:** A configuração de redes separadas pode ser complexa para usuários sem conhecimento técnico, o que pode levar a configurações incorretas que não garantem o isolamento efetivo.

- **Interoperabilidade Limitada:** Alguns dispositivos podem apresentar dificuldades de comunicação ou perda de funcionalidades ao serem controlados por um smartphone que está em uma rede diferente, exigindo configurações adicionais de permissão entre as redes, o que pode, se mal implementado, anular o propósito da segmentação.

- **Falsa Sensação de Segurança:** O usuário pode acreditar que a segmentação o protege de todos os tipos de ataques. No entanto, se um dispositivo IoT for comprometido, ele ainda pode ser usado para lançar ataques a alvos externos à rede doméstica ou para monitorar o tráfego dentro de sua própria sub-rede. A rede principal ainda pode ser vulnerável a outros tipos de ataques que não se originam dos dispositivos IoT.

Esses riscos são coerentes com achados da literatura, que ressalta que a segmentação melhora a segurança, mas não elimina a necessidade de boas práticas, como atualizações frequentes e autenticação reforçada.

Solução 2: Implementação de um Hub de Segurança Dedicado

A segunda solução identificada nos estudos consiste no uso de um hub centralizador equipado com firewall. Essa abordagem permite a inspeção unificada do tráfego IoT, aplicando regras específicas para dispositivos potencialmente mais vulneráveis e evitando que cada aparelho se conecte diretamente ao roteador.

Análise de Risco da Solução 2:

- **Ponto Único de Falha:** A centralização da conexão em um único hub cria um ponto crítico. Se o hub falhar ou for comprometido, todos os dispositivos de casa inteligente conectados a ele podem se tornar inoperantes ou vulneráveis simultaneamente.

- **Custo e Compatibilidade:** A aquisição de um hub de segurança dedicado representa um custo adicional para o usuário. Além disso, podem existir problemas de compatibilidade, pois nem todos os dispositivos IoT de diferentes fabricantes podem ser compatíveis com um único hub, limitando as opções do consumidor.

- **Dependência do Fabricante:** A segurança do sistema passa a depender diretamente da qualidade e do suporte oferecido pelo fabricante do hub. A falta de atualizações de firmware frequentes para o hub pode torná-lo uma vulnerabilidade crítica, expondo todos os dispositivos conectados a ameaças.

A literatura reforça essas limitações, especialmente a dependência do fabricante, que pode transformar o hub em um elo crítico caso não receba atualizações regulares.

Os resultados demonstram que a segurança em ambientes de domótica depende não apenas dos equipamentos adotados, mas da forma como são

configurados e integrados. A combinação das duas soluções segmentação da rede e uso de um hub seguro aparece como a abordagem mais robusta entre os estudos analisados, desde que o usuário compreenda suas limitações e mantenha práticas básicas de segurança. Dessa forma, as evidências encontradas sustentam que medidas relativamente simples podem reduzir significativamente os riscos associados à expansão dos dispositivos IoT no ambiente doméstico.

5. CONSIDERAÇÕES FINAIS

As análises realizadas ao longo deste estudo permitiram alcançar o objetivo proposto, que foi identificar as vulnerabilidades predominantes em sistemas de casas inteligentes baseados em IoT e avaliar estratégias de mitigação capazes de reduzir esses riscos no ambiente doméstico. Os resultados confirmam que a inserção de dispositivos inteligentes representa um avanço tecnológico ambíguo: embora ofereçam praticidade e automação, introduzem fragilidades significativas relacionadas ao software embarcado, ao firmware desatualizado e à configuração inadequada das redes às quais estão conectados.

A partir da revisão sistemática, foram identificadas duas soluções amplamente discutidas na literatura e adequadas ao contexto residencial: a segmentação da rede doméstica e o uso de um hub de segurança dedicado. A análise evidenciou que, apesar do potencial de aumentar a proteção contra movimentação lateral de invasores e monitoramento indevido, ambas apresentam limitações importantes, como a complexidade de implementação para usuários sem conhecimento técnico, custos adicionais, dependência do fabricante e risco de criação de pontos únicos de falha.

No entanto, os resultados reforçam que a segurança em sistemas de casas inteligentes depende não apenas da adoção de arquiteturas de proteção, mas também de uma postura proativa do usuário. Medidas como a escolha de fabricantes confiáveis, a atualização regular dos dispositivos, a utilização de senhas fortes e a adoção de autenticação multifator continuam sendo fundamentais para reduzir vulnerabilidades.

Embora este estudo tenha fornecido uma visão consolidada das ameaças e soluções associadas ao uso de dispositivos IoT no ambiente doméstico, reconhece-se como limitação a ausência de testes práticos ou estudos de caso que validem

empiricamente as soluções propostas, uma vez que a análise se baseou exclusivamente em revisão bibliográfica. Dessa forma, pesquisas futuras podem explorar experimentações em ambientes reais, avaliações de desempenho de hubs de segurança, testes comparativos de estratégias de segmentação de rede ou análises longitudinais sobre a evolução das vulnerabilidades em dispositivos IoT.

