



UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ
PROGRAMA DE PÓS-GRADUAÇÃO EM COMPUTAÇÃO
MESTRADO EM CIÊNCIA DA COMPUTAÇÃO

RAFAEL FERNANDES VIEIRA

**MEDSTRIDE: UM FRAMEWORK BASEADO EM STRIDE PARA ANÁLISE DE
RISCO EM SISTEMAS MÉDICOS CONECTADOS (IOMT)**

QUIXADÁ
2024

RAFAEL FERNANDES VIEIRA

MEDSTRIDE: UM FRAMEWORK BASEADO EM STRIDE PARA ANÁLISE DE RISCO
EM SISTEMAS MÉDICOS CONECTADOS (IOMT)

Dissertação apresentada ao Curso de Mestrado em Ciência da Computação do Programa de Pós-Graduação em Computação do Campus Quixadá da Universidade Federal do Ceará, como requisito parcial à obtenção do título de mestre em Ciência da Computação. Área de Concentração: Sistemas de Computação.

Orientador: Prof. Dr. Márcio Espíndola Freire Maia.

QUIXADÁ

2024

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Sistema de Bibliotecas
Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

V718m Vieira, Rafael Fernandes.

MEDSTRIDE: Um framework baseado em STRIDE para análise de risco em sistemas médicos conectados (IoMT) / Rafael Fernandes Vieira. – 2024.
112 f. : il. color.

Dissertação (mestrado) – Universidade Federal do Ceará, Campus de Quixadá, Programa de Pós-Graduação em Computação, Quixadá, 2024.

Orientação: Prof. Dr. Márcio Espíndola Freire Maia.

1. Internet das Coisas. 2. Internet das Coisas Médicas. 3. Modelagem de Riscos. 4. STRIDE. I. Título.
CDD 005

RAFAEL FERNANDES VIEIRA

MEDSTRIDE: UM FRAMEWORK BASEADO EM STRIDE PARA ANÁLISE DE RISCO
EM SISTEMAS MÉDICOS CONECTADOS (IOMT)

Dissertação apresentada ao Curso de Mestrado em Ciência da Computação do Programa de Pós-Graduação em Computação do Campus Quixadá da Universidade Federal do Ceará, como requisito parcial à obtenção do título de mestre em Ciência da Computação. Área de Concentração: Sistemas de Computação.

Aprovada em: 29/11/2024

BANCA EXAMINADORA

Prof. Dr. Márcio Espíndola Freire Maia (Orientador)
Universidade Federal do Ceará (UFC)

Prof. Dr. Michel Sales Bonfim
Universidade Federal do Ceará - UFC

Prof. Dr. Marcelo Anderson Batista dos Santos
Instituto Federal Sertão Pernambucano - IFSertãoPE

À minha família, pelo apoio incondicional em todos os momentos e pela compreensão durante minhas ausências. Sem vocês, este caminho não teria sido possível.

AGRADECIMENTOS

A Deus, fonte de sabedoria e força, pois "Dele, por Ele e para Ele são todas as coisas." sem sua graça e direção, este trabalho não seria possível.

À minha esposa Gleiciane e ao meu filho Ravi, pelo amor incondicional, paciência e apoio durante toda essa caminhada. Vocês são meu porto seguro e minha motivação.

À minha família: minha mãe, Luzia Cristina; meu irmão, Rubens; e meus amados avós, Maria de Castro e Raimundo Fernandes (em memória), que sempre acreditaram em mim e me ensinaram o valor do esforço e da dedicação.

Aos meus irmãos em Cristo e amigos, por suas orações, mensagens e palavras de incentivo, que trouxeram conforto e força nos momentos mais desafiadores.

Aos colegas de trabalho Roselina e Julierne, pela generosidade e disposição em me ajudar, mesmo nos momentos mais difíceis. Agradeço por todo o apoio e colaboração ao longo deste percurso.

Ao meu orientador, Prof. Dr. Márcio Maia, por sua orientação, paciência e valiosas contribuições, que foram essenciais para a realização desta dissertação.

Aos colegas da turma de mestrado e aos professores, pela parceria e pela construção de conhecimentos que levarei para a vida toda.

Por fim, dedico meu reconhecimento a cada trabalhador brasileiro que, muitas vezes enfrentando riscos e desafios diários, se levanta para cumprir sua jornada e, através de seus impostos, contribui para o avanço da educação e da ciência em nosso país.

A todos, minha mais profunda gratidão.

RESUMO

A crescente adoção de dispositivos de Internet das Coisas Médicas (IoMT) traz avanços significativos para a área da saúde, mas também amplia a superfície de exposição a ataques cibernéticos. Este trabalho aborda a cibersegurança em IoMT com foco na modelagem de risco. Para isso, foi proposta uma adaptação do *framework* STRIDE, denominada MedSTRIDE, voltada às particularidades de sistemas médicos. A pesquisa inclui uma classificação dos principais tipos de ataques em IoMT identificados na literatura e um modelo genérico de decomposição de componentes de arquitetura, que serve como base para modelagem de risco em diferentes cenários. Além disso, foi realizado um experimento de modelagem comparativo entre o MedSTRIDE e o STRIDE clássico, demonstrando as vantagens da abordagem proposta em capturar riscos específicos de sistemas IoMT. Os resultados confirmam que o MedSTRIDE oferece uma estrutura mais adequada para análise e identificação de vulnerabilidades nesse contexto.

Palavras-chave: internet de coisas médicas; IoMT; vulnerabilidades; riscos; STRIDE; modelagem de risco.

ABSTRACT

The growing adoption of Internet of Medical Things (IoMT) devices brings significant advances to healthcare, but also expands the surface area of exposure to cyberattacks. This work addresses cybersecurity in IoMT with a focus on risk modeling. To this end, an adaptation of the STRIDE *framework* was proposed, called MedSTRIDE, aimed at the particularities of medical systems. The research includes a classification of the main types of IoMT attacks identified in the literature and a generic model for decomposing architectural components, which serves as a basis for risk modeling in different scenarios. Furthermore, a comparative modeling experiment was carried out between MedSTRIDE and classic STRIDE, demonstrating the advantages of the proposed approach in capturing specific risks of IoMT systems. The results confirm that MedSTRIDE offers a more suitable framework for analyzing and identifying vulnerabilities in this context.

Keywords: internet of medical things; IoMT; vulnerabilities; risks; STRIDE; STRIDE-based; threat modeling.

LISTA DE FIGURAS

Figura 1 – Número de equipamentos IoT ligados à Internet.	21
Figura 2 – Arquitetura geral primitiva de quatro camadas.	28
Figura 3 – Composição do risco.	31
Figura 4 – Versões do Wi-Fi, espectros e finalidade.	51
Figura 5 – STRIDE <i>Threat Modeling</i>	56
Figura 6 – Fases do processo de modelagem de risco com STRIDE.	57
Figura 7 – Classificação da Pesquisa.	67
Figura 8 – Fluxograma de execução da pesquisa.	68
Figura 9 – Modelo de rede de IoMT baseado em arquitetura de quatro camadas.	76
Figura 10 – Ativos genéricos para modelagem de risco dos dispositivos da borda de IoMT.	77
Figura 11 – Ativos genéricos para modelagem de risco do dispositivo de coordenação e gerenciamento.	81
Figura 12 – Ativos genéricos para modelagem de risco do <i>gateway</i> médico.	82
Figura 13 – Fases do processo de modelagem com MedSTRIDE.	89
Figura 14 – Bomba de infusão de insulina.	91
Figura 15 – Panorama da arquitetura do sistema de infusão de insulina.	92
Figura 16 – Decomposição dos componentes da arquitetura.	93
Figura 17 – Classificação MedSTRIDE aplicada aos ativos.	94
Figura 18 – Bomba de infusão de medicamentos.	96
Figura 19 – Sistema Lifeview para gerenciamento de bombas de infusão de medicamentos.	97
Figura 20 – Panorama da arquitetura do estudo de caso.	98
Figura 21 – Planilha STRIDE para identificação de vulnerabilidades.	99
Figura 22 – Planilha MedSTRIDE para identificação de vulnerabilidades.	99
Figura 23 – Comparação dos resultados do experimento.	101

LISTA DE TABELAS

Tabela 1 – Características comuns entre modelos de arquiteturas de referência em IoT. .	27
Tabela 2 – Ataques que podem ser empregados em dispositivos com tecnologias <i>Bluetooth</i> . 47	
Tabela 3 – <i>frameworks</i> de modelagem de riscos e seus objetivos.	55
Tabela 4 – Comparação entre propostas para modelagem de risco.	65
Tabela 5 – <i>Strings</i> de busca utilizadas nas bases de dados selecionadas.	69
Tabela 6 – Classificação de ataques IoMT para a propriedade Spoofing.	84
Tabela 7 – Classificação de ataques IoMT para a propriedade Tampering.	85
Tabela 8 – Classificação de ataques IoMT para a propriedade Repudiation.	86
Tabela 9 – Classificação de ataques IoMT para a propriedade Information Disclosure. .	87
Tabela 10 – Classificação de ataques IoMT para a propriedade Denial of Service.	88
Tabela 11 – Classificação de ataques IoMT para a propriedade Elevation of Privilege. . .	89

LISTA DE ABREVIATURAS E SIGLAS

AES	Advanced Encryption Standard
BLE	Bluetooth Low Energy
DFD	Digrama de Fluxo de Dados
DoS	Denial of Service
IoMT	Internet of Medical Things
IoT	Internet of Things
MITM	Man-in-the-Middle
PGC	Protocolos de Gerenciamento de Coisas
UWB	Ultra Wideband
WI-FI	Wireless Fidelity

SUMÁRIO

1	INTRODUÇÃO	14
1.1	Contextualização e caracterização do problemática	14
1.2	Objetivos	16
1.3	Organização do Trabalho	17
2	REFERENCIAL TEÓRICO	18
2.1	Internet das Coisas Médicas	19
2.2	Arquitetura de Referência para IoT	25
2.2.1	<i>Modelo de Rede de IoMT Baseado em Arquitetura de Quatro Camadas . .</i>	26
2.2.1.1	<i>Camada das Física</i>	28
2.2.1.2	<i>Camada de Adaptação</i>	29
2.2.1.3	<i>Camada de Internet</i>	29
2.2.1.4	<i>Camada de Aplicação</i>	30
2.3	Ataques, Ameaças e Vulnerabilidades de Segurança em IoMT	30
2.3.1	<i>Tipos de Ataques Aplicados em Dispositivos IoMT</i>	32
2.3.2	<i>Riscos de Segurança Comuns na Borda da Rede da IoMT</i>	40
2.3.2.1	<i>Riscos de Segurança a Confidencialidade dos Dados</i>	40
2.3.2.2	<i>Riscos de Segurança a Integridade dos Dados</i>	41
2.3.2.3	<i>Riscos de Autenticação Fraca</i>	42
2.3.2.4	<i>Mecanismos de Controle de Acesso e Autorização</i>	43
2.3.2.5	<i>Mecanismo de Criptografia</i>	43
2.3.2.6	<i>Atualização de Firmware</i>	44
2.3.3	<i>Desafios de Comunicação na Camada de Percepção</i>	45
2.3.3.1	<i>Bluetooth</i>	45
2.3.3.2	<i>Bluetooth Low Energy (BLE)</i>	46
2.3.3.3	<i>ZigBee</i>	47
2.3.3.4	<i>Ultra Wideband (UWB)</i>	49
2.3.3.5	<i>Wireless Fidelity (WI-FI)</i>	50
2.3.3.6	<i>WI-FI HaLow</i>	50
2.3.3.7	<i>Ethernet</i>	52
2.4	Modelagem de Risco	53

2.4.1	<i>Frameworks para modelagem de riscos</i>	54
2.4.2	<i>Visão Geral do Processo de Modelagem de Risco e Aplicação do STRIDE</i>	55
2.4.3	<i>Modelagem de riscos em IoMT</i>	58
3	TRABALHOS RELACIONADOS	61
3.1	Levantamento bibliográfico	61
3.2	Avaliação Qualitativa	64
3.2.1	<i>Discussão sobre a relevância dos critérios de avaliação</i>	64
4	METODOLOGIA	67
4.1	Classificação da Pesquisa	67
4.2	Procedimentos de Realização da Pesquisa e Ferramentas Utilizadas	68
5	MEDSTRIDE: UM FRAMEWORK PARA ANÁLISE DE RISCO E PREVENÇÃO DE ATAQUES CIBERNÉTICOS EM SISTEMAS MÉDICOS	72
5.1	O Modelo Proposto	73
5.1.1	<i>Ativos Genéricos Baseados no Modelo de Rede de IoMT</i>	75
5.1.1.1	<i>Generalização de ativos para a camada física</i>	77
5.1.1.2	<i>Generalização de ativos para o dispositivo de coordenação e gerenciamento</i>	78
5.1.1.3	<i>Generalização de ativos para o gateway médico local</i>	80
5.1.2	<i>Classificação STRIDE dos Principais Tipos de Ataques em Sistemas Médicos</i>	83
5.1.2.1	<i>Classificação de ataques IoMT para a propriedade Spoofing</i>	83
5.1.2.2	<i>Classificação de ataques IoMT para a propriedade Tampering</i>	84
5.1.2.3	<i>Classificação de ataques IoMT para a propriedade Repudiation</i>	85
5.1.2.4	<i>Classificação de ataques IoMT para a propriedade Information Disclosure</i>	86
5.1.2.5	<i>Classificação de ataques IoMT para a propriedade Denial of Service</i>	87
5.1.2.6	<i>Classificação de ataques IoMT para a propriedade Elevation of Privilege</i>	88
5.1.3	<i>Fases do Processo de Modelagem com MedSTRIDE</i>	89
5.1.3.1	<i>Identificação dos componentes do sistema</i>	90
5.1.3.2	<i>Criação do panorama da arquitetura</i>	91
5.1.3.3	<i>Decomposição dos componentes da arquitetura</i>	92
5.1.3.4	<i>Aplicação da classificação STRIDE para identificação de vulnerabilidades</i>	93
6	ANÁLISE DOS RESULTADOS E DISCUSSÕES	95
6.1	Apresentação do Estudo de Caso	95

6.2	Execução do Experimento	97
6.3	Discussão dos Resultados e Ameaças a Validade	99
7	CONCLUSÕES E TRABALHOS FUTUROS	103
7.1	Conclusões	103
7.2	Limitações e Trabalhos Futuros	104
	REFERÊNCIAS	106

1 INTRODUÇÃO

Esta dissertação apresenta uma discussão abrangente sobre os riscos, ameaças e vulnerabilidades associados aos dispositivos de Internet das Coisas na área médica, bem como a modelagem de risco aplicada a esses sistemas. Este capítulo aborda, na Seção 1.1, a contextualização e a caracterização da problemática relacionada ao tema. Em seguida, na Seção 1.2, são apresentados os objetivos que impulsionaram a elaboração deste trabalho. Por fim, a Seção 1.3 apresenta a estrutura organizacional desta dissertação.

1.1 Contextualização e caracterização do problemática

A Internet of Medical Things (IoMT) é uma extensão da Internet of Things (IoT) voltada especificamente para o setor da saúde. No contexto da IoMT, dispositivos médicos e equipamentos são conectados à Internet para coletar, transmitir e compartilhar dados relacionados à saúde. Esses dispositivos podem incluir *wearables* (dispositivos vestíveis), sensores, monitores de pacientes, bombas de infusão e uma variedade de outros dispositivos médicos inteligentes.

O objetivo da IoMT é melhorar a eficiência dos cuidados de saúde, reduzir custos, possibilitar o monitoramento remoto de pacientes, facilitar a coleta de dados em tempo real e proporcionar uma gestão mais eficaz dos recursos médicos e hospitalares. Com as tecnologias da IoMT, é possível superar os limites de espaço e tempo nos cuidados médicos, pois, graças a essas inovações, o monitoramento de pacientes em tempo real melhora significativamente o tempo de resposta em situações de emergência. Além disso, os diversos algoritmos de *Machine Learning* (Aprendizado de Máquina) incorporados às diferentes camadas dos sistemas IoMT possibilitam diagnósticos muito mais rápidos e precisos, auxiliando os profissionais da saúde a prescreverem tratamentos adequados para seus pacientes (Yaqoob *et al.*, 2019).

No entanto, como em qualquer setor que lida com informações sensíveis, a segurança e a privacidade dos dados na IoMT são aspectos críticos que devem ser cuidadosamente considerados e gerenciados para garantir o bem-estar dos pacientes e a integridade das informações de saúde. Além disso, o contexto de dispositivos médicos extremamente diversificado e a crescente demanda por dispositivos de saúde tornam os sistemas de cuidados de saúde um campo altamente sensível, devido à alta criticidade em que muitos desses dispositivos operam. Vulnerabilidades de segurança podem não apenas comprometer a privacidade dos pacientes em casos de vazamento de dados, mas também causar sérios prejuízos à saúde, e, em situações

extremas, tais vulnerabilidades podem levar os pacientes a óbito (Ellouze *et al.*, 2013).

O desenvolvimento de software e hardware, de forma geral, sempre foi um trabalho desafiador. Entretanto, a construção de sistemas IoMT eleva ainda mais o nível de complexidade, exigindo um esforço significativo no planejamento e na implementação de soluções médicas. Diversos fatores contribuem para tornar o desenvolvimento de IoMT desafiador, entre os quais se destaca a característica distribuída desses sistemas, que operam em camadas distintas trabalhando de forma colaborativa para prover um serviço comum.

Outro aspecto desafiador na implementação de sistemas IoMT é a heterogeneidade dos diversos dispositivos que operam na camada de percepção (onde se encontram os sensores e atuadores). Essa heterogeneidade decorre das funções específicas desempenhadas por cada dispositivo, manifestando-se na implementação de hardware diversificado e na utilização de uma ampla gama de protocolos, mecanismos de autenticação, autorização e criptografia. Além disso, a constante evolução dessas tecnologias resulta na coexistência de diferentes gerações de dispositivos médicos em um mesmo ambiente. Todas essas características dificultam não apenas a criação e adoção de padrões gerais para a construção de dispositivos médicos, mas também o desenvolvimento de mecanismos de segurança eficientes (Hassan *et al.*, 2019).

Em um contexto onde a implementação de sistemas IoMT já é altamente desafiadora e o ambiente de operação é extremamente crítico, há um agravante ainda maior: a exposição a uma grande quantidade de ameaças, decorrentes de vulnerabilidades e brechas de segurança, tanto conhecidas quanto desconhecidas, presentes nas diversas camadas desses sistemas (Silva *et al.*, 2021).

Diante dos inúmeros desafios enfrentados em sistemas de IoMT, a modelagem de risco surge como uma ferramenta essencial para enfrentar os problemas de segurança. Ao proporcionar uma visão estruturada dos potenciais vetores de ataque e vulnerabilidades, essa abordagem permite que profissionais de segurança da informação antecipem ameaças e implementem medidas preventivas de forma eficiente. Em um ambiente onde a proteção de dados sensíveis e a integridade de dispositivos são cruciais, a modelagem de risco atua como uma aliada indispensável na construção de sistemas mais resilientes e confiáveis (Shostack, 2014; Chantzis *et al.*, 2021).

O modelo STRIDE, amplamente utilizado para a modelagem de riscos em sistemas tradicionais, apresenta uma estrutura consolidada para identificar e classificar ameaças em categorias específicas, como *spoofing*, *tampering*, Denial of Service (DoS), entre outras. Alguns

pesquisadores têm explorado a aplicação do STRIDE no contexto de IoMT, mas essa abordagem enfrenta limitações devido às particularidades dos sistemas médicos, como a interação com o ambiente físico e as restrições de recursos dos dispositivos. Em particular, a camada de percepção e os dispositivos médicos conectados apresentam riscos únicos, como ataques de exaustão energética, interferência eletromagnética, interceptação de dados e manipulação de *firmware*. Apesar da relevância dessas questões, ainda há uma lacuna significativa em diretrizes claras e específicas para modelagem e identificação de riscos em dispositivos IoMT.

Dessa forma, o desenvolvimento de um *framework* que facilite a modelagem de riscos e proponha soluções específicas para a IoMT é de grande importância. A adaptação do modelo STRIDE ao contexto de dispositivos médicos surge como uma resposta a essa necessidade, oferecendo uma abordagem estruturada e acessível para profissionais e pesquisadores da área. Espera-se, como impacto positivo, maior precisão na identificação e compreensão de vulnerabilidades, promovendo a resiliência contra ciberataques, além de garantir a preservação da confidencialidade, da integridade dos dados e da segurança física dos pacientes.

1.2 Objetivos

Esta dissertação de mestrado tem como objetivo geral desenvolver e fornecer uma extensão adaptada do consolidado *framework* STRIDE *Threat Modeling* ao contexto da IoMT. Busca-se elaborar um modelo genérico para decomposição de ativos de componentes da IoMT, abrangendo as camadas física e de adaptação, além de propor uma classificação STRIDE para os ataques mais comuns na IoMT, visando aumentar a precisão e a abrangência na identificação de vulnerabilidades.

- Analisar as características e peculiaridades da IoMT para identificar os principais desafios relacionados à segurança nas camadas física e de adaptação.
- Elaborar um modelo genérico de ativos para a IoMT, descrevendo componentes críticos das camadas física e de adaptação que precisam ser protegidos.
- Classificar os ataques mais comuns na IoMT com base no *framework* STRIDE, associando cada tipo de ataque às suas respectivas categorias de ameaça.
- Validar a extensão proposta do *framework* STRIDE, comparando sua eficácia na identificação de vulnerabilidades em relação ao STRIDE clássico, por meio de estudo de caso real e experimento prático.

Com base no objetivo geral desta dissertação, que é adaptar o *framework* STRIDE

Threat Modeling ao contexto da IoMT, e nos objetivos específicos estabelecidos, surgem questões fundamentais que orientam a pesquisa. Essas questões buscam avaliar a efetividade das propostas desenvolvidas, tanto em termos de modelagem de risco quanto na capacidade de identificar e classificar vulnerabilidades específicas da IoMT.

Assim, para alcançar os objetivos propostos, pretende-se responder às seguintes questões de pesquisa:

- De que forma a decomposição de componentes da arquitetura da IoMT pode influenciar na cobertura e identificação de vulnerabilidades?
- A classificação de ataques em dispositivos IoMT, baseada na adaptação do STRIDE, possibilita uma identificação mais abrangente de vulnerabilidades em comparação ao STRIDE clássico?

1.3 Organização do Trabalho

O restante deste trabalho está organizado da seguinte forma: no Capítulo 2, é apresentada a fundamentação teórica, abordando temas centrais como a IoMT, seus principais desafios, os ataques identificados na literatura e uma discussão sobre modelagem de risco e o *framework* STRIDE. O Capítulo 3 traz uma análise e comparação dos trabalhos relacionados a esta pesquisa. No Capítulo 4, são descritos a metodologia e os métodos utilizados para o desenvolvimento do estudo. O Capítulo 5 apresenta o modelo proposto, juntamente com o método sistemático de modelagem de risco. No Capítulo 6, são discutidos os resultados obtidos, bem como as limitações da pesquisa. Por fim, no Capítulo 7, são apresentadas as conclusões alcançadas e propostas para trabalhos futuros.

2 REFERENCIAL TEÓRICO

A saúde está diretamente relacionada à qualidade de vida de um indivíduo. Segundo a Organização Mundial da Saúde (OMS), o termo “saúde” pode ser definido como “um completo estado de bem-estar físico, mental e social, e não apenas a ausência de doenças e enfermidades”. Manter uma boa saúde é fundamental para que o indivíduo possa viver uma vida plena e satisfatória. Além disso, estar saudável permite que as pessoas realizem suas atividades diárias de forma eficiente, sem se preocupar com limitações físicas ou mentais. Sem dúvida, as tecnologias de IoT estão entre as ferramentas mais importantes e indispensáveis para os cuidados de saúde nos dias de hoje. Graças a essas tecnologias, os procedimentos de diagnóstico, tratamento e monitoramento de pacientes têm sido realizados com muito mais eficácia.

Neste contexto, a segurança dos dispositivos IoT é uma preocupação crucial, pois a integridade e a confidencialidade dos dados são essenciais. Com a crescente adoção de tecnologias de IoT para cuidados de saúde, as vulnerabilidades desses sistemas a ataques cibernéticos podem ter consequências graves, incluindo o comprometimento de informações sensíveis e a interrupção de serviços críticos. A proteção contra essas ameaças exige a implementação de protocolos de segurança robustos, como criptografia de dados, autenticação forte e atualização constante dos sistemas para corrigir falhas e vulnerabilidades. Além disso, a educação e a conscientização dos usuários sobre as melhores práticas de segurança são fundamentais para garantir que os dispositivos IoT operem de maneira segura e eficiente, protegendo tanto os dados dos pacientes quanto a infraestrutura de saúde. A adoção de medidas de segurança eficazes não só preserva a privacidade e a segurança física dos indivíduos, mas também assegura a continuidade e a confiabilidade dos serviços médicos oferecidos, promovendo um ambiente de saúde mais seguro e resiliente.

Neste capítulo, são apresentadas informações gerais sobre o IoMT, incluindo conceitos básicos, o crescimento global da IoT e os investimentos no setor. Além disso, o capítulo discute o potencial da IoMT para os cuidados de saúde e a redução de custos médicos. Também são abordados os riscos e as implicações causadas pelos problemas de segurança desses sistemas.

O panorama geral sobre a arquitetura genérica de quatro camadas para IoT é complementado com uma análise detalhada dos problemas de segurança encontrados nos protocolos usados na camada de percepção e adaptação. Isso inclui desde ataques clássicos, como DoS e injeção de comandos, até ameaças mais sofisticadas, como ataques Man-in-the-Middle (MITM).

O capítulo também discute os 22 tipos de ataques mais comuns em sistemas de IoMT,

como exploração de vulnerabilidades em dispositivos IoMT, sistemas operacionais e dispositivos obsoletos, ataques de desautenticação em dispositivos de comunicação sem fio (por exemplo, Wi-Fi), e exploração de falhas em protocolos de autenticação e criptografia. Esses ataques são analisados em termos de suas potenciais consequências para a integridade dos dados e para a saúde dos pacientes.

Por fim, o capítulo se debruça sobre a modelagem de risco adaptada a IoMT, aplicando o *framework* STRIDE para analisar ameaças e vulnerabilidades nos diferentes componentes do sistema. A adaptação do STRIDE para a IoMT leva em consideração as características específicas dos dispositivos médicos, a heterogeneidade dos sistemas e a necessidade de uma análise contínua e detalhada dos riscos associados. A modelagem de risco permite identificar ativos críticos, mapear ameaças e vulnerabilidades, e definir medidas de mitigação eficazes para garantir a segurança e a integridade dos dados em sistemas de IoMT.

2.1 Internet das Coisas Médicas

Um dispositivo IoT é um objeto físico equipado com tecnologias embarcadas para coletar, processar e transmitir dados. Exemplos de dispositivos IoT incluem sensores, câmeras, televisores, geladeiras, relógios e termostatos. Quando conectados à internet, esses equipamentos são capazes de coletar dados e compartilhá-los com outros dispositivos e sistemas para processamento e análise (Moraes; Hayashi, 2021). A IoT pode ser entendida como um novo paradigma global de comunicação entre objetos, pois a forma como os usuários, dispositivos e objetos físicos do nosso cotidiano interagem mudou drasticamente. A miniaturização dos equipamentos, a expansão das redes de banda larga e o avanço das tecnologias de comunicação sem fio possibilitaram a difusão desse paradigma (Maschietto *et al.*, 2021).

As tecnologias de IoT promoveram uma melhoria significativa na eficiência, segurança e produtividade em uma ampla gama de setores, como saúde, transporte, indústria, agricultura, varejo, entre outros. Os sistemas de IoT realizam a coleta, análise e compartilhamento de grandes quantidades de dados gerados pelos dispositivos conectados. De maneira geral, esses dados são utilizados para a tomada de decisões e para a melhoria dos processos nos diversos setores mencionados. Na saúde, uma das principais aplicações da IoT é a assistência médica remota. A partir das informações capturadas por dispositivos acoplados ou até mesmo implantados no corpo dos pacientes, os médicos conseguem monitorar remotamente dados como pressão arterial, temperatura, batimentos cardíacos, oxigenação, glicose, entre outros. A observa-

ção contínua dos sinais vitais, como frequência cardíaca, pressão arterial e temperatura corporal, pode permitir a detecção precoce de alterações significativas, o que possibilita o acionamento automático de um alerta de emergência e o encaminhamento do paciente a um centro médico adequado (Moraes; Hayashi, 2021; Maschietto *et al.*, 2021).

Existem diversos dispositivos IoMT que atendem a propósitos específicos na área da saúde, desde um simples smartwatch (termo em inglês para relógio inteligente), capaz de monitorar dados como frequência cardíaca, pressão arterial e qualidade do sono, até dispositivos médicos mais sofisticados, como o pacemaker (termo em inglês para marca-passo), utilizado para a manutenção da vida e com a função de regular os batimentos cardíacos do seu usuário (Moraes; Hayashi, 2021).

São diversos os benefícios proporcionados pelo *Health* IoT (terminologia que também é utilizada para designar IoT na saúde), entre os quais podemos destacar o monitoramento remoto de pacientes, a melhoria na precisão dos diagnósticos, a redução de custos, a prevenção de doenças, entre outros (Earle, 2022).

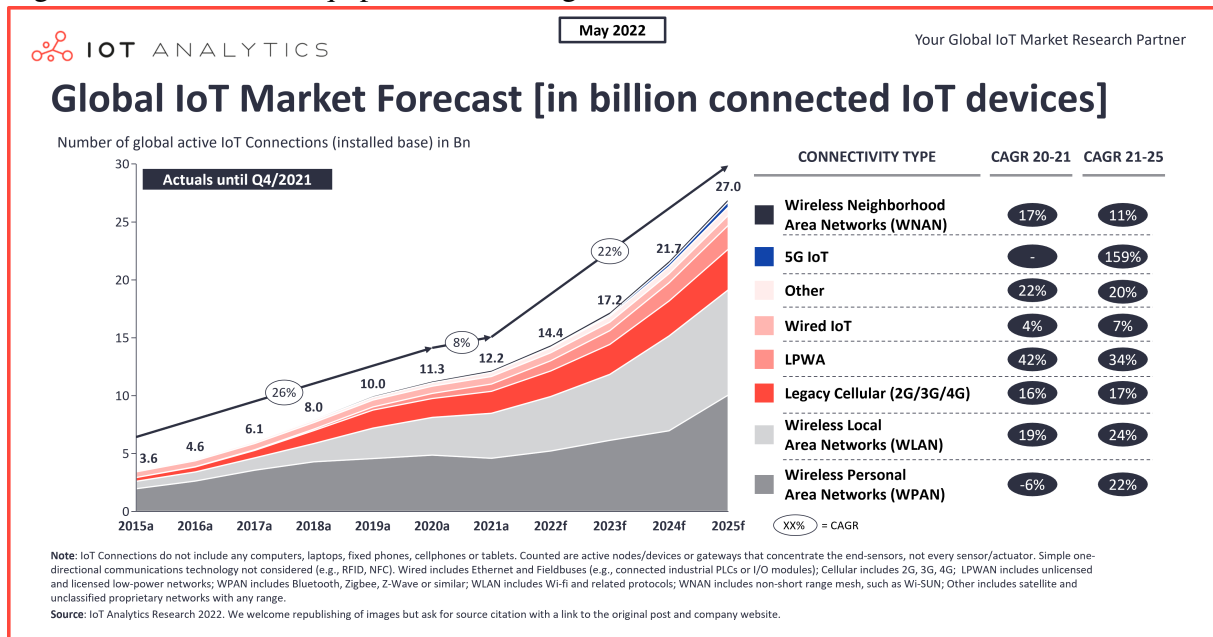
Os dispositivos IoT vêm apresentando um crescimento considerável. Segundo o relatório divulgado em maio de 2022 pela IoT Analytics (Analytics, 2022), o número de dispositivos IoT conectados globalmente atingiu a marca de 12,2 bilhões em 2021. De acordo com o relatório, o aumento percentual em relação ao ano anterior foi de 8%. Estima-se que, até 2027, haverá 27 bilhões de dispositivos IoT ativos.

Como se pode observar na Figura 1, é perceptível uma desaceleração no crescimento do número de dispositivos IoT no período entre 2020 e 2021. Ainda segundo o mesmo relatório da IoT Analytics, esse fenômeno ocorreu devido à escassez global de chips eletrônicos, que afetou o mercado mundial. A escassez foi resultado da crescente demanda por equipamentos eletrônicos durante a pandemia de COVID-19, quando muitas pessoas precisaram trabalhar remotamente. Ao mesmo tempo, diversas fábricas de chips precisaram fechar devido às medidas de contenção do vírus, o que agravou a situação. No entanto, como previsto no relatório de 2022 da IoT Analytics, o crescimento do setor de IoT foi retomado após a pandemia. De acordo com o relatório mais recente divulgado em 2023, o número de dispositivos IoT cresceu 18% em 2022, e as previsões indicam que esse número continuará a crescer, com um aumento de 16% até o final de 2023 (Analytics, 2022; Analytics, 2023).

Outro ponto a ser destacado sobre o mercado global de IoT são os recordes de investimentos de capital de risco em empresas do setor. Segundo o relatório de 2022 da IoT

ANALYTICS, os investimentos feitos por empresas de capital de risco atingiram um número recorde de US\$ 1,2 bilhão no primeiro trimestre de 2022, valor quase quatro vezes maior que o alcançado no mesmo período de 2021, quando a marca foi de US\$ 266 milhões. Isso demonstra o grande potencial transformador das tecnologias IoT e a busca pela eficiência operacional por parte dos diversos setores que as utilizam (Analytics, 2022).

Figura 1 – Número de equipamentos IoT ligados à Internet.



Fonte: IoT Analytics (2022).

A utilização de tecnologias IoMT pode proporcionar cuidados de saúde mais eficazes e colaborar para um maior cumprimento dos tratamentos de longo prazo. Além disso, estima-se que despesas médicas da ordem de 290 bilhões de dólares poderiam ser economizadas anualmente nos Estados Unidos, caso tecnologias IoMT voltadas para o tratamento de condições crônicas, como hipertensão, câncer e HIV, fossem amplamente adotadas (Vodafone, 2017).

A telemedicina refere-se à prática de cuidados médicos realizados a distância, iniciada na década de 1950 em Israel. Atualmente, ela é amplamente utilizada em diversos países, como Estados Unidos, Canadá e várias nações europeias, essa prática relativamente recente pode ter como forte aliada as tecnologias de monitoramento remoto como é o caso de IoMT, proporcionando um acompanhamento ainda mais eficaz. O relatório (BioSpace, 2021) revela que a adoção de dispositivos IoMT em hospitais resulta em maior eficiência no atendimento aos pacientes, além de permitir um melhor monitoramento dos resultados dos tratamentos administrados. O mesmo relatório também destacou que a pandemia de COVID-19 acelerou a adoção da telemedicina, proporcionando resultados satisfatórios. Em virtude disso, espera-se que a prática

conquiste uma significativa participação no mercado global de IoT na área da saúde.

Com o objetivo de prevenir a disseminação de infecções em ambientes hospitalares, a indústria GOJO lançou o GOJO Smartlink, um sistema de monitoramento eletrônico voltado para o controle da higienização das mãos. O sistema Smartlink da GOJO monitora a entrada e saída de pessoas nos quartos dos pacientes, detecta o acionamento de dispensadores de sabão e álcool, além de realizar alertas para a recarga dos dispensadores. Todo o processamento de dados é realizado na nuvem da Microsoft Azure, e o sistema ainda gera relatórios quase em tempo real (Industries, 2017).

Um sistema como o GOJO Smartlink oferece diversos benefícios às unidades de saúde que o utilizam. Além do risco de morte que um paciente pode correr ao contrair uma infecção hospitalar devido à falta de higienização das mãos dos profissionais, a aquisição de uma infecção hospitalar aumenta consideravelmente o tempo de permanência do paciente no ambiente, expondo-o a outras infecções e a riscos de vida. Além disso, os custos hospitalares aumentam significativamente, e, como contrapartida, a oferta de leitos para outros pacientes é reduzida.

A empresa Clean Hands Safe Hands desenvolveu um sistema para monitorar e lembrar os médicos de realizarem a higienização das mãos. O sistema é capaz de medir a taxa de higienização das mãos com precisão, além de emitir lembretes em tempo real para garantir que os médicos não se esqueçam de realizar o procedimento de higienização (Hands, 2018).

Dispositivos inovadores de IoMT têm sido desenvolvidos com o objetivo de proporcionar maior bem-estar aos indivíduos com diabetes tipo 1. Um exemplo disso é o sensor de detecção enzimática da empresa Noviosense. Esse sensor, que possui cerca de 2 cm de comprimento e 1,5 mm de diâmetro, foi projetado para ser colocado no olho de pessoas com diabetes. Seu formato é semelhante a uma mola, permitindo que se ajuste aos diversos formatos do olho humano. O sensor possui um revestimento de biopolímero em seus eletrodos, material que contém uma enzima que reage à presença de glicose nas lágrimas. De acordo com um experimento realizado com um grupo de 24 pessoas, o sensor da Noviosense, aliado a um algoritmo de regressão por rede neural (usado para converter dados de glicose lacrimal em dados equivalentes a glicose sanguínea), demonstrou ser possível obter resultados comparáveis aos obtidos por glicosímetros convencionais, que exigem perfurações nos dedos do paciente diariamente (Geelhoed-Duijvestijn *et al.*, 2020).

Em 2022, um grupo de pesquisadores realizou um estudo com jovens menores

de 15 anos, todos portadores de diabetes tipo 1. O objetivo do estudo foi testar o sistema MiniMed 780G. Este sistema conta com uma bomba de insulina avançada, capaz de monitorar de forma autônoma os níveis de glicose e enviar sinais para a bomba de insulina, de modo a estabilizar os níveis glicêmicos. O experimento contou com a participação de 12.870 pessoas. Com os resultados obtidos, foi possível constatar a eficácia do sistema, que atingiu o controle glicêmico esperado. Cerca de 75% dos participantes mantiveram seus níveis glicêmicos dentro das diretrizes estabelecidas pelo consenso internacional (Arrieta *et al.*, 2022).

A empresa *Dai Viet Controls and Instrumentation Company* (Daviteq) desenvolveu um sistema baseado em IoT para o monitoramento da temperatura em gabinetes de conservação de vacinas. Os sensores de temperatura utilizam tecnologia de comunicação sem fio e transmitem os dados para a nuvem. Enquanto isso, a equipe responsável pelo mantimento e controle dessas vacinas pode monitorá-las por meio de um smartphone ou tablet. Com a solução da Daviteq, é possível realizar o monitoramento contínuo em tempo real. O sistema faz chamadas de emergência, envia SMS ou e-mails para os responsáveis pelo estoque sempre que há problemas com o armazenamento das vacinas. Essa tecnologia garante maior qualidade às vacinas oferecidas e evita prejuízos e perdas (Daviteq,).

Uma dupla de pesquisadores desenvolveu um sistema baseado em IoT e Machine Learning (ML), que também é capaz de monitorar e controlar o armazenamento de vacinas. O sistema conta com um algoritmo de regressão linear que realiza previsões de temperatura para os próximos 20 minutos. Além disso, ele possui um alarme e uma luz indicadora, e ainda dispara mensagens de alerta caso detecte anomalias na temperatura do ambiente (Jain; Gawre, 2022).

Um grupo de pesquisadores desenvolveu um sistema chamado Vita-H1, que realiza o monitoramento da pressão arterial por meio de sinais de EEG e PPG. O dispositivo Vita-H1 é capaz de realizar a medição contínua da pressão arterial dos pacientes, algo que não seria viável com dispositivos convencionais, como esfigmomanômetro ou aparelhos digitais tradicionais (Lu *et al.*, 2017).

Os dispositivos IoMT conectados à internet podem ser configurados, operados e monitorados remotamente. Essas tecnologias desempenham suas funções primárias e geram dados que são transmitidos pela rede. Os sistemas que coletam esses dados, processam e geram relatórios médicos são fundamentais para diagnosticar pacientes, definir tratamentos e/ou realizar ações rápidas. De maneira geral, as unidades de saúde que utilizam dispositivos IoMT enfrentam diversos desafios para se proteger contra ameaças cibernéticas, pois, em muitos casos,

a interrupção dos serviços providos pelos sistemas médicos poderia provocar consequências graves, ou até mesmo irreversíveis, aos pacientes (Yaqoob *et al.*, 2019).

Os inúmeros benefícios do IoMT, como o monitoramento de doenças, o acompanhamento remoto de pacientes, a obtenção de diagnósticos rápidos, maior disponibilidade de serviços e a redução de custos para pacientes e unidades hospitalares, têm incentivado a indústria da saúde a considerar favoravelmente a adoção de tecnologias voltadas para o cuidado da saúde. No entanto, apesar dos muitos benefícios, a adoção do IoMT ainda enfrenta dificuldades, pois tanto médicos quanto pacientes temem por sua privacidade e segurança (Pulse, 2023).

Em 2016, Jay Radcliffe, pesquisador da Rapid7, revelou vulnerabilidades críticas na bomba de insulina da *Animas Corporation*, destacando riscos significativos à segurança dos pacientes. A primeira vulnerabilidade (CVE-2016-5084) envolvia a transmissão de dados sensíveis, como níveis de glicose e dosagens de insulina, em texto claro, o que os expunha a interceptações durante a comunicação entre o controle remoto e a bomba. A segunda vulnerabilidade (CVE-2016-5085) estava relacionada a um processo de emparelhamento fraco, no qual os dispositivos trocavam números de série e geravam uma chave CRC32, também transmitida sem criptografia. Essa falha permitia que atacantes falsificassem comandos, possibilitando a administração remota e não autorizada de insulina. A terceira vulnerabilidade (CVE-2016-5086) dizia respeito à ausência de mecanismos de defesa contra ataques de repetição, permitindo que invasores retransmitissem comandos previamente capturados, resultando na administração não intencional de insulina e aumentando o risco de hipoglicemia (Beardsley, 2016)

Em 2021, o *Ponemon Institute* conduziu uma pesquisa, divulgada em relatório, com a participação de 597 (quinhentos e noventa e sete) profissionais de tecnologia da informação (TI) e segurança da informação, que trabalham diretamente em organizações de prestação de cuidados de saúde. De acordo com o relatório, 43% dos profissionais entrevistados afirmaram ter sofrido ataques de *ransomware* em suas organizações. O estudo também apontou um impacto negativo significativo no atendimento aos pacientes, como o aumento no tempo de internação, atrasos em procedimentos, complicações durante os procedimentos realizados e um aumento de 22% na taxa de mortalidade dos pacientes (Institute, 2021).

Em setembro de 2022, a divisão de *cyber* segurança do FBI divulgou um relatório sobre o risco que dispositivos médicos desatualizados podem causar aos seus utilizadores. O relatório mostra que a grande maioria dos dispositivos IoMT são dispositivos de longa vida, os problemas de dispositivos de longa vida está principalmente na falta de atualização, outro fator

que devemos considerar são dispositivos mais antigos e com tecnologias de geração anterior coexistindo com dispositivos modernos em uma mesma rede, a falta de atualização possibilita a exploração de falhas tanto na construção do hardware como também no *firmware* do dispositivos, o relatório desta ainda que em janeiro do mesmo ano, foi conduzida uma investigação que constatou que 53% dos dispositivos médicos ativos continham vulnerabilidades conhecidas (Division, 2022).

Em março de 2019, pesquisadores da *Clever Security* identificaram falhas graves nos desfibriladores cardíacos fabricados pela empresa Medtronic. Esses dispositivos, implantados cirurgicamente nos pacientes, têm a função de aplicar choques elétricos no coração para restabelecer o ritmo cardíaco. De acordo com uma nota emitida pelo departamento de segurança interna dos Estados Unidos, as falhas encontradas nos dispositivos permitiriam que um atacante assumisse total controle, colocando em risco a vida dos pacientes (Khandelwal, 2019).

2.2 Arquitetura de Referência para IoT

Um dos maiores desafios no desenvolvimento de soluções para IoT é a falta de padrões gerais. Isso ocorre devido à heterogeneidade de dispositivos, protocolos e tecnologias de comunicação que coexistem em um mesmo sistema IoT. Além disso, cada uma das diversas áreas de aplicação de IoT possui suas próprias especificidades de construção, o que dificulta ainda mais a adoção de padrões gerais. Ao contrário de outros ramos da ciência da computação, essa heterogeneidade de tecnologias dificulta a criação de padrões gerais adequados para os diferentes casos de uso de IoT (Sun *et al.*, 2019).

A demanda do mercado e a alta concorrência entre empresas de IoT são fatores que levam à entrega de novos dispositivos e sistemas sem o devido processo que garantiria a qualidade e a segurança dos serviços por eles oferecidos. Outro ponto importante a destacar é que, em muitos países, ainda não existem restrições legais ou diretrizes claras para o desenvolvimento de novos dispositivos e sistemas, o que pode acarretar sérios problemas relacionados à segurança e à privacidade dos usuários. Além disso, é essencial ressaltar que aspectos como segurança e qualidade desses dispositivos são fundamentais para que os usuários tenham confiança e continuem adotando essas tecnologias. Em IoT, novos protocolos e padrões surgem constantemente, enquanto outras tecnologias se tornam obsoletas rapidamente. Isso aumenta a heterogeneidade e faz com que dispositivos legados coexistam com dispositivos novos, criando desafios relacionados à segurança, integração e manutenção dos sistemas (Analytics, 2022;

Maschietto *et al.*, 2021; Yaqoob *et al.*, 2019; Yaacoub *et al.*, 2020).

Devido aos diversos desafios enfrentados no desenvolvimento de sistemas IoT, muitas empresas e pesquisadores têm direcionado esforços para a criação de novas arquiteturas de referência. Em alguns casos, essas arquiteturas acabam se tornando padrões de construção para novos sistemas. De maneira geral, o objetivo dessas arquiteturas é resolver problemas de interoperabilidade, identificar ameaças, promover padronização e acelerar o desenvolvimento de sistemas mais confiáveis.

Uma arquitetura de referência para IoT é um modelo conceitual que define os componentes, as camadas e as relações entre eles, oferecendo uma estrutura para o *design* e a implementação de sistemas IoT. Essa arquitetura fornece diretrizes e melhores práticas para o desenvolvimento de soluções IoT, com foco na interoperabilidade, segurança e escalabilidade. Embora não seja uma implementação específica, a arquitetura de referência atua como um guia abstrato que pode ser adaptado e estendido para atender aos requisitos específicos de diferentes soluções, possibilitando a construção de sistemas IoT mais robustos, seguros, interoperáveis e padronizados (Martino *et al.*, 2018; Chowdhury *et al.*, 2015).

A Tabela 1 apresenta as características comuns entre modelos de arquiteturas de referência em IoT. Esses modelos incluem camadas hierárquicas, que organizam a arquitetura em níveis específicos, como borda, conectividade e processamento em nuvem. Os dispositivos de borda são responsáveis pela percepção do ambiente, coletando dados e executando ações baseadas em comandos. A conectividade trata da comunicação e transferência de dados entre dispositivos e a nuvem, empregando protocolos e tecnologias de rede. O processamento em nuvem possibilita o armazenamento e a análise dos dados coletados, utilizando infraestrutura em nuvem. Aplicações e serviços representam as interfaces e relatórios usados pelos usuários para interagir com os dispositivos IoT. A segurança é uma preocupação central, abrangendo medidas para proteger a integridade, confidencialidade e disponibilidade dos dados, especialmente em dispositivos médicos. O gerenciamento de dispositivos inclui registro, configuração e manutenção, enquanto padrões e protocolos garantem a interoperabilidade entre dispositivos e sistemas.

2.2.1 Modelo de Rede de IoMT Baseado em Arquitetura de Quatro Camadas

As diversas aplicações de IoT, como na indústria, saúde, agricultura e casas inteligentes, possuem características específicas que tornam inviável a adoção de um único modelo de arquitetura de referência como padrão de mercado. Além disso, pesquisadores, empresas e

Tabela 1 – Características comuns entre modelos de arquiteturas de referência em IoT.