Conclui-se, portanto, que a construção de um ambiente doméstico seguro exige não apenas boas práticas de configuração, mas também uma postura ativa do usuário e o acompanhamento contínuo da evolução das ameaças. A adoção dessas medidas é essencial para que a tecnologia opere como aliada e não como vetor de risco no cotidiano digital.

6. REFERÊNCIAS

CARRION, P.; QUARESMA, M. **Internet das Coisas (IoT): Definições e aplicabilidade aos usuários finais**. Human Factors in Design, Florianópolis, v. 8, n. 15, p. 49-66, 2019.

CHAHAR, Narendra Kumar. **Computer network security**. International Journal of Innovative Science and Research Technology, v. 7, n. 3, p. 1031–1034, mar. 2022. Disponível em: https://www.researchgate.net/profile/Narendra-Chahar/publication/359876244_Computer_Network_Security/links/625453734f88c3119cf27d84/Computer-Network-Security.pdf. Acesso em: 22 set. 2025.

LIMA, JEFERSON TADEU; PANHAM, ANDRÉ. **Gerenciamento de Riscos em Projetos de Casas Inteligentes-Smart Home**. Revista Científica e-Locução, v. 1, n. 16, p. 40-60, 2019. Disponível em: https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://periodicos.faex.edu.br/index.php/e-Locucao/article/download/213/165&ved=2ahUKEwjtr_bgvsOQAxUELbkGHUJ9DZAQFnoECCQQAQ&usg=AOvVaw00Up60xPUgzSzgUscjyuL2. Acesso em: 13 jun. 2022.

MASSOLA, Silze Cristina; PINTO, Giuliano Scombatti. **O uso da Internet das Coisas (IoT) a favor da saúde**. Revista Interface Tecnológica, v. 15, n. 2, p. 124-137, 2018. Disponível em: https://revista.fatectq.edu.br/interfacetecnologica/pt_BR/article/view/515. Acesso em: 21 set. 2025.

NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR. **Estatísticas do CERT.br apontam aumento de ataques de negação de serviço em 2019**. NIC.br, 27 fev. 2020. Disponível em: https://www.nic.br/noticia/releases/estatisticas-do-cert-br-apontam-aumento-de-ataques-de-negacao-de-servico-em-2019/. Acesso em: 22 set. 2025.

PRATES, Jean Carlos Moreira; SILVA, Alax Gomes da; PICCIN, Mario de Matos; LIMA, Leonardo Sampaio de; FREITAS, Vinicius Nunes de. **O reflexo da pandemia no aumento de incidentes de segurança da informação**. Revista Científica Semana Acadêmica, Fortaleza, v. 10, n. 228, p. 1–19, 2022. DOI: 10.35265/2236-6717-228-12308. Disponível em: https://semanaacademica.org.br/system/files/artigos/40_jean_artigo_semana_academica1_1_0.pdf. Acesso em: 22 set. 2025.

ROCHA, Wesley Sales; ANHESINE, Marcelo Wilson. **Automação residencial por comando de voz**. Revista Interface Tecnológica, v. 17, n. 1, p. 179-191, 2020. Disponível em: https://revista.fatectq.edu.br/interfacetecnologica/pt_BR/article/view/808. Acesso em: 22 set. 2025.

SEN, Ravi. **Challenges to Cybersecurity: Current State of Affairs**. Communications Of The Association For Information Systems, Textas, v. 48, n. 2, p. 1-21, 16 ago. 2018.

SIMPLÍCIO, Paulo Victor Galvão; LIMA, Beatriz Rêgo; SILVA, Givanildo Santos da. **Automação residencial: Uma solução social e econômica**. Caderno de Graduação-Ciências Exatas e Tecnológicas-UNIT-ALAGOAS, v. 4, n. 3, p. 17-24, 2018. Disponível em: https://periodicos.set.edu.br/cdgexatas/article/view/5562. Acesso em: 11 jun. 2022.

STATISTA RESEARCH DEPARTMENT. **Worldwide cybersecurity spending 2017–2021**. Statista, 2022. Disponível em: https://www.statista.com/statistics/991304/worldwide-cybersecurity-spending/. Acesso em: 12 jun. 2022.

TEIXEIRA, Vagner Facini; COSMO, Rafael. **Automação Residencial: uma análise técnica e de investimento**. Revista Esfera Acadêmica Tecnologia, p. 89, 2022. Disponível em: https://multivix.edu.br/wp-content/uploads/2022/02/revista-esfera-tecnologia-v06-n01-artigo05.pdf. Acesso em: 12 jun. 2022.