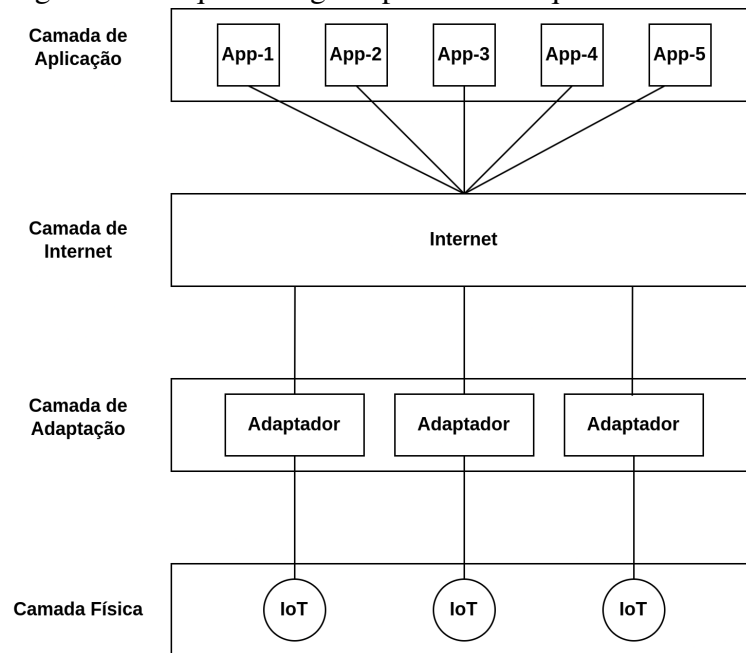
Característica Comum	Descrição
Possui Camadas Hierárquicas	A arquitetura é frequentemente organizada em camadas, cada uma desempenhando suas responsabilidades específicas. Exemplos de camadas podem incluir dispositivos de borda, conectividade, processamento em nuvem e aplicativos.
Dispositivos de Borda (<i>Edge Devices</i>)	Incluem sensores e atuadores. Esses dispositivos são responsáveis pela percepção do sistema, como por exemplo a coleta de dados de temperatura corporal, eles também podem realizar ações baseadas em comandos, como por exemplo um dispensador de medicamentos que disponibiliza a droga correta em horários específicos.
Conectividade	Gerencia a comunicação entre dispositivos e a transferência de dados para a nuvem. Pode envolver protocolos de comunicação, <i>gateways</i> e tecnologias de rede.
Processamento em Nuvem (<i>Cloud Processing</i>)	Envolve o armazenamento e o processamento de dados, para isso utiliza-se de serviços de infraestrutura em nuvem para computação.
Aplicações e Serviços	Representa as interfaces de usuário, <i>dashboards</i> , relatórios e aplicativos que interagem com os dados coletados pelos dispositivos IoT.
Segurança	Inclui medidas de segurança em todas as camadas, protegendo a integridade, confidencialidade e disponibilidade dos dados, além disso, em IoMT é necessário garantir a segurança e a integridade física dos utilizadores de dispositivos necessários para manutenção da vida.
Gerenciamento de Dispositivos	Trata do registro, configuração e manutenção dos dispositivos IoT.
Padrões e Protocolos	Define os padrões e protocolos recomendados para garantir a interoperabilidade entre os dispositivos e sistemas.

Fonte: Elaborada pelo autor.

organizações de padronização propõem uma variedade de modelos de referência, que vão desde modelos genéricos primitivos até aqueles mais específicos para aplicações em áreas como a saúde, exemplificado pelo modelo de telemedicina do ITU-T. Esta diversidade de abordagens reflete a complexidade e a heterogeneidade das aplicações IoT, o que torna desafiador o estabelecimento de um padrão único e universal (Maschietto *et al.*, 2021).

A Figura 2 apresenta o modelo de arquitetura IoT em quatro camadas descrito por (Chowdhury *et al.*, 2015), esse modelo organiza suas funções em níveis hierárquicos, cada um com responsabilidades específicas para permitir a integração de dispositivos e sistemas no ecossistema IoT.

Figura 2 – Arquitetura geral primitiva de quatro camadas.



Fonte: (Chowdhury *et al.*, 2015).

2.2.1.1 Camada das Física

A Camada Física é onde se localizam os sensores, atuadores e dispositivos responsáveis por interagir com o mundo físico. No contexto de IoMT, essa camada inclui uma vasta gama de equipamentos, como, por exemplo, marcapassos cardíacos, desfibriladores cardíacos, dispensadores de medicamentos, bombas de insulina, pulseiras inteligentes, ressonâncias magnéticas, entre outros.

Os dispositivos dessa camada são comumente classificados em três tipos: sensores implantáveis, sensores vestíveis e equipamentos locais. Os sensores implantáveis são mais invasivos, pois são inseridos no corpo do paciente por meio de cirurgia, entrando em contato direto com tecidos e fluidos corporais. Já os sensores vestíveis ficam em contato direto com a pele ou sobre o corpo do paciente. Por fim, os equipamentos locais são instalados e utilizados diretamente no estabelecimento de saúde ou no local de tratamento médico, como máquinas de hemodiálise, ultrassons, ventiladores mecânicos e equipamentos de monitoramento cardíaco.

Os dispositivos médicos apresentam características distintas em suas composições física, lógica, mecânica e elétrica, além de variações no uso de protocolos e tecnologias de comunicação. Entre as tecnologias mais comuns, destacam-se aquelas de curto alcance, como Bluetooth Low Energy (BLE), ZigBee, WPAN de baixa potência, Wi-Fi, Bluetooth, Ethernet, entre outras, que são empregadas para transmitir as informações detectadas aos *gateways* (Camada

de Adaptação) (Yaqoob *et al.*, 2019; Sun *et al.*, 2019; Yaacoub *et al.*, 2020; Chowdhury *et al.*, 2015; Papaioannou *et al.*, 2022).

2.2.1.2 *Camada de Adaptação*

A Camada de Adaptação é composta por um ou mais adaptadores (também chamados de *gateways*), cuja principal função é atuar como uma espécie de tradutor entre a Camada de Percepção e as camadas superiores do sistema. Devido à alta heterogeneidade dos sistemas IoT, é essencial que os adaptadores sejam capazes de lidar com os diversos protocolos utilizados na borda da rede e converter os diferentes formatos de dados gerados pelos dispositivos para um formato padrão compreensível pela Camada de Aplicação. Em resumo, os adaptadores dessa camada são responsáveis por facilitar a comunicação e a interoperabilidade entre dispositivos, sistemas de gerenciamento e aplicações. Além disso, serviços como filtragem, processamento, agregação de dados e segurança podem ser oferecidos por esta camada. A proximidade dessa camada com as equipes médicas também permite o acesso rápido a relatórios e informações em tempo real, facilitando a tomada de decisões mais ágil e eficiente (Yaqoob *et al.*, 2019; Sun *et al.*, 2019; Yaacoub *et al.*, 2020; Chowdhury *et al.*, 2015; Papaioannou *et al.*, 2022).

A comunicação entre essas camadas é realizada por meio de protocolos de comunicação padrão, como MQTT, CoAP, HTTP, e outros. Além disso, muitos sistemas de IoMT fazem uso de protocolos proprietários para a comunicação entre dispositivos e adaptadores, os quais são conhecidos como Protocolos de Gerenciamento de Coisas (PGC). A principal função desses protocolos na arquitetura é permitir a troca de informações entre dispositivos, entre dispositivos e aplicativos IoMT, e entre aplicativos IoMT (Maschietto *et al.*, 2021).

2.2.1.3 *Camada de Internet*

Um dos principais papéis da Camada de Internet é fornecer a infraestrutura necessária para a transmissão de dados entre a Camada de Adaptação e a Camada de Aplicação. Essa infraestrutura inclui redes locais, softwares de sistema, protocolos abertos e a própria infraestrutura fornecida pela Internet (Chowdhury *et al.*, 2015).

2.2.1.4 Camada de Aplicação

O papel da Camada de Aplicação é fornecer as aplicações necessárias para o controle e monitoramento dos diversos dispositivos médicos, além de oferecer outros serviços de valor agregado. É importante destacar que essa camada também precisa compreender os PGC, pois, dependendo dos requisitos da aplicação, pode ser necessário implementar *middlewares* para facilitar a comunicação e a gestão dos diferentes componentes do sistema (Yaqoob *et al.*, 2019; Sun *et al.*, 2019; Yaacoub *et al.*, 2020; Chowdhury *et al.*, 2015; Papaioannou *et al.*, 2022).

2.3 Ataques, Ameaças e Vulnerabilidades de Segurança em IoMT

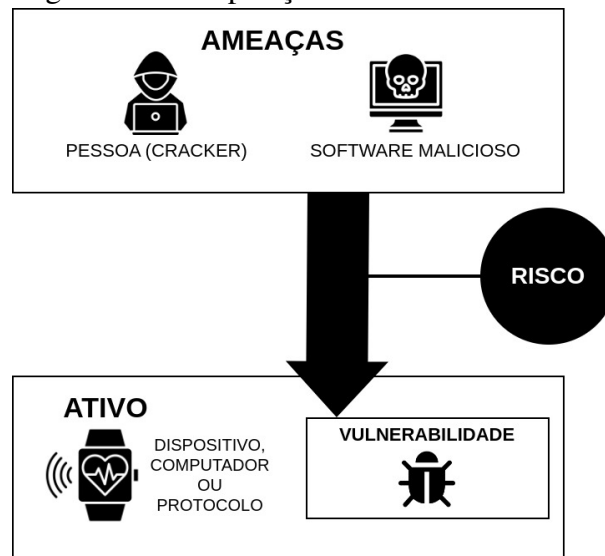
O termo “vulnerabilidade” refere-se, de forma geral, a uma condição de fraqueza presente em algo ou alguém. No contexto da computação, vulnerabilidade é entendida como um defeito ou fragilidade que permite a um invasor contornar medidas de segurança (Jr. *et al.*, 1990). Conforme definido por (Branquinho; Branquinho, 2021), vulnerabilidade é um ponto de fragilidade em um ativo, sendo que um ativo pode ser um computador, protocolo, software, dispositivo ou até mesmo uma pessoa envolvida em um processo.

Além disso, como ilustrado na Figura 3, o risco é resultante da convergência entre uma ameaça e uma vulnerabilidade. A ameaça pode se manifestar na forma de um atacante (cracker) ou de software malicioso que explora a vulnerabilidade encontrada. Quando o risco é concretizado, ou seja, quando a ameaça obtém sucesso na exploração da vulnerabilidade, podem ocorrer impactos potenciais, como vazamento de dados, interrupção de serviços, adulteração de informações, entre outros.

O ecossistema de IoMT é geralmente composto por uma ampla gama de componentes, incluindo dispositivos e sensores integrados, aplicativos móveis, infraestrutura baseada em nuvem e uma diversidade de protocolos de comunicação de rede. Entre esses protocolos, destacam-se os utilizados na pilha TCP/IP, além de tecnologias específicas para comunicação sem fio.

Protocolos de curto alcance incluem NFC, RFID, Bluetooth e Bluetooth Low Energy (BLE). Para comunicações de médio alcance, são amplamente utilizados o Wi-Fi, Wi-Fi Direct e Zigbee. Já para conectividade de longo alcance, destacam-se LoRa, LoRaWAN e Sigfox, que são amplamente adotados em cenários onde a comunicação à distância e o baixo consumo de energia são requisitos essenciais (Yaqoob *et al.*, 2019; Chantzis *et al.*, 2021).

Figura 3 – Composição do risco.



Fonte: Elaborada pelo autor.

A segurança em sistemas de computação tradicionais sempre representou um grande desafio para especialistas em cibersegurança e desenvolvedores. No contexto da Internet das Coisas Médicas (IoMT), esses desafios são ainda maiores devido à natureza diversificada e altamente interconectada dos dispositivos médicos. A heterogeneidade dos sistemas médicos torna sua construção extremamente complexa e difícil de testar de maneira abrangente.

Diferentemente dos testes de segurança convencionais, a avaliação de dispositivos IoMT exige abordagens específicas, como a inspeção detalhada e, em muitos casos, a desmontagem do hardware. Adicionalmente, é necessário lidar com protocolos de rede especializados, analisar os aplicativos móveis que controlam os dispositivos e examinar como esses sistemas interagem com serviços web e APIs em infraestrutura de nuvem (Chantzis *et al.*, 2021).

Os dispositivos médicos implantados de uso crítico, como marca-passos e desfibriladores cardíacos, demandam funcionamento contínuo e ininterrupto. Essa característica os torna ainda mais suscetíveis a tentativas de violação em diversas superfícies de ataque. Quando vulnerabilidades são descobertas e exploradas nesses dispositivos, os impactos podem ser significativamente mais graves do que em sistemas tradicionais. Além de comprometer a integridade dos dados e causar vazamento de informações, ataques direcionados a esses dispositivos podem resultar em danos severos à saúde ou até na perda de vidas humanas.

Diante disso, é essencial implementar estratégias robustas de segurança para proteger os sistemas médicos, com especial atenção aos dispositivos de uso crítico. O cenário desafiador exige inovações constantes e abordagens proativas para mitigar ameaças e garantir a confiabilidade desses sistemas na era das coisas conectadas (Hassan *et al.*, 2019; Moraes; Hayashi, 2021;

Yaqoob *et al.*, 2019; Chantzis *et al.*, 2021).

2.3.1 Tipos de Ataques Aplicados em Dispositivos IoMT

As ameaças a dispositivos médicos abrangem os aspectos de Confidencialidade, Integridade, Disponibilidade, Autenticação, Autorização e Não-repúdio:

- **Confidencialidade:** ocorre quando informações sensíveis são acessadas de forma não autorizada, expondo dados confidenciais de pacientes ou sistemas médicos.
- **Integridade:** envolve a alteração indevida de informações, comprometendo a precisão e a confiabilidade dos dados transmitidos ou armazenados.
- **Disponibilidade:** ataques, como a negação de serviço (DoS), têm como objetivo impedir o acesso legítimo a sistemas e dispositivos médicos, interrompendo operações críticas.
- **Autenticação:** falhas nesse aspecto permitem que atacantes se apresentem como entidades legítimas, obtendo acesso indevido aos dispositivos ou sistemas.
- **Autorização:** ameaças nesse domínio surgem quando acessos não autorizados a recursos e funcionalidades são permitidos, muitas vezes devido à ausência de controles adequados.
- **Não-repúdio:** a falta de mecanismos que garantam a rastreabilidade das ações dificulta a identificação de autores de atividades maliciosas, comprometendo a responsabilização.

Essas vulnerabilidades geralmente resultam de falhas em protocolos de comunicação, problemas de design em software e medidas de segurança inadequadas no desenvolvimento dos dispositivos médicos. A mitigação dessas ameaças requer um planejamento robusto de segurança que aborde todos esses aspectos de forma integrada.

A seguir, são apresentados os principais tipos de ataques direcionados as camadas física e adaptação de sistemas médicos conectados. Cada item inclui uma descrição detalhada do ataque e as possíveis consequências decorrentes da exploração dessas vulnerabilidades:

1. *Firmware Modification Attack:* O ataque de modificação de firmware é uma ameaça crítica à segurança dos dispositivos médicos, uma vez que envolve a alteração maliciosa do software embarcado que controla o funcionamento desses dispositivos. O firmware, sendo um componente de software de baixo nível, gerencia diretamente os recursos de hardware do dispositivo e garante a execução correta das funcionalidades previstas. Através desse tipo de ataque, um adversário pode introduzir código malicioso no firmware, possibilitando o controle remoto do dispositivo, a modificação dos dados coletados ou transmitidos, e até mesmo a desativação completa do equipamento. Esse comprometimento pode resultar

em consequências graves, incluindo falhas operacionais, exposição de dados sensíveis dos pacientes e a potencial ameaça à vida dos usuários dos dispositivos médicos (Yaqoob *et al.*, 2019; Papaioannou *et al.*, 2022; Rasool *et al.*, 2022).

2. *Eavesdropping*: O ataque de eavesdropping, ou interceptação de comunicação, constitui uma séria ameaça à segurança e privacidade dos dispositivos médicos conectados. Este tipo de ataque envolve a escuta clandestina e não autorizada das comunicações entre dispositivos médicos, servidores, ou redes. Utilizando técnicas de eavesdropping, um adversário pode capturar e analisar dados sensíveis transmitidos, como informações pessoais de saúde dos pacientes, comandos de controle dos dispositivos ou dados de monitoramento. A interceptação de tais informações pode levar à exposição de dados confidenciais, possibilitando ataques subsequentes, como a falsificação de dados ou a engenharia social. Além disso, a manipulação de informações críticas pode comprometer a integridade e a eficácia dos tratamentos médicos administrados (Yaqoob *et al.*, 2019; Hasan *et al.*, 2022; Yaacoub *et al.*, 2020; Papaioannou *et al.*, 2022; Rasool *et al.*, 2022).
3. *Sniffing*: O ataque de sniffing, conhecido também como farejamento de rede, é uma ameaça significativa à segurança dos dispositivos médicos interconectados. Este ataque envolve a captura passiva e não autorizada de dados que trafegam na rede, permitindo que um atacante monitore e registre informações transmitidas entre dispositivos médicos, servidores, ou redes de comunicação. Utilizando ferramentas de sniffing, o adversário pode interceptar e analisar pacotes de dados, obtendo acesso a informações sensíveis, como credenciais de autenticação, dados pessoais de saúde dos pacientes, e comandos de controle dos dispositivos. A exposição desses dados pode resultar em uma série de consequências adversas, incluindo a violação de privacidade, a manipulação maliciosa de dados, e a execução de ações não autorizadas nos dispositivos médicos (Yaqoob *et al.*, 2019; Yaacoub *et al.*, 2020, 2020; Rasool *et al.*, 2022).
4. *Information Disclosure*: O ataque de divulgação de informações representa uma séria ameaça à confidencialidade e integridade dos dados em dispositivos médicos conectados. Este tipo de ataque ocorre quando informações sensíveis, como dados pessoais de saúde dos pacientes, detalhes de tratamento, ou configurações de dispositivos, são expostas a partes não autorizadas. A divulgação de informações pode resultar de vulnerabilidades em sistemas de segurança, como configurações inadequadas de acesso, falhas em protocolos de comunicação, ou brechas de segurança não corrigidas. Quando um adversário obtém

acesso a essas informações, há um risco elevado de uso indevido dos dados, que pode levar à violação de privacidade dos pacientes, comprometimento da integridade dos tratamentos médicos, e potencial manipulação dos dispositivos para fins maliciosos (Yaqoob *et al.*, 2019; Hasan *et al.*, 2022; Yaacoub *et al.*, 2020; Papaioannou *et al.*, 2022; Rasool *et al.*, 2022).

5. *Man In The Middle*: O ataque Man-In-The-Middle (MITM) é uma ameaça sofisticada à segurança dos dispositivos médicos, onde um adversário intercepta e possivelmente altera a comunicação entre duas partes que acreditam estar se comunicando diretamente uma com a outra. No contexto dos dispositivos médicos, um ataque MITM pode permitir que o invasor capture dados sensíveis transmitidos entre dispositivos, servidores e redes, incluindo informações de saúde dos pacientes, comandos de controle, e configurações do dispositivo. O adversário pode também modificar essas comunicações, inserindo dados falsificados ou alterando os comandos enviados aos dispositivos médicos, potencialmente causando mau funcionamento ou comprometendo a integridade do tratamento administrado. As consequências de um ataque MITM em dispositivos médicos podem ser severas, incluindo a violação da privacidade do paciente, a falsificação de registros médicos, e a interrupção de terapias críticas (Yaqoob *et al.*, 2019; Yaacoub *et al.*, 2020; Papaioannou *et al.*, 2022; Rasool *et al.*, 2022).
6. *Unauthorized Access*: O acesso não autorizado ocorre quando indivíduos ou entidades sem permissões apropriadas obtêm acesso a sistemas, redes ou dados dos dispositivos médicos. Este tipo de ataque pode resultar da exploração de vulnerabilidades de software, credenciais fracas, ou falta de controles de acesso rigorosos. Uma vez que o atacante obtém acesso, ele pode visualizar, modificar ou excluir dados sensíveis, alterar configurações dos dispositivos, ou interromper os serviços, colocando em risco a saúde e a segurança dos pacientes (Yaqoob *et al.*, 2019; Rasool *et al.*, 2022).
7. *Spoofing*: O ataque de spoofing envolve a falsificação de identidade, onde o atacante se faz passar por uma entidade legítima para ganhar acesso a sistemas ou dados. Em dispositivos médicos, spoofing pode ser usado para enganar os sistemas de autenticação e controle, permitindo ao atacante enviar comandos maliciosos ou interceptar dados sem ser detectado. Um exemplo comum é o spoofing de endereço IP ou MAC, onde o invasor manipula pacotes de rede para parecer que estão vindo de uma fonte confiável. Consequências podem incluir a manipulação de dados de monitoramento de pacientes, envio de comandos

errados para dispositivos terapêuticos, e a violação de privacidade de dados médicos (Yaqoob *et al.*, 2019; Yaacoub *et al.*, 2020; Papaioannou *et al.*, 2022; Rasool *et al.*, 2022).

8. *Replay Attack*: O ataque de replay (ou ataque de repetição) é uma ameaça à segurança dos dispositivos médicos que envolve a interceptação e retransmissão de mensagens válidas e autenticadas para enganar o sistema e realizar ações não autorizadas. No contexto dos dispositivos médicos, um atacante pode capturar pacotes de dados ou comandos legítimos transmitidos entre dispositivos e servidores, e posteriormente retransmiti-los para executar operações fraudulentas ou comprometer o funcionamento do sistema. Em um replay attack, o invasor intercepta comunicações legítimas e as reapresenta como se fossem novas, aproveitando a falta de mecanismos de proteção contra a repetição de mensagens. Isso pode levar a ações indesejadas, como a reinicialização não autorizada de dispositivos, a repetição de comandos críticos ou a execução de operações fraudulentas que afetam a integridade dos dados e a segurança dos pacientes (Yaqoob *et al.*, 2019; Yaacoub *et al.*, 2020; Papaioannou *et al.*, 2022; Rasool *et al.*, 2022).
9. *Tampering*: O ataque de tampering, ou adulteração, refere-se à ataques de modificação não autorizada de dados ou componentes de um sistema, visando comprometer a integridade e a funcionalidade do dispositivo médico. Esse tipo de ataque pode ocorrer em diversas formas, incluindo a alteração física de dispositivos, a modificação de dados em trânsito, ou a manipulação de informações armazenadas. Em dispositivos médicos, a adulteração pode envolver a inserção de código malicioso, a alteração de configurações críticas, ou a manipulação de dados coletados e transmitidos. Por exemplo, um invasor pode alterar o firmware do dispositivo para modificar seu comportamento ou alterar dados de monitoramento para apresentar resultados incorretos. Essas ações podem levar a falhas no funcionamento do dispositivo, comprometendo a segurança do paciente e a eficácia do tratamento (Yaqoob *et al.*, 2019; Yaacoub *et al.*, 2020; Papaioannou *et al.*, 2022; Rasool *et al.*, 2022).
10. *DOS Attack*: O ataque de negação de serviço (DoS) é uma forma de ataque cibernético que visa sobrecarregar um sistema ou rede com tráfego excessivo, resultando na interrupção ou degradação dos serviços oferecidos. No contexto dos dispositivos médicos, um ataque DoS pode comprometer a disponibilidade e a funcionalidade desses dispositivos ao inundar suas interfaces de comunicação ou redes associadas com uma quantidade massiva de requisições, dados ou pacotes maliciosos. Esse tipo de ataque pode ter sérias implicações

para a operação de dispositivos médicos, incluindo a interrupção de serviços críticos, como o monitoramento em tempo real de pacientes, e a impossibilidade de realizar diagnósticos ou tratamentos eficazes. Em cenários extremos, ataques DoS podem resultar em falhas totais do sistema, prejudicando a segurança e o bem-estar dos pacientes (Yaqoob *et al.*, 2019; Hasan *et al.*, 2022; Yaacoub *et al.*, 2020; Papaioannou *et al.*, 2022; Rasool *et al.*, 2022).

11. *DDoS Attack*: Consiste em um ataque de negação de serviços aplicado de forma distribuída, ele tem por objetivo tornar um sistema ou serviço indisponível ao sobrecarregá-lo com uma quantidade massiva de tráfego malicioso proveniente de múltiplas fontes. Em dispositivos médicos conectados, um ataque DDoS pode comprometer a disponibilidade e o desempenho dos sistemas, impedindo o funcionamento correto de serviços críticos de saúde (Yaacoub *et al.*, 2020; Rasool *et al.*, 2022).
12. *Resource Depletion*: O ataque de exaustão de recursos (resource depletion) é uma forma de ataque que visa esgotar os recursos computacionais ou de rede de um sistema, tornando-o incapaz de funcionar corretamente ou de atender a requisições legítimas. Em dispositivos médicos, isso pode envolver a sobrecarga de recursos como CPU, memória, largura de banda ou armazenamento, através de solicitações excessivas ou manipulação maliciosa. Esse tipo de ataque pode comprometer a disponibilidade e o desempenho dos dispositivos médicos, levando a uma interrupção dos serviços essenciais, como monitoramento de pacientes, controle de dispositivos terapêuticos ou processamento de dados clínicos. A exaustão de recursos pode resultar em falhas no sistema, lentidão extrema, ou até mesmo na paralisação completa do dispositivo, afetando negativamente a segurança e o tratamento dos pacientes (Yaqoob *et al.*, 2019; Rasool *et al.*, 2022).
13. *Jamming Attack*: O ataque de interferência (jamming) é uma técnica utilizada para perturbar ou interromper a comunicação em redes sem fio, incluindo aquelas utilizadas por dispositivos médicos conectados. Nesse tipo de ataque, o invasor emite sinais de rádio ou frequências em uma faixa de frequência específica, de forma a criar interferência e sobrecarregar o canal de comunicação, tornando-o inutilizável para a transmissão de dados legítimos. Em dispositivos médicos, um ataque de jamming pode causar a perda ou corrupção de dados críticos, interromper a comunicação entre o dispositivo e sistemas de monitoramento ou controle, e afetar a precisão e a confiabilidade das operações realizadas. Isso pode resultar em falhas no monitoramento de pacientes, interrupções em tratamentos

terapêuticos e comprometimento da integridade dos dados médicos (Yaqoob *et al.*, 2019; Yaacoub *et al.*, 2020; Rasool *et al.*, 2022).

14. *Side Channel Attack*: Significa ataque de canal lateral, esse tipo de ataque explora informações adicionais não diretamente relacionadas aos dados ou operações de um sistema para obter *insights* sobre informações confidenciais. Em dispositivos médicos, esse tipo de ataque pode envolver a análise de informações secundárias, como padrões de consumo de energia, emissões eletromagnéticas, ou temporização de operações, para extrair dados sensíveis ou comprometer a segurança do dispositivo. Por exemplo, um invasor pode monitorar o consumo de energia de um dispositivo médico enquanto ele realiza operações criptográficas para descobrir informações sobre as chaves de criptografia usadas, ou analisar os sinais eletromagnéticos emitidos por um dispositivo para recuperar dados privados. A exploração dessas informações secundárias pode levar a uma quebra de segurança, permitindo que o atacante obtenha acesso não autorizado a dados sensíveis ou controle sobre o dispositivo (Yaqoob *et al.*, 2019; Yaacoub *et al.*, 2020; Papaioannou *et al.*, 2022; Rasool *et al.*, 2022).
15. *Ransomware DOS*: Esse tipo de ataque pode ocorrer em dispositivos médicos locais devido à utilização de sistemas operacionais desatualizados e protocolos proprietários inseguros. Esses ataques se assemelham ao ataque DoS convencional, onde usuários autorizados ficam impossibilitados de acessar os serviços médicos até que a administração do hospital efetue o pagamento do resgate exigido. As implicações desse ataque são extremamente graves, especialmente em situações de emergência, pois a indisponibilidade dos dispositivos médicos e a interrupção de tratamentos podem correr em dados sérios a saúde de pacientes ou levá-los a óbito (Yaqoob *et al.*, 2019; Hasan *et al.*, 2022; Rasool *et al.*, 2022).
16. *Buffer overflow*: Esse tipo de ataque é uma vulnerabilidade crítica de segurança que ocorre quando dados são escritos além dos limites de um buffer, sobrescrevendo a memória adjacente. Em dispositivos médicos, essa falha pode ser explorada para comprometer a integridade e a operação do sistema ao permitir a execução de código malicioso ou a corrupção de dados. Esse tipo de ataque pode resultar na execução de comandos arbitrários, comprometendo o funcionamento do dispositivo médico e permitindo ao invasor obter controle não autorizado sobre o sistema. Além disso, a corrupção de dados críticos pode afetar a precisão dos diagnósticos e tratamentos, enquanto a interrupção de serviços essenciais pode comprometer a continuidade do cuidado aos pacientes (Yaqoob *et al.*,

2019; Rasool *et al.*, 2022).

17. *Brute force attack*: O ataque de força bruta é uma técnica de ataque cibernético que busca comprometer sistemas de segurança através da tentativa exaustiva de todas as combinações possíveis de credenciais, como senhas ou chaves de criptografia, até encontrar a correta. Além disso, em dispositivos médicos conectados, esse tipo de ataque pode ser empregado em sensores médicos remotos e aplicações de monitoramento de pacientes. Esse tipo de ataque pode resultar em várias consequências adversas, como a exposição de informações pessoais e médicas dos pacientes, manipulação de dados clínicos, e controle indevido de dispositivos terapêuticos, o que pode levar a diagnósticos errados e tratamentos inadequados. Além disso, o uso de ataques de força bruta pode sobrecarregar os sistemas, causando degradação no desempenho e até interrupção de serviços críticos (Yaqoob *et al.*, 2019; Rasool *et al.*, 2022; Yaacoub *et al.*, 2020).
18. *Grey hole*: O ataque de grey hole é uma forma de ameaça cibernética em redes de dispositivos médicos, onde um nó malicioso participa da rede e descarta ou atrasa pacotes de dados, sem que isso seja facilmente detectado pelos mecanismos de monitoramento padrão. Ao contrário dos ataques de black hole, onde todos os pacotes são descartados, um grey hole se comporta de forma intermitente, dificultando a detecção. Esse tipo de ataque pode comprometer a integridade e a disponibilidade dos dados em dispositivos médicos, resultando na perda ou corrupção de informações críticas, interrupções no monitoramento de pacientes, e falhas na transmissão de dados essenciais entre dispositivos e sistemas de controle (Yaqoob *et al.*, 2019; Rasool *et al.*, 2022).
19. *Sybil attack*: O ataque de Sybil é uma vulnerabilidade em redes distribuídas onde um único adversário cria múltiplas identidades falsas para influenciar ou controlar a rede de forma desproporcional. Em IoMT, um ataque Sybil pode comprometer a integridade, a confiabilidade e a segurança das comunicações e dados. Esse tipo de ataque pode levar a uma série de problemas, incluindo a manipulação de dados transmitidos entre dispositivos médicos, a introdução de informações falsas, e a desestabilização das operações de rede. As identidades falsas podem ser usadas para votar em decisões de rede, manipular protocolos de consenso, ou comprometer a distribuição de recursos, resultando em diagnósticos incorretos, tratamentos inadequados e falhas no monitoramento de pacientes (Yaqoob *et al.*, 2019; Yaacoub *et al.*, 2020; Rasool *et al.*, 2022).
20. *Deauthentication Attacks*: É uma forma de ataque de negação de serviço direcionado

a rede sem fio, onde o atacante envia pacotes na tentativa de desautenticar um ou mais dispositivos, forçando-os a se desconectar da rede. Em alguns casos esse tipo de ataque é utilizado para obter acesso não autorizado de um dispositivo ou sistema. Além disso, esse tipo de ataque pode resultar em falhas no monitoramento contínuo dos pacientes, interrupções na transmissão de dados vitais e perda de conectividade com dispositivos médicos, outros problemas são diagnósticos errôneos e atrasos nos tratamentos (Yaacoub *et al.*, 2020; Rasool *et al.*, 2022).

21. *Masquerading Attacks*: Os ataques de mascaramento envolvem a atuação de um atacante que assume um nó legítimo da rede com a finalidade de retransmitir mensagens falsas sobre uma condição médica, ou até mesmo interromper a disponibilidade de um sistema. Esse tipo de ataque pode resultar em uma série de problemas críticos, como a inserção de dados falsos no sistema, a execução de comandos maliciosos em dispositivos médicos, e a coleta de informações sensíveis, como dados de pacientes, sem o consentimento ou conhecimento dos usuários legítimos. Além disso, o mascaramento pode levar a diagnósticos incorretos, tratamentos inadequados e interferências na operação de dispositivos terapêuticos (Yaacoub *et al.*, 2020; Papaioannou *et al.*, 2022; Rasool *et al.*, 2022).
22. *Malware Attack*: Esse ataque envolve a utilização de softwares maliciosos, que comprometem a segurança de computadores, redes e dispositivos médicos, sem o consentimento do usuário e dos administradores do sistema. No contexto de sistemas médicos, o atacante pode injetar um *malware* em um dispositivo móvel, por exemplo, após isso, o dispositivo começa a enviar informações falsas aos equipamentos médicos podendo causar graves consequências a saúde dos pacientes. Nesse mesmo cenário, o *malware* também poderia expor informações sigilosas ou mesmo abrir uma *backdoor* para posterior exploração por parte do atacante. Esse tipo de ataque pode causar a adulteração de dados clínicos, interrupção de serviços essenciais, e comprometimento da privacidade dos pacientes. O *malware* pode ser usado para roubar informações sensíveis, alterar configurações críticas, ou tomar controle de dispositivos médicos, resultando em diagnósticos errôneos, tratamentos inadequados, ou falhas no monitoramento de pacientes. Além disso, o *malware* pode se propagar pela rede, afetando outros dispositivos e sistemas conectados, aumentando o alcance e o impacto do ataque (Hasan *et al.*, 2022; Yaacoub *et al.*, 2020; Papaioannou *et al.*, 2022; Rasool *et al.*, 2022; Kim *et al.*, 2015).

2.3.2 Riscos de Segurança Comuns na Borda da Rede da IoMT

A análise do estado atual dos sistemas IoMT revela que os dispositivos médicos possuem vulnerabilidades intrínsecas. Fatores como microcontroladores com baixo poder de processamento, limitações de memória e espaço de armazenamento, consumo restrito de energia e a elevada heterogeneidade tecnológica dificultam significativamente a implementação de mecanismos de segurança eficazes (Yaqoob *et al.*, 2019; Hasan *et al.*, 2022; Papaioannou *et al.*, 2022; Yaacoub *et al.*, 2020; Sun *et al.*, 2019).

A segurança de dispositivos médicos conectados deve ser uma prioridade essencial, mas diversas vulnerabilidades ainda comprometem a integridade, confidencialidade e disponibilidade desses sistemas. Entre os principais riscos estão falhas de implementação, como autenticação insuficiente, mecanismos inadequados de controle de acesso, ausência de criptografia robusta e falta de atualizações regulares de *firmware*. Essas fragilidades tornam os dispositivos médicos suscetíveis a uma ampla gama de ataques, colocando em risco não apenas a confiabilidade dos sistemas e a proteção dos dados, mas também a segurança e o bem-estar dos pacientes. Ademais, tais lacunas de segurança podem prejudicar a reputação de empresas fornecedoras, governos e instituições de saúde, além de ocasionar prejuízos financeiros significativos e litígios legais. A seguir, são discutidas algumas das principais fragilidades associadas a sistemas médicos conectados.

2.3.2.1 Riscos de Segurança a Confidencialidade dos Dados

A confidencialidade dos dados na borda da IoMT é uma preocupação crescente devido à natureza sensível das informações processadas e transmitidas por esses dispositivos. Na borda, onde os dispositivos interagem diretamente com os sensores e atuadores, a exposição a ameaças como interceptação de dados, acessos não autorizados e ataques de intermediários MITM é considerável. A descentralização do processamento na borda, embora ofereça vantagens em termos de latência e eficiência, também amplia a superfície de ataque, uma vez que os dados são processados fora do ambiente controlado da nuvem centralizada. A falta de padronização em protocolos de segurança, juntamente com a diversidade de tecnologias empregadas na borda, contribui para vulnerabilidades que podem comprometer a confidencialidade das informações dos pacientes (Papaioannou *et al.*, 2022; Chantzis *et al.*, 2021).

Além disso, a natureza distribuída da IoMT, com dispositivos dispersos em diversos

ambientes, amplia a superfície de ataque e torna a detecção e resposta a incidentes mais complexas. Muitos dispositivos na borda da IoMT possuem recursos limitados de processamento e armazenamento, o que dificulta a implementação de técnicas avançadas de criptografia e autenticação robusta. Essas limitações podem ser exploradas por atacantes, que visam a execução de ataques como a injeção de *malwares* e o sequestro de dispositivos para acessar e expor dados confidenciais. A necessidade de equilibrar eficiência e segurança no processamento local torna-se, assim, um desafio crucial para manter a proteção da confidencialidade dos dados. Portanto, a mitigação dos riscos à confidencialidade na borda da IoMT exige soluções que integrem tanto inovações tecnológicas quanto a implementação de normas regulatórias e melhores práticas de segurança.

2.3.2.2 *Riscos de Segurança a Integridade dos Dados*

Na borda, os dados são frequentemente gerados, analisados e transmitidos por dispositivos com recursos limitados, o que aumenta a vulnerabilidade a ataques que visam comprometer sua integridade, como a injeção de dados falsos, manipulação de pacotes de informações e ataques de repetição. Esses riscos são ampliados pela natureza distribuída da arquitetura na borda, onde o controle centralizado sobre os fluxos de dados é reduzido, facilitando a ação de agentes maliciosos que podem interferir nos dispositivos e alterar dados críticos. Tais alterações podem afetar diretamente a confiabilidade dos sistemas médicos, comprometendo a precisão e a qualidade dos cuidados prestados aos pacientes (Yaqoob *et al.*, 2019).

Outro fator que agrava os riscos à integridade dos dados na borda da IoMT é a ausência de mecanismos robustos de verificação e auditoria. Sem a implementação adequada de algoritmos de verificação de integridade, como hashes criptográficos ou assinaturas digitais, torna-se difícil assegurar que os dados permaneçam inalterados desde a sua origem até o destino final. A falta de controles eficazes pode permitir que atacantes alterem ou corrompam dados críticos, prejudicando a confiança nos sistemas médicos. Portanto, proteger a integridade dos dados na borda da IoMT exige soluções que combinem segurança em várias camadas, desde a implementação de técnicas criptográficas robustas até o fortalecimento da resiliência dos dispositivos frente a ataques físicos e lógicos, garantindo a autenticidade e a precisão das informações compartilhadas. (Papaioannou *et al.*, 2022).

2.3.2.3 Riscos de Autenticação Fraca

A autenticação fraca na borda representa uma vulnerabilidade significativa, pois expõe sistemas críticos a uma ampla gama de ataques. Muitos dispositivos IoMT operam com métodos de autenticação simplificados devido a limitações de processamento, armazenamento e energia, o que pode resultar no uso de credenciais fracas ou na reutilização de senhas. Esses fatores tornam os dispositivos vulneráveis a acessos não autorizados, comprometendo dados sensíveis e colocando em risco a segurança e a privacidade dos pacientes. Além disso, a natureza distribuída dos dispositivos na borda dificulta a implementação de autenticação robusta, o que aumenta a superfície de ataque e torna esses sistemas mais suscetíveis a invasões, especialmente quando comparados a ambientes centralizados, onde o controle de acesso pode ser mais facilmente gerido.

Entre os principais tipos de ataques que se aproveitam de autenticação fraca estão os ataques de força bruta e de credenciais, nos quais os atacantes tentam repetidamente adivinhar combinações de login até obter sucesso. Outro risco comum é o *phishing*, que visa a coleta de informações de autenticação de operadores e administradores de dispositivos, resultando em acessos indevidos. Adicionalmente, ataques de *spoofing* podem ocorrer, onde o invasor se passa por um dispositivo legítimo para interceptar e manipular dados (Yaqoob *et al.*, 2019; Hasan *et al.*, 2022; Yaacoub *et al.*, 2020).

Além disso, a falta de mecanismos robustos para validar identidades facilita a execução de ataque do tipo *Sybil*, que consiste basicamente em criar múltiplas identidades falsas para assumir o controle da rede, permitindo que dispositivos maliciosos imitem dispositivos legítimos e manipulam dados sensíveis. Isso pode levar à tomada de decisões clínicas com base em informações corrompidas, comprometendo a segurança dos pacientes (Papaioannou *et al.*, 2022).

Para mitigar esses riscos, é essencial a implementação de métodos de autenticação mais robustos, como autenticação multifator, autenticação baseada em certificados ou chaves criptográficas, que dificultam a exploração de vulnerabilidades. Além disso, a adoção de protocolos de autenticação contínua, que realizam verificações dinâmicas e constantes da identidade dos dispositivos, é fundamental para reduzir as janelas de oportunidades para ataques. Essas abordagens garantem um controle mais rigoroso sobre o acesso e a integridade dos sistemas, dificultando a execução de ataques que se aproveitam de autenticação fraca e assegurando a proteção das informações sensíveis dos pacientes.

2.3.2.4 *Mecanismos de Controle de Acesso e Autorização*

Mecanismos inadequados de autorização podem permitir que usuários ou dispositivos obtenham permissões indevidas, acessando dados ou funções críticas sem o devido controle. Esse tipo de vulnerabilidade não apenas expõe informações de saúde a acessos não autorizados, mas também possibilita que atacantes modifiquem configurações de dispositivos médicos, gerando sérias implicações para a segurança dos pacientes e para a operação eficiente dos sistemas. A ausência de uma autorização granular, combinada com políticas de controle de acesso mal configuradas, agrava o problema ao ampliar a superfície de ataque (Yaqoob *et al.*, 2019; Papaioannou *et al.*, 2022; Chantzis *et al.*, 2021).

(Rasool *et al.*, 2022) aborda os aspectos de autorização sob a ótica dos dispositivos ingeríveis, pois a integração desses dispositivos com infraestruturas sem fio traz preocupações de privacidade e segurança, especialmente devido à ausência de mecanismos robustos de autorização. A falta de autenticação adequada, decorrente das limitações de tamanho e poder de processamento desses dispositivos, possibilita acessos não autorizados e compromete a privacidade dos dados transmitidos, além de gerar possíveis anomalias nos diagnósticos e tratamentos.

2.3.2.5 *Mecanismo de Criptografia*

Devido a limitações de recursos computacionais nos dispositivos da borda, muitas vezes a criptografia robusta não é implementada adequadamente, expondo os dados à interceptação e manipulação durante a transmissão. Essa fragilidade permite que adversários acessem informações confidenciais de forma não autorizada, comprometendo a confidencialidade e a integridade dos dados médicos. Além disso, sem mecanismos de criptografia eficazes, os dispositivos ficam vulneráveis a ataques de falsificação de dados, que podem prejudicar o monitoramento e o tratamento de pacientes.

Entre os principais tipos de ataques que exploram a falta de criptografia estão os ataques de interceptação de comunicação, como o *eavesdropping*, no qual os invasores conseguem monitorar e capturar dados enquanto são transmitidos entre os dispositivos e as estações móveis. Outro ataque comum é o *man-in-the-middle*, em que o adversário intercepta e possivelmente altera as comunicações entre duas partes sem que elas percebam. Ataques de *replay* também podem ocorrer, permitindo que dados legítimos capturados sejam retransmitidos de forma maliciosa para alterar decisões clínicas ou operações de dispositivos. Para mitigar esses

riscos, é fundamental que sejam adotadas técnicas de criptografia leve, adaptadas às limitações dos dispositivos da borda, garantindo, assim, a proteção dos dados durante todo o ciclo de transmissão e processamento (Yaqoob *et al.*, 2019; Hasan *et al.*, 2022; Papaioannou *et al.*, 2022; Yaacoub *et al.*, 2020; Sun *et al.*, 2019).

2.3.2.6 Atualização de Firmware

A atualização de *firmware* nos dispositivos IoMT é um processo crítico para garantir a segurança e a integridade do sistema, uma vez que atualizações regulares corrigem vulnerabilidades e aprimoram as funcionalidades dos dispositivos. No entanto, a ausência de um mecanismo eficaz de atualização ou a falta de atualizações periódicas expõe esses dispositivos a diversos riscos, na maioria das vezes significativos. Dispositivos IoMT com *firmware* desatualizado tornam-se suscetíveis a falhas de segurança já conhecidas, que podem ser exploradas por atacantes para comprometer o sistema, manipular dados médicos ou desativar funcionalidades críticas. Além disso, a atualização de *firmware* na borda enfrenta desafios adicionais, como limitações de conectividade, restrições de recursos e a necessidade de garantir que o processo não interrompa a operação contínua dos dispositivos, especialmente em aplicações de saúde crítica.

Entre os principais ataques que exploram a ausência ou a ineficiência de atualizações de *firmware* estão os ataques de exploração de vulnerabilidades conhecidas, nos quais invasores aproveitam falhas não corrigidas para obter controle sobre os dispositivos. Um exemplo comum é o ataque de injeção de código, em que um *firmware* comprometido pode permitir a execução de comandos maliciosos. (Zubair *et al.*, 2019) descreve um vetor de ataque conhecido como *Blue Print*, no qual o atacante coleta informações detalhadas sobre o fabricante do dispositivo e o *firmware* utilizado. Com esses dados em mãos, o invasor pode localizar a versão exata instalada e, a partir daí, realizar engenharia reversa para identificar possíveis vulnerabilidades de segurança.

Além disso, os mecanismos de atualização de *firmware* conhecidos como OTA (over the air) enfrentam desafios consideráveis, principalmente devido às limitações de recursos de hardware, conectividade e segurança. Devido às capacidades limitadas de processamento e energia, os dispositivos podem ter dificuldade em realizar atualizações complexas sem interromper suas operações, especialmente em ambientes de saúde crítica. A confiabilidade da conectividade também é um fator crucial, pois a interrupção de uma atualização OTA pode resultar em falhas no dispositivo, tornando-o inutilizável ou deixando o sistema vulnerável a ataques. Além disso,

o processo de atualização deve ser protegido contra interferências externas, garantindo que o *firmware* atualizado não seja comprometido durante a transmissão, o que exige protocolos de segurança robustos, como criptografia e autenticação. A implementação eficaz de OTA em IoMT requer, portanto, uma abordagem cuidadosa, que considere tanto as restrições operacionais dos dispositivos quanto a necessidade de segurança rigorosa (Chantzis *et al.*, 2021; Yaqoob *et al.*, 2019; Qasem *et al.*, 2021; Moraes; Hayashi, 2021).

2.3.3 Desafios de Comunicação na Camada de Percepção

A eficácia da IoMT depende, em grande parte, da capacidade de comunicação entre os dispositivos na camada de percepção. Essa camada, responsável pela coleta e transmissão dos dados biométricos e clínicos, exige um alto nível de confiabilidade e segurança para garantir a qualidade do atendimento aos pacientes. No entanto, a complexidade dos ambientes clínicos, a diversidade de dispositivos e a presença de interferências externas representam desafios significativos para a comunicação. A seguir, discutiremos os principais problemas referentes aos protocolos de comunicação e como esses problemas podem afetar a segurança dos sistemas IoMT.

2.3.3.1 Bluetooth

Criada pelo *Bluetooth Special Interest Group*, formado por empresas como Ericsson, IBM, Intel, Nokia e Toshiba, a tecnologia *Bluetooth* foi desenvolvida com o objetivo de interligar uma ampla variedade de dispositivos, como celulares, computadores, aparelhos médicos, fones de ouvido e outros dispositivos eletrônicos portáteis. Seu propósito principal era viabilizar a comunicação sem fio de curto alcance, operando em frequências entre 2,4 GHz e 2,5 GHz, que pertencem a uma faixa de uso aberto, permitindo sua utilização por diferentes dispositivos sem a necessidade de licenciamento. No entanto, o uso compartilhado dessa faixa de frequência pode gerar problemas, especialmente em ambientes com muitos dispositivos operando simultaneamente, o que aumenta as chances de colisões e congestionamentos na comunicação. Essas interferências podem resultar em perda de desempenho e comprometer a confiabilidade das comunicações sem fio. Apesar desses desafios, a tecnologia *Bluetooth* trouxe avanços significativos, como baixo consumo de energia e a capacidade de transmitir dados e voz de maneira simultânea (Bisdikian, 2001; Silva *et al.*, 2021; Lonzetta *et al.*, 2018).

As vulnerabilidades de segurança em tecnologias *Bluetooth* apresentam uma consi-

derável variação entre diferentes versões, devido às correções implementadas de uma para outra. Segundo Zubair *et al.* (2019), é possível encontrar diversas vulnerabilidades no *Bluetooth* até a versão 4.0; dentre os muitos problemas, destaca-se o problema de autenticação, que compromete as informações e o acesso a chaves secretas.

A segurança de um dispositivo médico que usa o *Bluetooth* como tecnologia de comunicação pode ser drasticamente comprometida, especialmente quando os dispositivos estão em modo detectável. Nesse estado, eles se tornam vulneráveis a ataques, pois podem ser facilmente identificados por outros dispositivos dentro de um raio de aproximadamente 10 metros. Durante o processo de descoberta, informações sensíveis, como o nome do dispositivo, sua classe, a lista de serviços e dados técnicos, são transmitidas, facilitando a ação de potenciais atacantes. Além disso, é importante destacar que cada dispositivo *Bluetooth* possui um identificador único de 48 bits, conhecido como BD_ADDR, que é atribuído pelo fabricante. Esse identificador funciona de maneira similar a um endereço MAC. Embora o BD_ADDR seja essencial para a identificação do dispositivo, ele também pode ser explorado por adversários para mapear e rastrear dispositivos vulneráveis, ampliando os riscos de segurança, especialmente em ambientes com muitos dispositivos conectados (Lonzetta *et al.*, 2018).

A tabela 2 apresenta alguns dos principais ataques que podem ser empregados para comprometer a segurança de dispositivos médicos que usam tecnologias *Bluetooth*.

2.3.3.2 BLE

Criação da Nokia em 2007, o BLE é uma evolução derivada do *Bluetooth* e desempenha um papel fundamental em dispositivos IoMT, destacando-se pela sua capacidade de facilitar a comunicação entre dispositivos de pequeno porte com restrições de consumo de energia. O BLE opera nas faixas de frequência de 2.400 a 2.483,5 MHz, utilizando apenas 40 canais. Atualmente, a tecnologia está em sua quinta geração e permite comunicação bidirecional, além de contar com *Electronic Shelf Label* (ESL), que permite a um único dispositivo enviar sinais para diversos dispositivos receptores ao mesmo tempo. Em sua quinta geração, o BLE consegue atingir distâncias de até 40 metros e taxas de transferência de até 50 Mbps.

Atualmente, o *Bluetooth* tem sido a tecnologia favorita na construção de dispositivos IoT, devido ao baixo consumo de energia e à melhoria na comunicação entre dispositivos. No entanto, assim como outras versões, o BLE não está livre de problemas de segurança, sendo suscetível aos diversos ataques relatados anteriormente nas versões convencionais (Yaqoob *et al.*,

Tabela 2 – Ataques que podem ser empregados em dispositivos com tecnologias *Bluetooth*.

Tipo de Ataque	Descrição
<i>Blue smacking</i>	Ataque DoS, consistem em sobrecarregar os dispositivos com pacotes redundantes e aleatórios.
<i>Blue snarfing</i>	Roubo de informações, consiste na exploração do protocolo de transferência de arquivos (OBEX).
<i>Bluejacking</i>	Consiste no envio de mensagens falsas com o intuito de obter chaves que permitam o acesso de informações do dispositivo.
<i>Blue bugging</i>	Consiste na tentativa de obtenção do controle do dispositivo.
<i>Blue Printing</i>	Busca a obtenção de informações gerais do dispositivo, como por exemplo o <i>firmware</i> , isso pode ser um problema caso o atacante faça engenharia reversa no software que controla o dispositivo, visando a descoberta de novas brechas de segurança.
<i>Mac spoofing attack</i>	O atacante obtém informações da vítima interceptando os dados com um dispositivo que se passa por um receptor autentico das mensagens.
<i>MITM/Impersonation attack</i>	O atacante interrompe a conexão entre dois dispositivos autênticos e faz com que os mesmos se conectem ao dispositivo do atacante, se colocando no meio entre a comunicação.
<i>PIN Cracking Attack</i>	O atacante utiliza uma ferramenta de detecção de frequência para coletar o RAND e o BD_ADDR e depois lança um ataque de força bruta na tentativa de acertar o código PIN.

Fonte: Elaborada pelo autor.

2019; Silva *et al.*, 2021; Lonzetta *et al.*, 2018).

Em (Chantzis *et al.*, 2021), os autores demonstram a utilização de ferramentas como Bettercap e GATTTool para descobrir e capturar dados de dispositivos IoT com BLE habilitado. Com ferramentas simples, diversos dados podem ser capturados, incluindo ataques como *Spoofing* de BD_ADDR e MITM.

2.3.3.3 ZigBee

A tecnologia ZigBee desempenha um papel fundamental na operação de uma ampla variedade de dispositivos baseados em sensores, sendo especialmente notável por sua eficiência em ambientes com restrições de energia. Projetada para aplicações que utilizam radiofrequência

e exigem longa duração de bateria, segurança de rede, eficiência energética e baixas taxas de transmissão de dados, ZigBee é amplamente utilizada em sistemas com essas demandas. Dispositivos compatíveis com ZigBee, muitas vezes alimentados por baterias de longa duração, podem operar por vários anos, beneficiando-se do modo de espera para conservar energia. A estrutura da rede ZigBee é composta por três componentes principais: dispositivos finais, roteadores e coordenadores. Baseada no padrão IEEE 802.15.4, ZigBee opera em diferentes frequências, como 868 MHz na Europa, 915 MHz nos Estados Unidos e 2,4 GHz em outros países. Além disso, a tecnologia permite comunicação entre dispositivos em um alcance que varia de 10 a 100 metros (Yaqoob *et al.*, 2019; Silva *et al.*, 2021).

O protocolo ZigBee utiliza o algoritmo de criptografia AES com a chave de 128 bits, além disso para reforçar os mecanismos de segurança o ZigBee utiliza três chaves em seu mecanismo, sendo elas:

- **Chave Mestra:** consiste em uma chave única compartilhada entre os dispositivos dentro de uma rede Zigbee. Ela é usada para derivar outras chaves importantes, como as chaves de link e de rede, ela é crucial para a segurança dos dispositivos ZigBee, pois serve como a base para a geração de outras chaves além de ser usada para autenticar e criptografar as comunicações entre os dispositivos.
- **Chave de Link:** esta chave é derivada da chave mestra e é usada para autenticar e proteger as comunicações entre dois dispositivos específicos dentro da rede ZigBee, a chave de link é única para cada par de dispositivos da rede ZigBee, isso garante que apenas os dispositivos autorizados possam se comunicar entre si de maneira segura.
- **Chave de Rede:** derivada da chave mestra, essa chave é usada para autenticar a comunicação dos dispositivos dentro da rede ZigBee, ela consiste em uma chave única compartilhada por todos os dispositivos pertencentes a uma mesma rede.

O ZigBee é, de fato, uma tecnologia adequada para dispositivos IoMT devido às suas características de baixa potência e também seus mecanismos de segurança. Contudo, (Yaqoob *et al.*, 2019) destaca que, ao estabelecer a conexão em uma rede ZigBee, cada nó necessita requisitar a chave de rede atual, empregando a chave mestra pré-configurada. Apesar dessa abordagem, que visa garantir a segurança da comunicação, sua aplicação apresenta vulnerabilidades notáveis. Dentre os desafios enfrentados, destacam-se ameaças como ataques de esgotamento de energia, DoS, ataques de repetição e *sniffing*.

Um fator adicional que pode comprometer a segurança dos sistemas médicos é a

inadequação do algoritmo de criptografia Advanced Encryption Standard (AES) para dispositivos sensoriais com recursos limitados. Embora o AES seja reconhecido por sua robustez, sua complexidade intrínseca demanda uma quantidade considerável de energia e capacidade de processamento, tornando-o impraticável em ambientes onde a eficiência energética e o poder de processamento são recursos escassos. Dessa forma, o AES se torna uma opção desafiadora e muitas vezes inviável para dispositivos sensoriais com recursos restritos.

Diante dessas considerações, é crucial buscar estratégias de segurança alternativas, mais adequadas para ambientes ZigBee, que considerem as limitações específicas dos dispositivos sensoriais. Essas abordagens devem garantir não apenas a integridade das comunicações, mas também otimizar o desempenho e prolongar a vida útil dos dispositivos.

2.3.3.4 UWB

O padrão IEEE 802.15.6, também conhecido como UWB, foi desenvolvido para atender às demandas de comunicação em dispositivos de saúde, sendo amplamente utilizado em *Wireless Body Area Networks* (BAN), redes sem fio que interconectam dispositivos localizados na área corporal. Essas redes são comumente aplicadas em dispositivos biomédicos, como sistemas de monitoramento de saúde e sensores vestíveis. O padrão IEEE 802.15.6 define três níveis de segurança: o nível 0, o mais básico, que não implementa nenhum mecanismo de autenticação ou criptografia; o nível 1, que inclui autenticação, mas não criptografia; e o nível 3, que incorpora tanto autenticação quanto criptografia.

A tecnologia UWB oferece suporte a uma alta capacidade de canal devido à sua largura de banda ampla, o que possibilita a transmissão de baixa potência e minimiza as interferências com outras tecnologias sem fio que operam em faixas de frequência menores. O UWB também utiliza uma técnica conhecida como *Impulse Radio* UWB, que, ao invés de transmitir sinais contínuos de rádio, faz uso de pulsos de radiofrequência extremamente curtos, na ordem de nanosegundos ou até pico-segundos. Além disso, essa tecnologia opera em faixas de frequência superiores a 500 MHz e tem sido utilizada como referência para tecnologias sem fio em dispositivos médicos (Silva *et al.*, 2021; Coppens *et al.*, 2022; Kwak *et al.*, 2010)

Apesar de ser considerada uma tecnologia revolucionária de transmissão, o uso do UWB apresenta algumas limitações importantes. A primeira delas é que, em transmissões de baixa potência, as distâncias de conexão entre os sensores e os receptores são relativamente curtas. Outro ponto a ser destacado é que a alta largura de banda pode causar maiores distorções

nos sinais transmitidos, o que pode reduzir significativamente o desempenho dos dispositivos.

2.3.3.5 WI-FI

A especificação IEEE 802.11 define padrões para redes locais sem fio (WLAN), abrangendo as camadas física e de enlace de dados. Em ambientes de banda baixa, como os utilizados nos padrões IEEE 802.11b, g e n, a transmissão de dados atinge velocidades de até 11 Mbps e 54 Mbps, com distâncias de até 32 metros em ambientes internos e 95 metros em ambientes externos. Notavelmente, o padrão IEEE 802.11n utiliza o dobro da largura de espectro em comparação com os padrões IEEE 802.11a ou 802.11g. Enquanto as tecnologias IEEE 802.11a e ac oferecem taxas de transmissão na ordem de Gbps, superando em mais de duas vezes o alcance das tecnologias b e g. Além disso, é importante destacar que o Wi-Fi de banda baixa opera na faixa ISM de 2,4 GHz, enquanto o de banda alta transmite na faixa de 5 GHz.

Embora seja amplamente utilizada para altas transferências de dados, a tecnologia WI-FI é inadequada para ser embarcada em muitos tipos de dispositivos médicos devido ao seu alto consumo de energia. No entanto, o WI-FI continua sendo, sem dúvida, a tecnologia mais utilizada em redes sem fio convencionais, incluindo em ambientes hospitalares e de saúde em geral. Nessas redes, encontram-se diversos dispositivos, como celulares, computadores e notebooks, utilizados para acessar sistemas e configurar dispositivos médicos. Além disso, a tecnologia WI-FI apresenta diversos problemas de segurança já conhecidos, como interfaces de configuração de *firmwares* e configurações de fábrica não alteradas, quebra de chaves criptográficas devido a algoritmos fracos, entre outros (Challoo *et al.*, 2012; Forouzan; Mosharraf, 2013; Silva *et al.*, 2021; Yaqoob *et al.*, 2019).

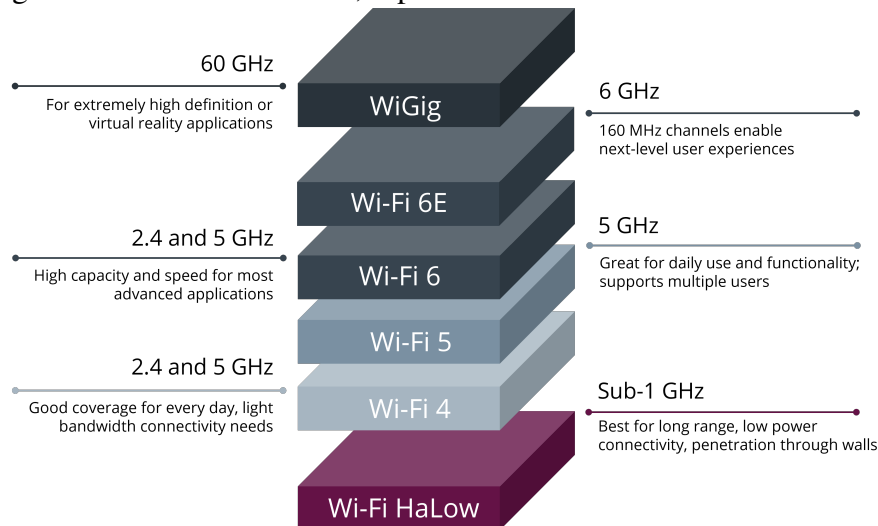
Além disso, *toolkits* como *Aircrack-ng*, foram desenvolvidas com o intuito de testar, monitorar e avaliar a segurança de redes WI-FI, no entanto, essas mesmas ferramentas podem ser usadas por cibercriminosos para realizar ataques repetição de sinal, desautenticação, injeção de pacotes, quebra de criptografia e muito mais (*Aircrack-ng*... ,)

2.3.3.6 WI-FI HaLow

O padrão IEEE 802.11ah foi criado em 2010, mas só foi lançado oficialmente em 2017 pela WI-FI Alliance. O WI-FI HaLow é uma especificação que pode ser aplicada em diversos contextos da IoT, como indústria, prédios inteligentes, agricultura e saúde. A tecnologia HaLow opera em frequências abertas de 1 GHz e não exige licença, o que possibilita atender aos

requisitos funcionais de uma ampla variedade de dispositivos médicos, vestíveis e implantáveis. Características como eficiência energética, interoperabilidade entre dispositivos, configuração sem interrupção da rede WI-FI e maior alcance de sinal são aspectos fundamentais para a IoMT, e o HaLow abrange todos esses requisitos. Além disso, o HaLow opera em frequências mais baixas e, por isso, tem maior capacidade de transpor obstáculos, podendo atingir distâncias de até 1 km. O HaLow pode ser aplicado tanto em topologia estrela quanto em comunicação ponto a ponto; além disso, é possível conectar até 8000 dispositivos em uma rede. O HaLow ainda implementa os mecanismos de segurança mais modernos do WI-FI (Qiao *et al.*, 2018; Moussa; Jabri, 2021). A Figura 4 apresenta as versões do WI-FI, suas características e o espectro em que atuam.

Figura 4 – Versões do Wi-Fi, espectros e finalidade.



Fonte: (Anjielo, 2022) (Autoria desconhecida).

O estudo de (Moussa; Jabri, 2021) se concentra em investigar o impacto de ataques ao mecanismo *Ready To Send* (RTS) e *Clear To Send* (CTS). Esse mecanismo tem como objetivo resolver o problema do “nó oculto”, uma situação em que dois nós em uma rede sem fio estão dentro do alcance um do outro, mas não conseguem detectar a transmissão um do outro devido a obstáculos físicos ou interferências no ambiente. Quando um nó deseja enviar dados, ele transmite um pacote RTS para os nós ao seu alcance. Esse pacote contém informações sobre a transmissão planejada, incluindo a duração estimada da transmissão. O RTS serve como um aviso prévio aos nós vizinhos de que o nó está prestes a iniciar uma transmissão. Quando um nó vizinho recebe o RTS e determina que não há conflito iminente com outras transmissões, ele responde com um pacote CTS. O CTS é transmitido de volta ao nó remetente para confirmar que

o canal está “livre” e que ele pode prosseguir com a transmissão. Além disso, o CTS é ouvido pelos nós ao redor, especialmente aqueles que podem não ter ouvido o RTS inicial, ajudando a evitar colisões.

No entanto, um exemplo específico de vulnerabilidade está relacionado à troca de pacotes RTS/CTS no padrão IEEE 802.11. Esse mecanismo, concebido para mitigar o problema do nó oculto, pode ser alvo de exploração por invasores. Um invasor mal-intencionado pode deliberadamente enviar pacotes RTS ou CTS, com o intuito de bloquear a comunicação de seu vizinho. Essa ação maliciosa interrompe a troca de informações entre as estações, comprometendo a eficácia do padrão e, potencialmente, prejudicando o desempenho da rede sem fio (Moussa; Jabri, 2021).

2.3.3.7 *Ethernet*

O IEEE 802.3 é um conjunto de padrões que define a especificação para redes locais com fio, sendo amplamente conhecido como *Ethernet*. Desenvolvidos pelo *Institute of Electrical and Electronics Engineers* (IEEE), esses padrões são fundamentais para a implementação e operação de redes locais. Além disso, o IEEE 802.3 especifica diversas características de subpadrões, incluindo o método de acesso ao meio, como o CSMA/CD, que foi substituído pelo CSMA/CA, utilizado em redes modernas. O *Ethernet* também define as características elétricas e físicas do meio de transmissão, como taxas de transmissão, formatos de quadros e os meios físicos, como cabos coaxiais, de par trançado e fibras ópticas (Yaqoob *et al.*, 2019).

Redes *Ethernet* podem empregar muitas configurações de topologia de rede, abrangendo conexões ponto a ponto, redes em barra e redes em estrela, no entanto, as velocidades de transmissão variam de acordo com a especificação empregada, alguns padrões mais conhecidos incluem:

- 10BASE-T: Ethernet de 10 Mbps sobre cabos de par trançado.
- 100BASE-TX: Fast Ethernet de 100 Mbps sobre cabos de par trançado.
- 1000BASE-T: Gigabit Ethernet de 1000 Mbps sobre cabos de par trançado.
- 10GBASE-T: 10 Gigabit Ethernet sobre cabos de par trançado.

O meio físico de transmissão de dados em redes locais, especialmente em ambientes hospitalares de grande porte, é vulnerável a diversas ameaças, como *sniffing*, injeção de pacotes, *spoofing* de endereço MAC e ataques de negação de serviço. Embora a execução desses ataques exija, em princípio, acesso físico à rede, a possibilidade de agentes internos maliciosos ou

invasores externos se aproveitarem de pontos de acesso expostos, como tomadas RJ45, demanda a implementação de medidas de segurança robustas. Afinal, mesmo com o acesso físico restrito a áreas críticas, a rede hospitalar continua suscetível a riscos, o que exige a adoção de políticas e práticas de segurança rigorosas.

2.4 Modelagem de Risco

Segundo Adam Shostack, autor renomado e especialista em modelagem de risco com ampla experiência na área, “A modelagem de ameaças é a chave para uma defesa focada. Sem modelagem de ameaças, você nunca vai parar de brincar de whack-a-mole” (Shostack, 2014).

Diante dos inúmeros desafios enfrentados em sistemas de IoMT, a modelagem de risco surge como uma ferramenta essencial para enfrentar os problemas de segurança. Ao proporcionar uma visão estruturada dos potenciais vetores de ataque e vulnerabilidades, essa abordagem permite que profissionais de segurança da informação antecipem ameaças e implementem medidas preventivas de forma eficiente. Em um ambiente onde a proteção de dados sensíveis e a integridade de dispositivos são cruciais, a modelagem de risco atua como uma aliada indispensável na construção de sistemas mais resilientes e confiáveis.

A modelagem de risco consiste em um processo sistemático para identificar e mitigar ameaças de segurança em sistemas antes que estas se materializem. Este processo usa modelos que abstraem detalhes técnicos, permitindo uma visão ampliada do sistema e de seus potenciais problemas, ao invés de focar diretamente no código ou em implementações específicas (Shostack, 2014).

A utilização de modelos tem dois propósitos principais: antecipar ameaças antes da construção de sistemas e encontrar vulnerabilidades de maneira proativa. Isso torna a modelagem uma prática essencial para reduzir custos e esforços associados a correções posteriores. Além disso, o processo permite que desenvolvedores e engenheiros tenham uma compreensão mais abrangente das ameaças que podem impactar a segurança de um sistema, auxiliando na criação de soluções mais robustas desde as fases iniciais de *design*.

2.4.1 Frameworks para modelagem de riscos

Existe uma ampla variedade de métodos para modelagem de risco, cada um com abordagens e objetivos distintos. Alguns desses métodos focam na criação de abstrações de sistemas, fornecendo uma visão mais ampla das possíveis ameaças. Outros são voltados para aspectos específicos, como o comportamento humano ou a identificação detalhada de vulnerabilidades. Enquanto certos modelos priorizam a classificação de riscos, outros buscam compreender o impacto e a explorabilidade das ameaças, oferecendo uma análise mais profunda sobre as possíveis consequências e caminhos de ataque. Essa diversidade de enfoques permite que a modelagem de risco seja adaptada às necessidades de diferentes contextos e sistemas (Shevchenko *et al.*, 2018).

Alguns profissionais buscam combinar diferentes métodos, pois, a partir dessas combinações, é possível obter uma visão mais robusta e abrangente, promovendo a segurança e a resiliência de sistemas específicos. De modo geral, essa prática oferece um caminho estruturado para enfrentar os desafios complexos na construção de sistemas variados, contribuindo para a proteção de dados sensíveis, a privacidade dos usuários e a integridade dos diversos componentes envolvidos.

Segundo Shevchenko *et al.* (2018), “pensar sobre requisitos de segurança com modelagem de ameaças pode levar a decisões arquitetônicas proativas que permitem que as ameaças sejam reduzidas desde o início”. No entanto, é importante frisar que a modelagem de riscos é uma atividade prática e, para que seja efetiva, é necessário que os profissionais que a utilizam possuam vivência prática com o modelo adotado. Caso contrário, sua aplicabilidade pode se tornar ineficiente, não atingindo os objetivos inerentes a prática (Shostack, 2014). A Tabela 3 apresenta seis dos principais *frameworks* de modelagem de riscos e seus objetivos.

Tabela 3 – *frameworks* de modelagem de riscos e seus objetivos.

Framework	Objetivos
STRIDE	Desenvolvido pela Microsoft, tem como objetivo identificar ameaças de segurança categorizadas em seis propriedades (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) e ajudar no entendimento de como mitigar riscos associados.
VAST	Um acrônimo para (Visual, Agile, and Simple Threat), possui foco em organizações ágeis, visa integrar a modelagem de ameaças no fluxo de desenvolvimento de software, fornecendo uma abordagem escalável que facilita a comunicação entre diferentes partes interessadas.
OCTAVE	Propõe avaliar os riscos organizacionais por meio da análise de ativos críticos, ameaças e vulnerabilidades, com o objetivo de priorizar a segurança baseada no impacto nos negócios.
PASTA	Baseia-se em simulações de ataque para identificar ameaças potenciais, com foco em alinhar os resultados às metas de negócios e priorizar ameaças de maior impacto.
DREAD	Um modelo de pontuação de ameaças que busca avaliar riscos com base em cinco fatores (Damage, Reproducibility, Exploitability, Affected Users, Discoverability) para priorizar e mitigar as vulnerabilidades identificadas.
TRIKE	Focado na análise de risco, combina modelagem de ameaças com controle de requisitos de segurança, visando fornecer uma análise quantificada do impacto das ameaças sobre os sistemas.

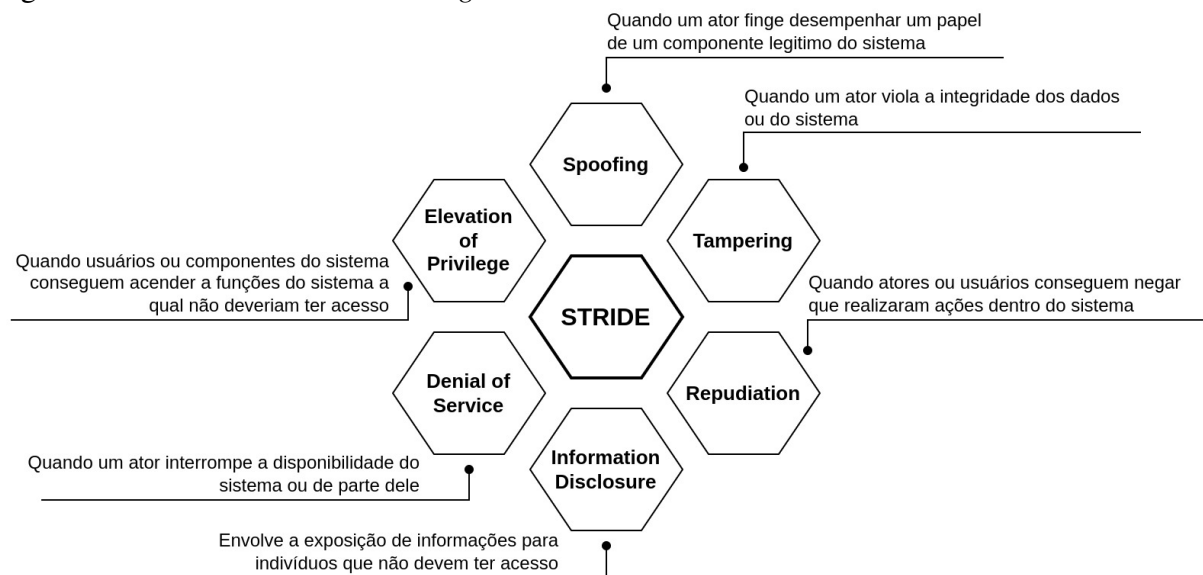
Fonte: Elaborada pelo autor.

2.4.2 Visão Geral do Processo de Modelagem de Risco e Aplicação do STRIDE

O STRIDE é um *framework* amplamente utilizado para a modelagem de ameaças, pois ele oferece uma estrutura sistemática para a identificação e classificação de riscos. Originalmente desenvolvido pela Microsoft, o STRIDE foi projetado para abranger seis categorias principais de ameaças: Spoofing (falsificação de identidade), Tampering (manipulação de dados), Repudiation (não repúdio), Information Disclosure (divulgação de informações), Denial of Service (negação de serviço) e Elevation of Privilege (elevação de privilégios). Cada uma dessas categorias permite que os desenvolvedores analisem vulnerabilidades em diferentes camadas dos sistemas e, a partir disso, promovam uma abordagem proativa à mitigação de riscos. Dessa forma, o STRIDE se consolidou como uma metodologia eficaz para garantir que potenciais ameaças sejam compreendidas e endereçadas adequadamente, colaborando para o fortalecimento da segurança em diversas arquiteturas tecnológicas, incluindo sistemas de IoMT (Khan *et al.*,

2017; Asif *et al.*, 2021). Ver detalhes das categorias do STRIDE na Figura 5.

Figura 5 – STRIDE Threat Modeling.



Fonte: Elaborada pelo autor.

A modelagem de risco consiste na identificação de potenciais ameaças que possam comprometer a segurança de um sistema, por meio de uma avaliação detalhada de sua funcionalidade e arquitetura. Esse processo é crucial para reconhecer e classificar fraquezas que possam ser exploradas por agentes maliciosos. O objetivo é identificar pontos vulneráveis no sistema que necessitam de atenção especial para evitar possíveis explorações. Não existe necessariamente um consenso de quantas fases o processo de modelagem de risco deve ter, de fato o STRIDE pode ser aplicado em apenas três fases, porém o processo de modelagem de risco envolve atividades que vão além da identificação do risco, alguns autores por exemplo, abordam o processo dentro de seis fases, pois eles consideram atividades de documentação, classificação e priorização de ameaças (Chantzis *et al.*, 2021; Khan *et al.*, 2017; Cagnazzo *et al.*, 2018; Asif *et al.*, 2021).

Neste trabalho utilizaremos a abordagem de seis fases para exemplificar o processo de modelagem de risco com STRIDE, pois assim conseguimos separar melhor as responsabilidades de cada uma das fases, trazendo mais clareza para uma melhor compreensão do processo. Conforme demonstrado na Figura 6, as fases do processo de modelagem segue uma sequência ordenada de processos que perpassam pela identificação dos componentes que compõem a arquitetura, diagramação do panorama da arquitetura, decomposição dos componentes da arquitetura em ativos menores (partes que compõem um componente de um sistema), identificação de vulnerabilidades para cada um dos ativos (aplicação do STRIDE), documentação de vulnerabilidades, e por fim a classificação das vulnerabilidades.

Figura 6 – Fases do processo de modelagem de risco com STRIDE.



Fonte: Elaborada pelo autor.

A primeira fase, consiste na identificação dos componentes principais do sistema, como dispositivos médicos que fazem parte da rede ciberfísica, *gateways*, servidores de aplicação, banco de banco e outros.

A fase dois consiste, portanto, na criação de um panorama da arquitetura do sistema, em que os componentes identificados na primeira fase são organizados de forma sistemática, considerando o fluxo de dados e os limites de confiança entre os diferentes componentes da arquitetura.

A terceira fase corresponde ao que diversos autores denominam “*Breaking the Architecture into Components*” (quebrar a arquitetura em componentes), onde basicamente cada componente da arquitetura é decomposto em partes menores chamadas de ativos (Chantzis *et al.*, 2021; Asif *et al.*, 2021). Por exemplo, uma bomba de infusão de insulina poderia ser decomposta nos seguintes ativos:

- *Hardware* da bomba
- *Firmware* da bomba
- Sistema operacional
- Biblioteca de alimentos
- Protocolo de comunicação sem fio

Ainda sobre a fase três, os ativos identificados em cada componente da arquitetura também serão organizados de maneira sistemática, a fim de oferecer uma visão mais detalhada e precisa das possíveis vulnerabilidades do componente em questão.

A fase quatro é onde as propriedades do STRIDE são aplicadas de fato. Para cada um dos ativos de um componente específico da arquitetura, cada uma das seis categorias de

ameaças é analisada em relação às características e funcionalidades desse ativo. Basicamente, o processo envolve examinar como o ativo lida com dados, interage com outros ativos e sistemas e quais recursos de segurança estão implementados ou ausentes.

Na quinta fase, cada ameaça deve ser bem documentada, para isso, é necessária uma estrutura organizada que forneça detalhes sobre cada ameaça identificada, como, por exemplo, uma descrição detalhada da ameaça, os ativos que ela afeta, o ataque empregado para exploração e o mecanismo de mitigação.

A sexta fase do processo de modelagem de riscos consiste na utilização de algum modelo de classificação de ameaças, como por exemplo, o DREAD (acrônimo para Damage, Reproducibility, Exploitability, Affected Users e Discoverability). O modelo DREAD é uma metodologia amplamente adotada para avaliar e classificar riscos de segurança em sistemas complexos. Ele considera cinco fatores fundamentais: Danos (Damage Potential), Reprodutibilidade (Reproducibility), Explorabilidade (Exploitability), Atingibilidade (Affected Users) e Descobribilidade (Discoverability). Cada uma dessas categorias permite a análise detalhada dos riscos, facilitando o processo de atribuição de uma pontuação baseada na severidade potencial de uma ameaça, e por conseguinte facilitando a priorização das mesmas (Cagnazzo *et al.*, 2018; Chantzis *et al.*, 2021).

2.4.3 Modelagem de riscos em IoMT

No ambiente hospitalar, você está cercado pela Internet das Coisas Médicas. Nos corredores, dispositivos médicos inteligentes monitoram continuamente os sinais vitais dos pacientes, transmitindo dados em tempo real para sistemas centrais. Nas salas de cirurgia, equipamentos conectados, como ventiladores e bombas de infusão, trabalham em sincronia, garantindo precisão e segurança. Nos laboratórios, sensores avançados analisam amostras com alta eficiência, enviando os resultados diretamente para os prontuários digitais dos pacientes. Em todas essas situações, a ubiquidade da IoMT transforma o atendimento à saúde, ampliando a capacidade de resposta e a qualidade dos serviços, mas também introduzindo desafios significativos relacionados à segurança e privacidade (Mathkor *et al.*, 2024).

A modelagem de risco é essencial no contexto da IoMT devido às inúmeras limitações e vulnerabilidades inerentes aos dispositivos conectados. Muitos dispositivos IoMT utilizam plataformas de hardware e sistemas operacionais genéricos, como distribuições de Android ou Linux, que frequentemente oferecem mais funcionalidades do que o necessário, ampliando as

superfícies de ataque disponíveis. Esses sistemas passam, em muitos casos, por personalizações realizadas por desenvolvedores que, frequentemente, não consideram controles de segurança adequados. Isso pode comprometer as proteções originais desses sistemas operacionais, expondo os dispositivos a ataques cibernéticos (Yaqoob *et al.*, 2019; Chantzis *et al.*, 2021).

No caso de dispositivos baseados em sistemas operacionais em tempo real (RTOS), a minimização do tempo de processamento resulta em padrões de segurança ainda menos robustos, uma vez que esses dispositivos geralmente carecem de suporte para ferramentas de segurança modernas, como antivírus ou listas de permissões de software. Adicionalmente, muitos dispositivos IoMT utilizam protocolos proprietários ou não padronizados, o que agrava as dificuldades de implementar medidas de segurança consistentes e sofisticadas, como controle de integridade de software e atestação de dispositivos.

A ausência de atualizações de segurança contínuas e a distribuição ampla por fornecedores de marca branca também dificultam a manutenção e a aplicação de *patches* de segurança. Somado a isso, o ambiente hospitalar, que muitas vezes apresenta redes inseguras, potencializa os riscos de ataques.

A modelagem de risco é uma etapa fundamental na análise de segurança, direcionada a identificar, avaliar e mitigar vulnerabilidades que possam comprometer a integridade, confidencialidade e disponibilidade de sistemas IoMT. Esse processo visa estruturar uma compreensão ampla e detalhada dos potenciais vetores de ataque, considerando as especificidades e interdependências de cada componente do sistema. Ao adotar uma estrutura de modelagem que mapeia ameaças e/ou riscos, busca-se não apenas detectar pontos fracos, mas também visualizar e priorizar estratégias de defesa que possam minimizar impactos de forma sistemática (Cagnazzo *et al.*, 2018).

Segundo Asif *et al.* (2021), “a modelagem de ameaças é uma medida bem aceita para projetar infraestrutura de cibersegurança que ajuda a identificar, enumerar e priorizar ameaças para um sistema, é uma parte da inteligência de ameaças que visa aplicar controles apropriados contra ameaças”. Além disso, ao destacar os desafios de interoperabilidade de dispositivos médicos conectados, e as limitações de conhecimento de segurança cibernética dos operadores dos sistemas, (Almohri *et al.*, 2017) argumenta que a modelagem de ameaças em sistemas médicos conectados é uma questão nova e recente devido às características exclusivas desses sistemas, e que a falta de modelagem ou a modelagem mal aplicada na construção de sistemas médicos pode introduzir vulnerabilidades inéditas suscetíveis a ataques.

A *Food and Drug Administration* (FDA), agência federal norte-americana responsável pela segurança de produtos, medicamentos, produtos biológicos e dispositivos médicos, tem enfatizado a importância da modelagem de ameaças por meio de orientações recentes apresentadas em diversos documentos emitidos pela própria agência e por órgãos parceiros. Além disso, o MITRE, que oferece orientação técnica e soluções tecnológicas para o governo dos EUA, desenvolveu, em colaboração com a FDA, o *Playbook for Threat Modeling Medical Devices*, um manual destinado a ajudar empresas e organizações a desenvolverem e aperfeiçoarem suas práticas de modelagem de ameaças para sistemas médicos conectados (Food and Drug Administration (FDA), 2024; Bochniewicz *et al.*, 2021).

Diante desse cenário, uma atenção especial tem sido dada aos *frameworks* de modelagem de risco. Por exemplo, (Malamas *et al.*, 2021) revisa e avalia diversas metodologias de análise de riscos aplicadas ao contexto da IoMT. Em (Cagnazzo *et al.*, 2018), os autores apresentam uma abordagem de modelagem de ameaças específica para sistemas de saúde móvel. Já (Alsubaei *et al.*, 2017) propõe uma taxonomia de ataques e uma abordagem de avaliação de risco baseada nessa taxonomia. Em (Almohri *et al.*, 2017), os autores utilizam o STRIDE para identificar vulnerabilidades, incluindo ataques à comunicação, software e hardware, destacando como falhas podem comprometer a segurança do paciente. Além disso, propõem contramedidas baseadas em resiliência cibernética e monitoramento em tempo real, enfatizando a importância de uma abordagem sistemática para proteger a integridade e a disponibilidade de sistemas médicos conectados.

3 TRABALHOS RELACIONADOS

No campo da IoMT, a crescente integração de dispositivos conectados em redes de assistência médica tem despertado o interesse de pesquisadores em diversas áreas, especialmente no que se refere à segurança. Nos últimos anos, estudos têm buscado compreender o estado da arte em IoMT, com ênfase na identificação de vulnerabilidades e ameaças que comprometem a segurança e a privacidade dos pacientes e dos dados médicos.

Diante desse cenário, o presente capítulo revisa trabalhos que representam as principais vertentes de pesquisa em modelagem de risco para IoMT. Os trabalhos aqui analisados abordam desde a aplicação de modelos bem estabelecidos, até a elaboração de classificações ou taxonomias de ataques e vulnerabilidades.

3.1 Levantamento bibliográfico

Em (Mnjama *et al.*, 2017), os autores fornecem uma estrutura conceitual de avaliação de ameaças para identificar os elementos necessários para proteger os dispositivos vestíveis de saúde do consumidor. A estrutura consiste em seis elementos principais identificados a partir da tríade CIA e do modelo STRIDE. Além disso, com base em uma arquitetura abstrata de dispositivos vestíveis e um estudo da literatura relacionada, os autores identificaram quatorze vulnerabilidades dentro dos seis elementos do STRIDE.

Ao comparar o trabalho de (Mnjama *et al.*, 2017) com a proposta MedSTRIDE, devemos primeiramente destacar que os autores aqui apenas consideraram os dispositivos do tipo vestível, já o MedSTRIDE considera não apenas os vestíveis como também os dispositivos implantáveis e os equipamentos locais. Além disso, os autores ainda declaram que a propriedade de elevação de privilégio do STRIDE não pode ser considerada em equipamentos vestíveis, pois eles argumentam que essa propriedade concentra-se em sistemas que possuem muitos usuários e que as aplicações de vestíveis só possuem um único usuário. No entanto, nos trabalhos de (Rasool *et al.*, 2022; Yaqoob *et al.*, 2019), vimos que dispositivos vestíveis são altamente propensos a ataques de escalonamento de privilégios, além dos aplicativos que controlam esses dispositivos.

(Almohri *et al.*, 2017), realizaram um trabalho onde os autores examinaram os componentes de sistemas médicos ciberfísicos (MCPS) e as partes interessadas. Com isso, os autores apresentam algumas perspectivas de modelagem para MCPS. Ademais, os autores

esboçaram um modelo de arquitetura abstrata para MCPS e detalham os riscos que MCPS enfrentam, como ameaças à integridade, confidencialidade e disponibilidade dos dados.

A principal contribuição do artigo é um modelo de ameaças voltado para MCPS, o modelo categoriza tipos de ataques específicos com base na Tríade CIA. Esse modelo permite identificar vulnerabilidades em pontos diferentes do sistema, incluindo comunicação, software, hardware e usuários, no entanto, o trabalho ainda carece de validação prática da proposta. Além disso, ao compararmos a Tríade CIA com base do MedSTRIDE que é o STRIDE, podemos perceber que STRIDE já incorpora confidencialidade, integridade e disponibilidade dentro de suas propriedades, além de estender outros aspectos como por exemplo, o não repúdio.

O trabalho de (Malamas *et al.*, 2021), contribui significativamente para a área ao consolidar o conhecimento existente sobre metodologias de avaliação de risco aplicadas à IoMT. Além disso, os autores oferecem uma análise crítica e uma taxonomia das metodologias de avaliação de risco que ajuda a identificar quais abordagens são mais adequadas ou quais necessitam de adaptação. No entanto, apesar desse trabalho não ter como contribuição principal a criação ou adaptação de um *framework* de modelagem de risco, resolvemos considerar-lo, pois os autores apresentam uma tabela STRIDE para classificar os riscos mais comuns identificados em sua revisão de literatura.

Ao comparar a classificação de (Malamas *et al.*, 2021) com MedSTRIDE, é possível perceber que eles apresentam uma mescla entre riscos e alguns tipos de ataques, enquanto que MedSTRIDE apresenta os tipos de ataques para identificação dos riscos. Em *repudiation* por exemplo, os autores classificaram apenas o risco de exclusão de *logs* e alteração de dados, mas não especificaram quais ataques poderiam ser empregados para alcançar tal propósito, pois ao considerar o aspecto do ataque, é possível identificar novos riscos e vulnerabilidades que permanecem ocultas quando focamos apenas no risco.

O trabalho de (Alsubaei *et al.*, 2017) tem como objetivo principal criar uma taxonomia abrangente das ameaças à segurança e à privacidade da IoMT e propor um modelo de avaliação de risco que ajude a entender e gerenciar essas ameaças em ambientes médicos. O trabalho foca em categorizar e avaliar os riscos para facilitar a compreensão dos impactos potenciais e ajudar na criação de contramedidas. No entanto, o MedSTRIDE se difere do modelo de (Alsubaei *et al.*, 2017), pois tem um foco mais direcionado à modelagem de riscos de sistemas de IoMT e não na avaliação do risco. Além disso, outra diferença é que (Alsubaei *et al.*, 2017) classificou os ataques com base nas camadas e nos tipos de dispositivos IoMT (vestível, implan-

tável e local), enquanto que nossa proposta fornece modelos de genéricos de ativos componentes do sistema, e adapta os ataques as categorias de ameaça do STRIDE para se ajustar aos requisitos únicos do ambiente médico, priorizando a identificação de vulnerabilidades e propondo uma estrutura para mapear ameaças com base nos ativos críticos do sistema.

Em (Khan *et al.*, 2017), a contribuição principal dos autores foi a formalização de uma metodologia sistemática para caracterização de ameaças de sistemas ciber-físicos usando a abordagem STRIDE. Os autores utilizam o STRIDE como uma base para classificar ameaças em sistemas ciber-físicos, mas adaptaram as categorias para refletir as interações e vulnerabilidades específicas entre componentes lógicos e físicos. A metodologia envolve a criação de Digrama de Fluxo de Dados (DFD) e a identificação de pontos críticos onde as categorias STRIDE são mais relevantes em um contexto ciber-físico.

No entanto, para testar seu método os autores realizaram a modelagem em um sistema *smart grid*, enquanto que o MedSTRIDE também usa o STRIDE como base, mas adapta suas categorias de ameaça para refletir o cenário específico da IoMT com base em ataques comuns aos dispositivos. Além disso, a proposta do MedSTRIDE inclui uma generalização de DFD para identificação de vulnerabilidades em componentes da rede ciber-física para cinco ativos críticos médicos, como *firmware*, *hardware* e protocolos de comunicação.

O trabalho de (Cagnazzo *et al.*, 2018) visa criar um modelo de ameaças específico para sistemas de saúde móvel (mHealth), onde dispositivos portáteis (*smartphones*, *wearables*) desempenham um papel essencial no monitoramento de saúde e na coleta de dados do paciente. Os autores usaram STRIDE para identificar os principais riscos de uma arquitetura de mHealth e aplicaram o modelo DREAD para classificar o impacto de cada risco identificado. No entanto como os próprios autores registram em seu trabalho, essa contribuição fornece uma visão geral de alto nível das ameaças, sendo necessário a realização de uma análise de ameaças específica para casos particulares de sistemas médicos.

Em (Omotosho *et al.*, 2019), os autores concentraram seus esforços na identificação e classificação de ameaças para onze tipos de dispositivos de IoMT. O *framework* STRIDE foi utilizado pra a identificação das ameaças e o DREAD para a classificação do risco, além disso, os autores ainda criaram um sistema web com o modelo proposto.

A diferença entre MedSTRIDE e o trabalho de (Omotosho *et al.*, 2019), é que MedSTRIDE é uma proposta geral para a identificação de riscos de IoMT, enquanto que a proposta de (Omotosho *et al.*, 2019) foca em onze tipos de dispositivos específicos. Devemos

considerar o fato de existirem uma grande variedade de dispositivos IoMT, e novos dispositivos surgem o tempo todo, logo considerar ameaças para onze tipos de dispositivos é uma contribuição válida, mas que deixa uma grande quantidade de dispositivos médicos descoberta.

3.2 Avaliação Qualitativa

Com base no levantamento dos trabalhos relacionados, elaboramos uma tabela comparativa entre eles, considerando oito critérios de avaliação que se mostram relevantes para modelos de identificação de riscos em IoMT. Os critérios não tem ordem de importância e são identificados por siglas. Na Tabela 4 apresentamos a comparação entre a proposta MedSTRIDE e os trabalhos relacionados a este estudo.

1. **C1:** Ampla cobertura de dispositivos IoMT (abrange dispositivos vestíveis, implantáveis e equipamentos locais e outros);
2. **C2:** Considera partes críticas (ativos) de um componente do sistema médico como vetor de exploração;
3. **C3:** Considera o fluxo de dados da rede médica para identificação de vulnerabilidades;
4. **C4:** Considera componentes da camada de adaptação para identificação de vulnerabilidades;
5. **C5:** Propõe metodologia sistemática para identificação de vulnerabilidades;
6. **C6:** Atende aos aspectos Confidencialidade, Integridade, Disponibilidade, Autenticação, Autorização e Não-repúdio;
7. **C7:** Classificação ou taxonomia de ataques de IoMT para identificação de vulnerabilidades;
8. **C8:** Validação prática do modelo.

3.2.1 Discussão sobre a relevância dos critérios de avaliação

A seleção dos critérios de avaliação é essencial para garantir uma análise abrangente e relevante de metodologias de segurança no contexto de IoMT. O critério **C1** (Ampla cobertura de dispositivos IoMT) é fundamental, pois o ecossistema IoMT dispõe de uma diversidade de dispositivos médicos conectados, incluindo os vestíveis, implantáveis, ingeríveis e equipamentos locais. Cobrir essa variedade é crucial para assegurar que o modelo avaliado seja eficaz em proteger uma ampla gama de dispositivos médicos, reconhecendo as diferentes demandas e vulnerabilidades associadas a cada tipo de dispositivo.

Tabela 4 – Comparação entre propostas para modelagem de risco.

Modelo	C1	C2	C3	C4	C5	C6	C7	C8
(Mnjama <i>et al.</i> , 2017)			✓	✓	✓	✓		
(Almohri <i>et al.</i> , 2017)	✓	✓	✓	✓	✓		✓	
(Malamas <i>et al.</i> , 2021)	✓	✓	✓	✓		✓		
(Alsubaei <i>et al.</i> , 2017)	✓	✓	✓	✓			✓	
(Khan <i>et al.</i> , 2017)					✓	✓		
(Cagnazzo <i>et al.</i> , 2018)			✓	✓	✓	✓	✓	
(Omotosho <i>et al.</i> , 2019)		✓	✓		✓	✓	✓	
MedSTRIDE	✓	✓	✓	✓	✓	✓	✓	✓

Fonte: Elaborada pelo autor.

O **C2** (Considera partes críticas de um componente do sistema médico como vetor de exploração) justifica-se pela necessidade de identificar vulnerabilidades específicas em componentes essenciais do sistema, que, quando exploradas, podem comprometer diretamente a integridade e a funcionalidade do dispositivo médico. Um enfoque nos ativos críticos ajuda a alinhar o modelo de segurança com os elementos mais suscetíveis de comprometer a saúde e a segurança dos pacientes.

O **C3** (Considera o fluxo de dados da rede médica para identificação de vulnerabilidades) é igualmente indispensável, pois o fluxo de dados em uma rede médica conecta múltiplos dispositivos e sistemas que compartilham informações sensíveis. Mapear essas interações permite identificar potenciais pontos de vulnerabilidade, reduzindo o risco de comprometer a confidencialidade e a integridade dos dados de saúde, essenciais para o funcionamento seguro de sistemas médicos conectados.

O critério **C4** (Consideração de componentes da camada de adaptação para identificação de vulnerabilidades) destaca-se pela importância de uma visão holística. A camada de adaptação, que gerencia a comunicação e a interoperabilidade entre dispositivos médicos e sistemas de controle, pode ser um ponto fraco se negligenciada. Incluir essa camada na análise oferece uma proteção mais robusta, considerando todo o ecossistema médico.

O **C5** (Proposição de metodologia sistemática para identificação de vulnerabilidades) é crucial, pois uma abordagem sistemática assegura que as vulnerabilidades sejam identificadas de maneira estruturada e consistente. Modelos sem uma metodologia clara podem deixar lacunas e, assim, comprometer a confiabilidade dos resultados, especialmente em ambientes onde a segurança é crítica.

Os aspectos de Confidencialidade, Integridade, Disponibilidade, Autenticação, Autorização e Não-repúdio (**C6**) são padrões reconhecidos na segurança da informação e essenciais no contexto de IoMT. Incorporar esses aspectos como critérios garante que a avaliação cubra um espectro completo de requisitos de segurança, evitando comprometer informações sensíveis e protegendo a continuidade e confiabilidade dos dispositivos médicos. O MedSTRIDE incorpora cada um desses aspectos ao estender as propriedades do STRIDE (Shostack, 2014).

A **C7** (Classificação ou taxonomia de ataques de IoMT para identificação de vulnerabilidades) é um critério essencial, pois fornece uma estrutura organizada que facilita o entendimento e a análise dos diferentes tipos de ameaças que podem afetar dispositivos e redes no ecossistema IoMT. Ao classificar os ataques, é possível identificar padrões de vulnerabilidade, mapear vetores de ataque comuns e priorizar medidas de mitigação conforme o tipo de ameaça e o impacto esperado.

Por fim, o critério **C8** (Validação prática do modelo) assegura que a metodologia não seja apenas teórica, mas também eficaz quando aplicada a casos reais. A validade prática de um modelo é crucial para demonstrar sua aplicabilidade e impacto em situações concretas, oferecendo confiança aos stakeholders quanto à sua eficácia na mitigação de riscos em ambientes IoMT.

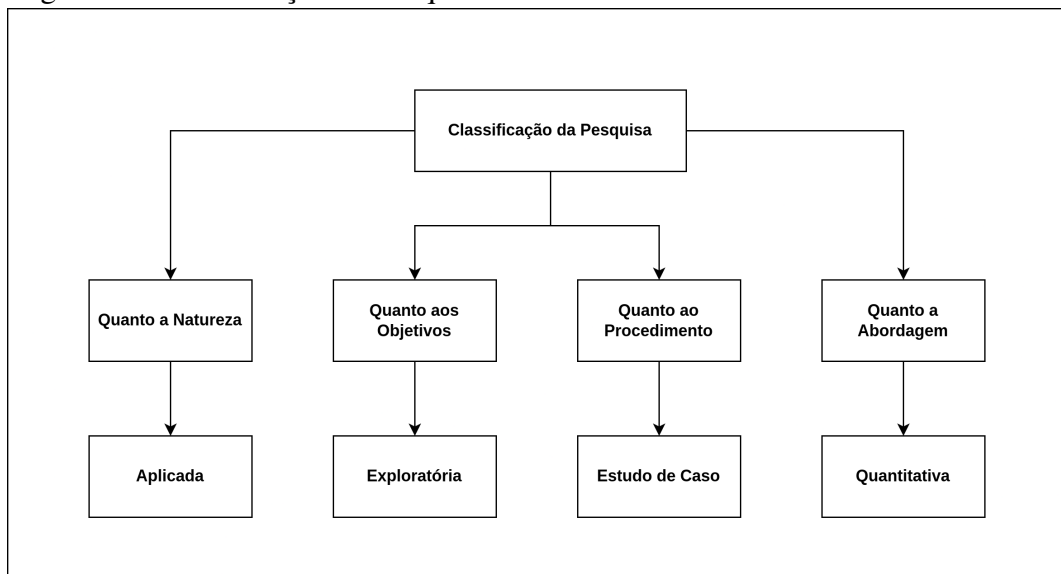
4 METODOLOGIA

Neste capítulo, detalhamos a execução desta pesquisa, abordando aspectos como classificação, estruturação e as ferramentas empregadas ao longo do processo.

4.1 Classificação da Pesquisa

A classificação desta pesquisa conforme o exposto na Figura 7, foi fundamentada nos conceitos e nas orientações propostas por Prodanov e Freitas, conforme descrito em (Prodanov; Freitas, 2013). Esse referencial forneceu as bases metodológicas para estruturar e categorizar a investigação, garantindo a adoção de critérios científicos amplamente reconhecidos para a condução do estudo.

Figura 7 – Classificação da Pesquisa.



Fonte: Adaptada de (Prodanov; Freitas, 2013).

Do ponto de vista da natureza, esta pesquisa é classificada como aplicada, pois busca gerar conhecimentos voltados para a solução de problemas específicos. O objetivo principal é desenvolver diretrizes práticas que contribuam para a identificação de falhas de segurança em dispositivos de IoMT, promovendo benefícios diretos para a área da saúde e a segurança de sistemas médicos.

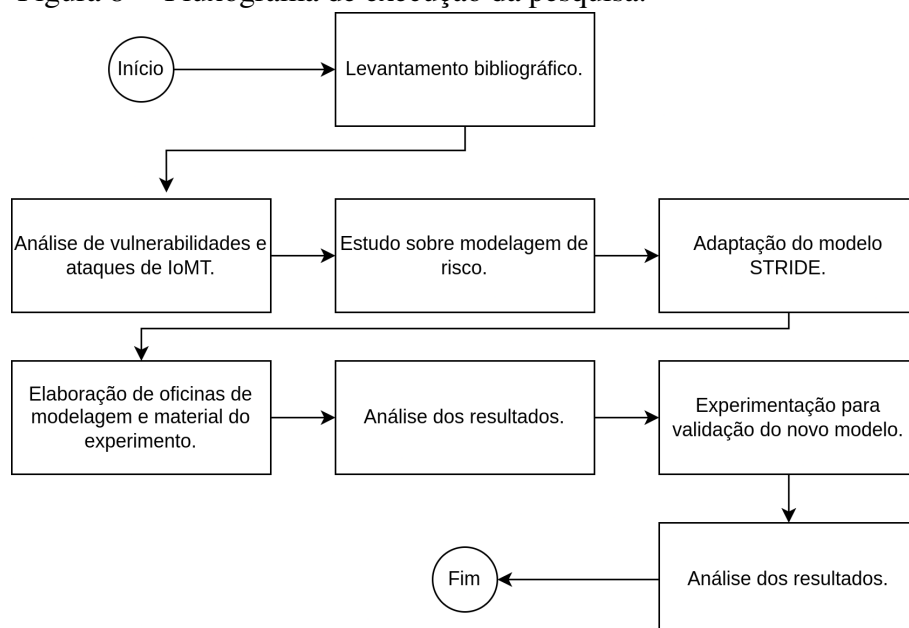
Quanto aos objetivos, esta pesquisa é classificada como exploratória, uma vez que busca aprofundar o entendimento sobre os problemas de segurança em dispositivos IoMT através de levantamento bibliográfico relevante. Além disso, hipóteses foram formuladas com o intuito de descobrir novas perspectivas a respeito da modelagem de risco com STRIDE.

Quanto ao procedimento, esta pesquisa adota o método de estudo de caso comparativo. A análise foi realizada com base em um cenário específico envolvendo uma bomba de infusão de medicamentos, onde os participantes aplicaram tanto o modelo STRIDE quanto o MedSTRIDE para a modelagem de risco. Além disso, utilizamos uma abordagem quantitativa que permite comparar os resultados obtidos a partir de cada método, avaliando suas diferenças, vantagens e limitações. Ao final, os dados são analisados e comparados, possibilitando uma compreensão mais aprofundada sobre a eficácia dos dois modelos no contexto da segurança de dispositivos IoMT.

4.2 Procedimentos de Realização da Pesquisa e Ferramentas Utilizadas

Inicialmente, os passos comuns de pesquisa foram executados a fim de estabelecer a definição do tema, os objetivos e as questões de pesquisa que serviriam de base para este trabalho. Os procedimentos empregados na realização desta pesquisa foram cuidadosamente planejados para garantir a confiabilidade e a validade dos resultados. Além das etapas iniciais, a pesquisa foi conduzida em sete etapas principais: levantamento bibliográfico, análise de vulnerabilidades e ataques de IoMT, estudo sobre modelagem de risco, adaptação do modelo STRIDE, elaboração de oficinas de modelagem de risco e material para o experimento, experimentação para validação e análise dos resultados. O fluxograma na Figura 8 representa a sequência de etapas de execução dessa pesquisa.

Figura 8 – Fluxograma de execução da pesquisa.



Fonte: Elaborada pelo autor.

O levantamento bibliográfico foi realizado com o objetivo de mapear o estado da arte em segurança da IoMT, como ataques e vulnerabilidades conhecidas no domínio médico conectado. Além disso, realizamos uma busca por *frameworks* de modelagem de risco aplicados à IoMT, e também novas extensões de *frameworks* para esse contexto.

Para realização desta pesquisa, realizamos um levantamento bibliográfico nas bases de dados IEEE, *Science Direct* e *Wiley Online Library*. É importante destacar que priorizamos a seleção de trabalhos relevantes, publicados em revistas, congressos e capítulos de livros relevantes. Além disso, também consideramos literatura cinza ao analisar relatórios técnicos de empresas e organizações públicas como NIST, FBI e FDA, por exemplo. A Tabela 5 apresenta as bases de dados e as respectivas *strings* de busca utilizadas. Além disso, foram priorizados artigos publicados nos últimos oito anos.

Tabela 5 – *Strings* de busca utilizadas nas bases de dados selecionadas.

Base de Dados	String de Busca
IEEE Xplore (Busca por ataques e vulnerabilidades de IoMT)	((("Author Keywords": "medical devices" OR "Author Keywords": "Internet of Medical Things" OR "Author Keywords": "IoMT security" OR "Author Keywords": "healthcare systems") AND ("Author Keywords": "security vulnerabilities" OR "Author Keywords": "encryption attacks" OR "Author Keywords": "network attacks" OR "Author Keywords": "privacy")) OR (("Document Title": "medical devices" OR "Document Title": "Internet of Medical Things" OR "Document Title": "IoMT security framework" OR "Document Title": "healthcare systems") AND ("Document Title": "security vulnerabilities" OR "Document Title": "encryption attacks" OR "Document Title": "network attacks" OR "Document Title": "privacy")) OR (("Abstract": "medical devices" OR "Abstract": "Internet of Medical Things" OR "Abstract": "IoMT security" OR "Abstract": "healthcare systems") AND ("Abstract": "security vulnerabilities" OR "Abstract": "encryption attacks" OR "Abstract": "network attacks" OR "Abstract": "privacy"))
IEEE Xplore (Busca por modelagem de risco em IoMT)	((("Consumer Health" AND Wearables AND Privacy AND Security) OR ("Threat Modeling" AND ("Medical Cyber-Physical Systems" OR "Mobile Health Systems"))) OR ("Risk Assessment" AND "Internet of Medical Things" AND Security AND Vulnerability) OR ("Taxonomy" AND "Internet of Medical Things" AND Privacy AND "Risk Assessment") OR (STRIDE AND "Threat Modeling" AND "Cyber-Physical Systems"))
Science Direct (Busca por ataques e vulnerabilidades de IoMT)	(Healthcare AND "Internet of Medical Things" AND Security AND Privacy) OR (Healthcare AND IoMT AND "Medical Cyber Physical Systems" AND "Medical Devices")
Wiley Online Library (Busca por ataques e vulnerabilidades de IoMT)	("Internet of Medical Things" AND Security AND "Security Threats" AND Privacy AND Healthcare) OR ("Internet of Medical Things" AND ("Security" OR "Security Threats") AND "Privacy" AND Healthcare)

Fonte: Elaborada pelo autor.

Ainda algumas ferramentas foram utilizadas para apoiar nossa revisão, como Elicit, Litmaps e ResearchRabbit. O Elicit, por exemplo, foi importante na identificação dos trabalhos mais relevantes relacionados a revisão de literatura sobre ataques, vulnerabilidades e contramedidas. As ferramentas Elicit e Litmaps também nos auxiliaram na análise das relações entre os trabalhos selecionados.

Na fase de análise de vulnerabilidades e ataques de IoMT, realizou-se um estudo detalhado das vulnerabilidades e dos ataques mais relevantes que afetam dispositivos da IoMT.

A análise incluiu a revisão de literatura científica e técnica, além de casos documentados de ataques em ambientes reais, com o objetivo de identificar os principais vetores de ataque, falhas de segurança e ameaças que impactam os dispositivos e os dados sensíveis que eles processam. Esse levantamento foi essencial para compreender os desafios de segurança específicos deste domínio e subsidiar as próximas etapas da pesquisa.

A modelagem de risco envolveu um estudo aprofundado sobre técnicas e modelos de identificação de riscos voltados para sistemas IoT e, em especial, para o contexto de dispositivos IoMT. O objetivo foi identificar as abordagens mais eficazes e adaptáveis à identificação, categorização e mitigação de riscos em sistemas médicos conectados. O estudo incluiu tanto métodos tradicionais de modelagem de risco quanto adaptações recentes aplicadas a cenários específicos da IoMT.

Com base no conhecimento adquirido nas fases anteriores, o modelo STRIDE, amplamente utilizado para análise de riscos, foi adaptado para atender às particularidades da IoMT. A adaptação considerou as características únicas deste ambiente, como protocolos de comunicação, restrições de energia e diversos outros aspectos inerentes a sistemas médicos. Essa customização visou preencher lacunas existentes no modelo original e proporcionar uma abordagem mais adequada à mitigação de ameaças em sistemas IoMT.

Para validar a adaptação do modelo STRIDE, foram elaborados materiais didáticos e oficinas práticas de modelagem. Esses recursos foram projetados para capacitar os participantes no uso do modelo adaptado, assegurando que compreendessem os conceitos fundamentais e pudessem aplicá-los em cenários simulados. As oficinas serviram como base para a experimentação e coleta de dados.

Na fase de experimentação, o modelo adaptado foi submetido a testes práticos para validar sua eficácia. Foram realizados experimentos controlados, nos quais participantes aplicaram o modelo adaptado em um estudo de caso baseado em um sistema de bomba de infusão de medicamentos. Os resultados obtidos durante essa etapa foram comparados com o modelo tradicional para avaliar a precisão, a aplicabilidade e a capacidade do novo modelo em mitigar riscos.

Por fim, os dados coletados durante a experimentação foram analisados de forma sistemática, utilizando métricas quantitativas. A análise buscou verificar a eficácia do modelo adaptado na identificação e mitigação de ameaças, bem como sua conformidade com as necessidades específicas da IoMT. Os resultados foram consolidados para subsidiar as conclusões da

pesquisa e propor futuras melhorias no modelo.

5 MEDSTRIDE: UM FRAMEWORK PARA ANÁLISE DE RISCO E PREVENÇÃO DE ATAQUES CIBERNÉTICOS EM SISTEMAS MÉDICOS

A identificação e a priorização de ameaças, intrínsecas ao processo de modelagem, constituem um pilar fundamental para a construção de sistemas robustos e seguros. Ao antecipar possíveis ataques e suas consequências, a modelagem de ameaças possibilita a implementação de medidas de segurança eficazes, reduzindo a probabilidade de incidentes e minimizando seus impactos. A compreensão aprofundada das ameaças e a adoção de mitigações adequadas são, portanto, imperativas para garantir a confidencialidade, integridade e disponibilidade da informação (Asif *et al.*, 2021; Chantzis *et al.*, 2021).

Segundo o relatório técnico sobre modelagem de ameaças centrada em dados, realizado pelo *National Institute of Standards and Technology* (NIST), “O objetivo da modelagem de ameaças é reduzir vulnerabilidades de software, impedir classes específicas de invasores, melhorar a segurança geral do sistema, proteger tipos específicos de dados, e outros” (Souppaya; Scarfone, 2016).

A modelagem de risco em sistemas de IoMT representa um desafio significativo devido à complexidade inerente desses ecossistemas, que combinam dispositivos médicos conectados, redes de comunicação, infraestrutura de armazenamento e processamento de dados. O principal objetivo da modelagem é identificar, avaliar e mitigar ameaças que possam comprometer o sistema. Entretanto, a vasta heterogeneidade tecnológica entre os dispositivos, o uso de diferentes protocolos de comunicação e a interação com ambientes críticos de saúde aumentam a dificuldade de prever e mapear com precisão todos os possíveis vetores de ataque.

Além disso, a modelagem de risco em IoMT deve considerar não apenas as ameaças tradicionais da segurança cibernética, como ataques DoS, injeções de código e espionagem de dados, mas também riscos físicos devem ser considerados. Fatores como a sensibilidade dos dados médicos, a necessidade de resposta em tempo real dos dispositivos e as regulamentações específicas do setor de saúde tornam a avaliação de riscos mais complexa, exigindo uma abordagem multidisciplinar que envolva especialistas em segurança cibernética, engenheiros de sistemas e profissionais de saúde.

Outro aspecto crítico da modelagem de risco é a dificuldade de prever a evolução das ameaças ao longo do tempo. Novos ataques e vulnerabilidades surgem à medida que os sistemas IoMT se expandem, o que demanda que as metodologias de modelagem de risco sejam dinâmicas e continuamente atualizadas. Além disso, como os dispositivos IoMT frequentemente

operam em ambientes com recursos limitados, como energia e capacidade de processamento, o desenvolvimento de contramedidas eficazes pode ser limitado, exigindo estratégias de mitigação que equilibrem segurança e eficiência operacional.

Portanto, o esforço de modelar riscos em sistemas IoMT exige uma abordagem integrada e iterativa, onde a segurança é tratada como um componente central desde as fases iniciais de concepção e desenvolvimento. Soluções tradicionais de modelagem de risco podem não ser suficientes, sendo necessária a adaptação ou incorporação de recursos adicionais aos *frameworks*, recursos que possibilitem uma melhor identificação dos riscos e que considerem as especificidades dos sistemas médicos conectados.

Diante desse cenário, o principal objetivo deste trabalho adaptar o *framework* STRIDE, a fim de que ele seja capaz de acomodar aspectos específicos de IoMT. Conforme representado na Figura 6, esse trabalho tem por intuito aprimorar duas fases importantes do processo de modelagem de risco, a fase três que consiste na decomposição dos componentes da arquitetura, e a fase quatro onde se realiza a identificação de riscos dos ativos, reduzindo o esforço para identificação dos ativos e melhorando o processo de identificação dos riscos.

As principais contribuições do trabalho são:

- MedSTRIDE: Um *framework* baseado em STRIDE para modelagem de risco com foco no modelo geral de rede de IoMT
- Uma classificação STRIDE dos principais tipos de ataques que podem ser empregados em sistemas médicos;
- Uma classificação genérica de ativos de sistema IoMT baseada no modelo de rede de sistemas médicos.

5.1 O Modelo Proposto

A modelagem de riscos é um processo técnico e analítico, que visa mapear as possíveis ameaças, vulnerabilidades e seus impactos em um sistema específico. Em geral, o processo de modelagem de risco tem como resultado uma representação detalhada que permite entender os pontos de falha e as interações entre os componentes do sistema e os riscos associados.

Ao adotar uma metodologia de modelagem de risco, é crucial compreender as distinções entre os diferentes modelos, incluindo o processo e os objetivos específicos de cada abordagem. Adicionalmente, as metodologias focam em aspectos específicos, como a avaliação de ameaças, a identificação de vulnerabilidades e a compreensão de impacto (Shevchenko *et*

al., 2018). No entanto, (Shostack, 2014) diz que é preferível centrar-se em um modelo com apenas um objetivo específico, pois a combinação de muitos modelos tende a tornar a modelagem confusa.

Escolhemos aprimorar o STRIDE para IoMT por se tratar de um *framework* consolidado, e que tem sido objeto de estudo para a realização de modelagem de risco de sistemas de IoT em geral, incluindo IoMT (Khan *et al.*, 2017; Asif *et al.*, 2021; Cagnazzo *et al.*, 2018; Omotosho *et al.*, 2019; Mnjama *et al.*, 2017).

Além disso, no contexto de segurança, é mais fácil identificar vulnerabilidades e propor contramedidas do que identificar as ameaças e eliminá-las, pois as vulnerabilidades são fraquezas específicas e identificáveis do sistema, como, por exemplo, uma configuração incorreta, falha de autenticação ou software desatualizado. Essas vulnerabilidades são elementos técnicos concretos onde normalmente podem ser antevistas por meio de modelagem de risco, ou ferramentas automatizadas e inspeções manuais (Shostack, 2014).

Segundo Shevchenko *et al.* (2018), “O STRIDE avalia o projeto detalhado do sistema. O objetivo da etapa é modelar o sistema no local. Ao construir diagramas de fluxo de dados, você identifica entidades do sistema, eventos e limites do sistema”. As entidades do sistema, eventos e limites de confiança citados em Shevchenko *et al.* (2018), são o que chamamos nesse trabalho de ativos. Os ativos são essencialmente importantes para o processo de modelagem, pois é a partir dos ativos que realizamos o exercício para identificação dos pontos fracos do sistema.

Contudo, os ativos usados no processo de modelagem implicam em algumas dificuldades. De acordo com Shostack (2014), não existe um caminho direto entre os ativos e as ameaças, nem um conjunto bem definido de etapas a serem seguidas. Ele destaca que o tempo investido na identificação de ativos acaba sendo um tempo que poderia ser dedicado à detecção ou mitigação de ameaças. Adicionalmente, Shostack (2014) argumenta a necessidade que especialistas têm de discutir o que constitui um ativo ou qual tipo de ativo está sendo abordado, e mesmo que isso gere uma lista de ativos a serem observados no modelo, o autor sugere que seria mais produtivo construir o modelo diretamente.

Considerando o exposto, na Subseção 5.1.1, o modelo MedSTRIDE oferece uma generalização de ativos de componentes para a camada física e a camada de adaptação. Esses ativos servem como uma base para reduzir o gasto de tempo e esforço no processo de decomposição da arquitetura da IoMT. Além disso, na Subseção 5.1.2, apresentamos a classificação baseada no modelo STRIDE, aplicada aos 22 tipos de ataques comuns da IoMT. Essa classificação

pode auxiliar especialistas em modelagem de risco e profissionais de cibersegurança a mapear vulnerabilidades e identificar possíveis falhas em sistemas médicos conectados. Por fim, um processo sistemático de modelagem de risco com MedSTRIDE é apresentado na Subseção 5.1.3.

5.1.1 Ativos Genéricos Baseados no Modelo de Rede de IoMT

O modelo de rede apresentado na Figura 9 é uma adaptação da arquitetura geral de IoT descrita por (Chowdhury *et al.*, 2015). Além disso, também nos baseamos nos modelos de rede de IoMT apresentados por (Yaqoob *et al.*, 2019; Ghubaish *et al.*, 2020; Yaacoub *et al.*, 2020; Sun *et al.*, 2019; Rasool *et al.*, 2022). Esse modelo é de vital importância para entendermos as características da arquitetura básica de IoMT, ele também foi utilizado como base para identificação dos ativos que compõem os modelos genéricos dessa proposta. Uma discussão detalhada dessa arquitetura foi realizada na Subseção 2.2.1.

Sob uma perspectiva defensiva, a identificação de ativos de um sistema desempenha um papel central, permitindo que analistas de segurança foquem em vulnerabilidades específicas. Essa abordagem permite que as vulnerabilidades sejam identificadas de maneira estruturada, possibilitando um melhor direcionamento dos esforços de mitigação. O processo de identificação, em geral, é iterativo, iniciando com uma avaliação abrangente de todas as vulnerabilidades potenciais que podem impactar cada ativo do sistema.

De acordo com Shostack (2014), conceito de ativo, de maneira geral, é associado a um elemento de valor dentro de um sistema. No contexto da modelagem de ameaças, ativos são frequentemente considerados como componentes que um invasor poderia almejar acessar, manipular ou danificar.

Além disso, a ausência de uma compreensão compartilhada entre os envolvidos sobre o que constitui um ativo pode comprometer a eficácia do processo, levando a mal-entendidos ou discussões improdutivas. Dessa forma, estabelecer um consenso sobre o significado e a relevância dos ativos no início da modelagem é fundamental para assegurar a clareza e a cooperação ao longo do processo, contribuindo para uma identificação e priorização mais precisa das vulnerabilidades.

Para Shostack (2014), o termo “ativo” pode ser interpretado de três maneiras distintas, são elas:

- Coisas que os atacantes querem;
- Coisas que você quer proteger;

- Ativos trampolins (ou caminho das pedras).

Geralmente, as coisas que os atacantes querem podem ser compreendidas por ativos “tangíveis”, isto é, bancos de dados médicos, acesso a configurações de sistema, chaves criptográficas, protocolos e outros. As coisas que você quer proteger, não necessariamente são ativos “tangíveis”, mas também intangíveis. No contexto de sistemas médicos conectados, ativos intangíveis podem ser compreendidos por reputação da empresa, confiança dos pacientes, e a credibilidade dos dispositivos ou sistemas usados. Não menos importante, os ativos trampolins são elementos que, embora possam não ser os principais alvos de um ataque, no entanto, servem como pontos de acesso ou facilitadores para atingir ativos mais valiosos. Esses ativos têm a capacidade de levar um invasor a outros ativos que ele realmente deseja comprometer (Shostack, 2014).

Essas diferentes interpretações refletem as várias perspectivas ou enfoques que profissionais e especialistas podem ter ao se referirem a um ativo dentro do processo de modelagem. Ao introduzir essas três formas de uso, sugerimos que uma compreensão mais precisa do termo é essencial para garantir que todos os envolvidos na modelagem de ameaças estejam alinhados em relação ao que está sendo protegido e por que.

Figura 9 – Modelo de rede de IoMT baseado em arquitetura de quatro camadas.



Fonte: Elaborada pelo autor.

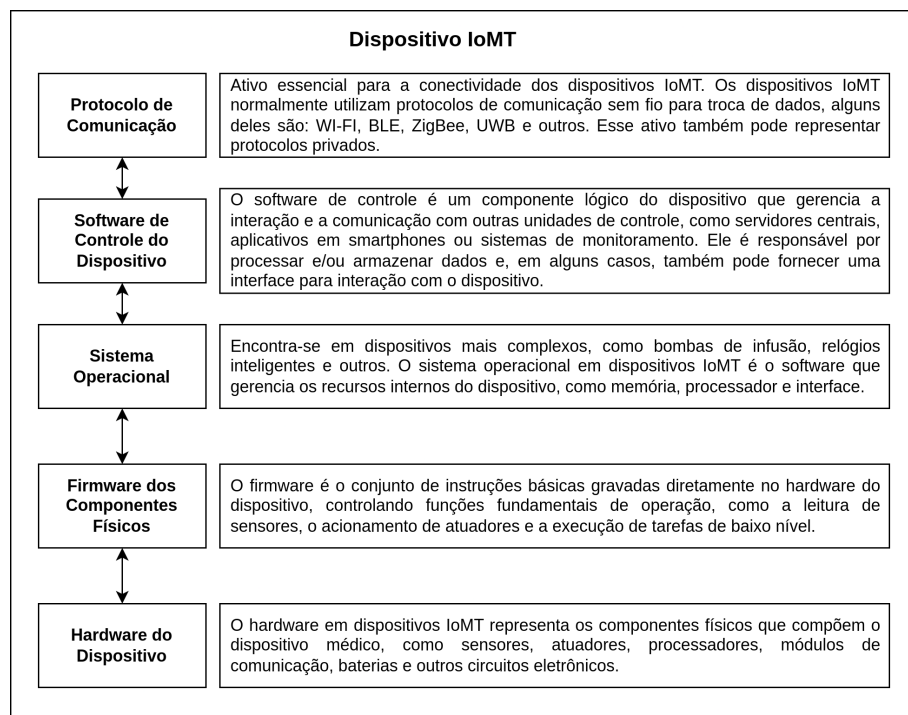
Por fim, os ativos apresentados neste estudo constituem um ponto de partida para a modelagem de risco, não representando a modelagem final. A natureza modular da arquitetura permite a inclusão, exclusão ou adaptação de ativos, de acordo com a expertise do especialista e as particularidades do contexto em análise. Essa flexibilidade assegura que a modelagem de

risco seja personalizada e capaz de capturar os riscos específicos do sistema em questão.

5.1.1.1 Generalização de ativos para a camada física

Para justificar a generalização dos ativos propostos para dispositivos da camada física, é importante considerar a natureza essencial desses elementos na configuração física e lógica dos diversos dispositivos médicos, sejam eles, implantáveis, vestíveis ou equipamentos locais. Conforme representado na Figura 10, a seleção dos ativos que inclui o protocolo de comunicação, software de controle, sistema operacional, *firmware* e *hardware*, busca contemplar os principais elementos críticos envolvidos no funcionamento de dispositivos da camada física de IoMT, devido a exposição de ameaças potenciais (Yaqoob *et al.*, 2019).

Figura 10 – Ativos genéricos para modelagem de risco dos dispositivos da borda de IoMT.



Fonte: Elaborada pelo autor.

O protocolo de comunicação representa um ponto de interação fundamental entre os dispositivos da borda e seus sistemas de configuração e controle que rodam na camada de adaptação. O protocolo de comunicação é responsável pela transferência de dados, que deve ser realizada de forma segura e eficiente, protocolos como Wi-Fi, *Zigbee*, *Bluetooth* e outros são frequentemente utilizados em dispositivos médicos, o que exige uma avaliação detalhada de sua segurança e confiabilidade.

O software de controle desempenha um papel central na interface entre o dispositivo médico e o sistema ou usuário que o monitora ou configura. Em alguns dispositivos como bombas de infusão de medicamentos, bombas de insulina e monitores de sinais vitais, esse ativo é responsável pelo recebimento e execução de comandos, o que implica que sua integridade e autenticidade são essenciais para a prevenção de comandos não autorizados ou maliciosos.

O sistema operacional, por sua vez, constitui a base sobre a qual vários dispositivos médicos operam. Os dispositivos que possuem um SO pode variar desde dispositivos simples como *smartwatches* até dispositivos de uso mais crítico como bombas de infusão, respiradores, monitores cardíaco e outros. O sistema operacional é responsável por gerenciar a execução de tarefas e recursos, o que o torna um alvo em potencial para exploração, caso não seja devidamente protegido.

O *firmware* é outro ativo crítico, pois representa o conjunto de instruções específicas que controla o funcionamento de sensores e atuadores. A modificação não autorizada desse componente pode levar à falhas no dispositivo ou à alteração das suas funções, colocando em risco a segurança dos pacientes.

Por fim, o hardware é o elemento físico que compõe o dispositivo. Vulnerabilidades ou falhas em seus componentes podem abrir brechas para ataques de baixo nível que exploram a infraestrutura física, afetando o funcionamento do dispositivo.

Esse conjunto de ativos foi proposto com o objetivo de abranger os principais elementos estruturais dos dispositivos médicos conectados. Entretanto, o modelo mantém flexibilidade para acomodar contextos específicos, permitindo a inclusão de novos ativos ou a exclusão de elementos que não sejam aplicáveis a determinadas aplicações. Essa adaptabilidade torna o modelo aplicável a uma ampla gama de dispositivos no ecossistema de IoMT, reforçando sua relevância como estrutura para análise de segurança.

5.1.1.2 Generalização de ativos para o dispositivo de coordenação e gerenciamento

A generalização dos ativos para o dispositivo de coordenação e gerenciamento (DCG) visa estabelecer uma base para a identificação de vulnerabilidades desses dispositivos médicos. Esse dispositivo em específico, pode ser caracterizado como um smartphone ou PDA equipado com um aplicativo de controle que permite a comunicação entre o usuário e o dispositivo médico, oferecendo uma interface essencial para a operação e configuração dos dispositivos IoMT. Conforme apresentado na Figura 11, a generalização de ativos para esses dispositivos

incluem: Interface Restritiva de Usuário, Protocolo de Comunicação, Software de Controle, Banco de dados, Sistema Operacional, *Firmware* e *Hardware*.

A interface restritiva de usuário constitui o ponto de contato direto entre o operador (médico, técnico ou paciente) e o dispositivo médico. É através dela que se emitem comandos, ajustam-se configurações e monitoram-se os dados enviados pelo dispositivo médico. Devido à sua importância, esta interface deve ser protegida contra acessos não autorizados, injeção de código e outros.

O protocolo de comunicação do DCG representa tecnologias que permitem a comunicação entre o DCG e os dispositivos médicos, o DCG e o gateway, e entre o DCG e a nuvem médica. A segurança para esse ativo é crítica, pois qualquer falha pode permitir a interceptação ou a modificação de dados que trafegam entre os componentes do sistema.

O software de controle consiste basicamente em um aplicativo instalado no DCG, dentre algumas de suas funções, ele é responsável por estabelecer conexão com os dispositivos médicos e demais componentes da arquitetura, interpretar e enviar comandos do usuário, exibir informações e em alguns casos lidar com o banco de dados. Em razão desse ativo ser o ponto intermediário entre o usuário e o dispositivo médico, exige-se que a construção do software do DCG seja realizada com base em critérios e boas práticas que possam garantir a qualidade e confiabilidade desse serviço, isso inclui mecanismos de validação de entrada, testes de funcionalidades e criptografia para garantir que somente comandos autorizados sejam transmitidos.

O banco de dados é um ativo relevante, pois em muitos casos o DCG precisa armazenar dados temporários ou permanentes como configurações, histórico de comandos e dados do paciente. Dispositivos como bombas de infusão de medicamentos e insulina tendem a guardar configurações como bibliotecas de medicamentos e alimentos, além disso, monitores cardíacos e *wearebles* tendem a armazenar históricos do usuário, já os dispensadores de medicamentos precisam armazenar dosagens e horários. Esse armazenamento deve ser seguro, protegendo informações sensíveis contra acessos não autorizados e garantindo a privacidade e integridade dos tratamentos e dos dados do paciente.

O sistema operacional do DCG fornece a base sobre a qual o software de controle e a interface funcionam. Dispositivos como *smartphones* e PDAs utilizam sistemas operacionais complexos (como Android, iOS e outros), esses ativos precisam ser protegidos contra vulnerabilidades que possam comprometer o sistema e abrir brechas para acessos indevidos.

O *firmware* compreende o conjunto de instruções que controla diretamente o hardware e auxilia o sistema operacional na interação com os componentes físicos do DCG. Este ativo pode ser considerado redundante para o caso de um *smartphone* ou *tablet*, pois o sistema operacional pode assumir a maioria das funções, no entanto, o *firmware* pode ser um ativo a se considerar para o caso de alguns dispositivos, como por exemplo, um gerenciador pessoal de diabetes, pois nesses casos o *firmware* controla diretamente os componentes do *hardware*.

A respeito do hardware por exemplo, temos os chips de memória flash dos DCGs, esses componentes frequentemente armazenam o *firmware* e outras informações sensíveis, essenciais para o funcionamento seguro desses sistemas. Ao realizar o *dump* desses chips, é possível realizar uma análise desses dados que podem revelar detalhes significativos sobre o DCG ou sobre o dispositivo IoMT, incluindo possíveis *backdoors*, chaves de criptografia, contas ocultas e outros elementos críticos de segurança.

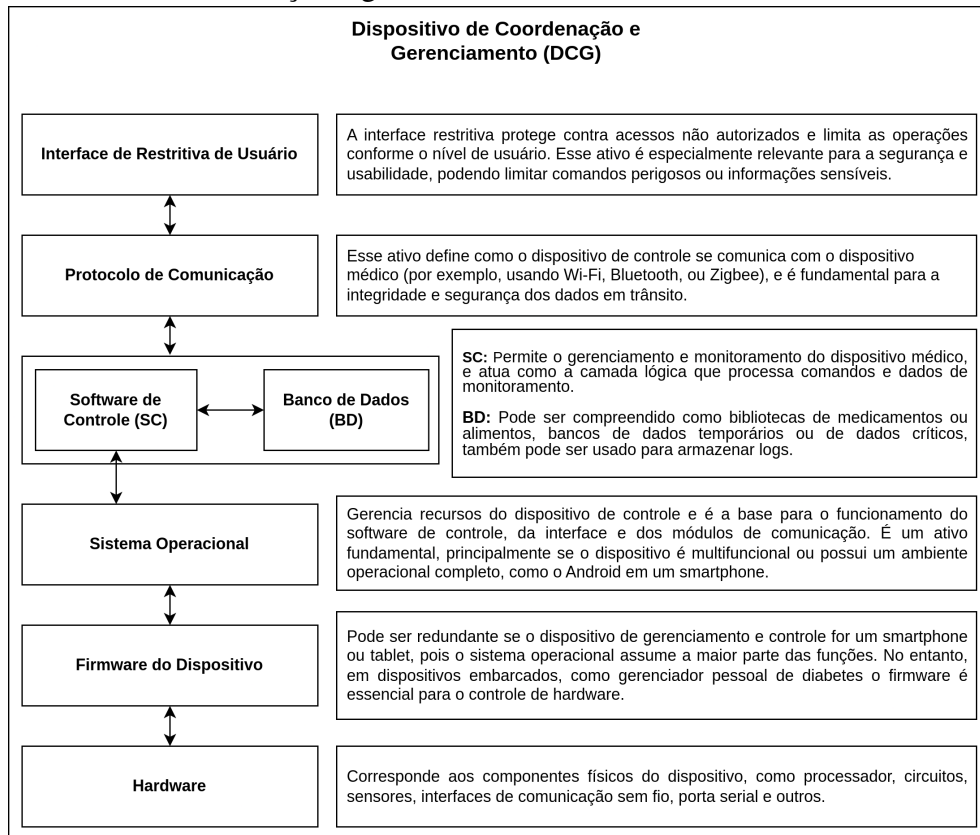
Assim como na generalização de ativos para os dispositivos IoMT, o modelo de ativos para o DCG é flexível. Ele permite a adaptação a diferentes contextos e a inclusão de novos ativos conforme necessário, ou a exclusão daqueles que não se aplicam a determinadas implementações. Essa abordagem modular visa fortalecer a segurança de dispositivos de coordenação e gerenciamento em IoMT, assegurando uma visão mais abrangente do componente.

5.1.1.3 Generalização de ativos para o gateway médico local

O *gateway* médico local é também chamado de adaptador, ele consiste de um ou mais servidores com sistema médico que permite a comunicação entre as diferentes redes de IoMT. Um dos papéis principais do *gateway*, é traduzir os diversos protocolos dos dispositivos IoMT para que os dados possam ser compreendidos pelas camadas superiores. Ademais, esses *gateways* centralizam o processamento de dados, controlam o fluxo de informações e devem ser capazes de garantir uma comunicação segura. Os ativos que compoem o gateway de nosso modelo são: Interface Restritiva de Usuário, Protocolo de Comunicação, Software de Controle, Banco de Dados, Sistema Operacional, *Firmware* e *Hardware*.

Assim como o DCG, o *gateway* também possui uma interface restritiva de usuário, esse ativo oferece uma camada essencial de proteção, devendo assegurar que apenas usuários autorizados interajam com o sistema. Ela deve ser configurada para limitar o acesso a funções críticas, evitando operações indevidas que possam comprometer a segurança do *gateway* e dos dispositivos que se conectam a ele.

Figura 11 – Ativos genéricos para modelagem de risco do dispositivo de coordenação e gerenciamento.



Fonte: Elaborada pelo autor.

O protocolo de comunicação representa os meios pelos quais o *gateway* troca dados com dispositivos médicos e outras partes da rede. A escolha de protocolos seguros é fundamental para prevenir interceptações, ataques de man-in-the-middle e outros riscos associados à comunicação.

O software de controle coordena as funções do *gateway*, permitindo a configuração e o monitoramento dos dispositivos conectados. No *gateway* esse ativo é responsável armazenar e processar dados, controlar o fluxo de informações dentre muitas outras funções, dessa maneira, é imprescindível que o software de controle seja protegido para garantir que apenas usuários autorizados possam acessar informações, realizar configurações e enviar comandos válidos para os demais componentes do sistema.

O banco de dados armazena informações sensíveis, incluindo registros de configuração e dados coletados dos dispositivos médicos. A segurança desse ativo é crítica, pois ele preserva a integridade e a confidencialidade das informações, protegendo-as contra acessos não autorizados e corrupção de dados.

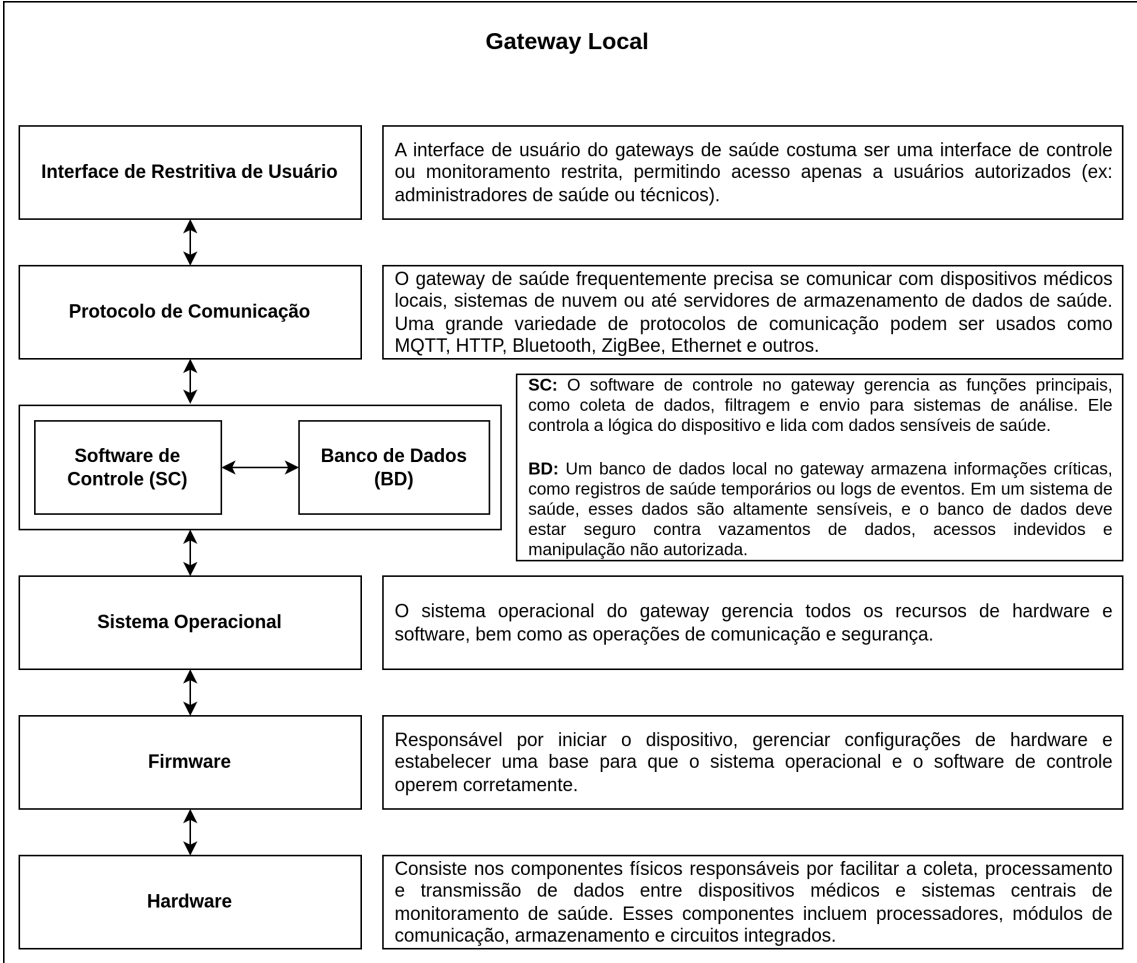
O sistema operacional sustenta toda a infraestrutura de software do *gateway*. Este

ativo deve ser robusto, atualizado e configurado para evitar vulnerabilidades que possam comprometer a segurança do sistema e expô-lo a invasões ou manipulações.

O *firmware* consiste em instruções para comunicação e controle sobre hardware, ele é o primeiro pedaço de código que o *gateway* executa. Além disso, o *firmware* inicializa o sistema operacional e fornece serviços de tempo de execução específicos para os programas, comunicando-se com vários componentes de hardware. De acordo com a OWASP *Firmware Security*, algumas técnicas de extração de *firmware* podem ser aplicadas, esse tipo de técnica pode ser utilizada para exploração de fraquezas por meio de engenharia reversa (OWASP, 2024).

Por fim, o hardware constitui a base física de operação do *gateway*. Este ativo deve ser seguro e confiável, pois falhas ou vulnerabilidades no nível físico podem comprometer todas as outras camadas de segurança implementadas.

Figura 12 – Ativos genéricos para modelagem de risco do *gateway* médico.



Fonte: Elaborada pelo autor.

5.1.2 Classificação STRIDE dos Principais Tipos de Ataques em Sistemas Médicos

O STRIDE é um modelo consolidado de categorização de ameaças para sistemas convencionais, no entanto, a aplicação direta à IoMT ainda demanda adaptação que aprimore o modelo para uma identificação de ameaças mais eficiente, tendo em vista as características únicas inerentes aos sistemas médicos conectados (Malamas *et al.*, 2021).

Considerando as questões mencionadas, propomos uma classificação denominada MedSTRIDE, que utiliza as seis categorias do acrônimo STRIDE para organizar os 22 tipos de ataques mais comuns em sistemas IoMT identificados na literatura. A classificação MedSTRIDE possibilita um mapeamento estruturado desses ataques, que já demonstraram eficácia no contexto de IoMT. Além disso, a efetividade desses ataques em sistemas médicos conectados é amplamente documentada em diversos estudos disponíveis na literatura atual (Yaqoob *et al.*, 2019; Hasan *et al.*, 2022; Papaioannou *et al.*, 2022; Yaacoub *et al.*, 2020; Sun *et al.*, 2019; Rasool *et al.*, 2022; Malamas *et al.*, 2021).

Ao utilizar o MedSTRIDE, os ataques identificados na literatura puderam ser organizados de forma lógica e abrangente, essa proposta proporciona um entendimento mais granular das ameaças, de maneira que futuras iniciativas em segurança médica conectada tenham uma base sólida e direcionada na identificação de fraquezas em seus componentes.

Além disso, subentende-se que a maioria das falhas de segurança decorre de vulnerabilidades não mapeadas ou desconhecidas, que muitas vezes são exploradas por invasores para causar danos. Ao investir no processo de identificação de ameaças, é possível diminuir o conjunto de ameaças desconhecidas e documentar potenciais riscos que, de outra forma, poderiam passar despercebidos. Adicionalmente, ao examinar um ativo de um componente da rede IoMT com MedSTRIDE, torna-se possível obter uma visão mais ampla das vulnerabilidades potenciais, considerando como cada ataque poderia ser direcionado especificamente a esse ativo.

5.1.2.1 Classificação de ataques IoMT para a propriedade Spoofing

A Tabela 6 apresenta a classificação dos ataques de IoMT para a propriedade *spoofing*. Uma discussão sobre a classificação dos ataques é apresentada abaixo.

A respeito de *spoofing* e *unauthorized access*, falhas de segurança em dispositivos médicos possibilitam que um agente mal-intencionado obtenha de forma ilegítima, dados confidenciais sobre a saúde e até simular a identidade de prestadores de serviços de saúde. Esses

tipos de ataques são amplamente documentados na literatura em relação a diversos dispositivos.

Nessa classificação, um ataque do tipo *masquerading*, empregado por um atacante, poderia assumir um nó legítimo da rede com a finalidade de retransmitir mensagens falsas sobre uma condição médica. Em um ataque do tipo MITM, o atacante se coloca no meio da comunicação entre duas partes que acreditam estar se comunicando diretamente uma com a outra.

Em um *Replay Attack*, um atacante pode retransmitir pacotes legítimos a fim de executar operações fraudulentas no sistema, enquanto que em ataques do tipo *sybil*, um atacante poderia criar múltiplas entidades falsas em um sistema distribuído.

Ataques do tipo *gray hole* utiliza-se de nó malicioso para atrasar e/ou descartar pacotes de dados na rede IoMT. Os ataques de *deauthentication* desconectem qualquer dispositivo de uma rede, mesmo que o atacante não estejam conectado a ela. Para isso, o atacante pode utilizar a técnicas de clonagem de endereços físico do cliente de destino e do ponto de acesso, após isso, ele realiza o envio de solicitações de desautenticação para ambos, fazendo com que o cliente se desconecte.

Tabela 6 – Classificação de ataques IoMT para a propriedade Spoofing.

Categorias	Tipos de Ataques	Referências
STRIDE - Spoofing	Spoofing [7]	(Yaqoob <i>et al.</i> , 2019; Yaacoub <i>et al.</i> , 2020; Papaioannou <i>et al.</i> , 2022; Rasool <i>et al.</i> , 2022)
	Unauthorized Access [6]	(Yaqoob <i>et al.</i> , 2019; Rasool <i>et al.</i> , 2022)
	Masquerading Attacks [21]	(Yaacoub <i>et al.</i> , 2020; Papaioannou <i>et al.</i> , 2022; Rasool <i>et al.</i> , 2022)
	Man In The Middle [5]	(Yaqoob <i>et al.</i> , 2019; Yaacoub <i>et al.</i> , 2020; Papaioannou <i>et al.</i> , 2022; Rasool <i>et al.</i> , 2022)
	Replay Attack [8]	(Yaqoob <i>et al.</i> , 2019; Yaacoub <i>et al.</i> , 2020; Papaioannou <i>et al.</i> , 2022; Rasool <i>et al.</i> , 2022)
	Sybil Attack [19]	(Yaqoob <i>et al.</i> , 2019; Yaacoub <i>et al.</i> , 2020; Rasool <i>et al.</i> , 2022)
	Grey Hole [18]	(Yaqoob <i>et al.</i> , 2019; Rasool <i>et al.</i> , 2022)
	Deauthentication Attacks [20]	(Yaacoub <i>et al.</i> , 2020; Rasool <i>et al.</i> , 2022)

Fonte: Elaborada pelo autor.

5.1.2.2 Classificação de ataques IoMT para a propriedade Tampering

A Tabela 7 apresenta a classificação dos ataques de IoMT para a propriedade *tampering*. Uma discussão sobre a classificação dos ataques é apresentada abaixo.

O ataque de modificação de *firmware* envolve a alteração maliciosa do software embarcado que controla o funcionamento do dispositivo. Ao introduzir código malicioso no *firmware*, o atacante pode obter controle remoto do dispositivo, e a partir disso realizar

modificações nos dados coletados e transmitidos (Yaqoob *et al.*, 2019; Papaioannou *et al.*, 2022; Rasool *et al.*, 2022).

Os ataques de *tampering* pode ter muitas facetas, segundo Ghubaish *et al.* (2020), “Qualquer tipo de modificação nos dados dos sistemas IoMT no estágio de coleta, trânsito ou armazenamento é considerado um ataque de adulteração”.

O ataque MITM é uma ameaça sofisticada à segurança dos dispositivos médicos, um adversário intercepta a comunicação entre duas partes autênticas sem ser percebido, além disso, o invasor pode alterar os dados interceptados antes de enviá-los ao destino original (Ghubaish *et al.*, 2020; Yaqoob *et al.*, 2019; Yaacoub *et al.*, 2020; Papaioannou *et al.*, 2022; Rasool *et al.*, 2022).

Envolve a utilização de softwares maliciosos, que comprometem a segurança de computadores, redes e dispositivos médicos, sem o consentimento do usuário e dos administradores do sistema. Além disso, esse tipo de ataque pode causar a adulteração de dados clínicos (Hasan *et al.*, 2022; Yaacoub *et al.*, 2020; Papaioannou *et al.*, 2022; Rasool *et al.*, 2022).

O *Buffer overflow* é um tipo de ataque que pode ser usado para comprometer a integridade e a operação do sistema ao permitir a execução de código malicioso e a corrupção de dados (Yaqoob *et al.*, 2019; Rasool *et al.*, 2022).

Tabela 7 – Classificação de ataques IoMT para a propriedade Tampering.

Categorias	Tipos de Ataques	Referências
STRIDE - Tampering	Firmware Modification Attack [1]	(Yaqoob <i>et al.</i> , 2019; Papaioannou <i>et al.</i> , 2022; Rasool <i>et al.</i> , 2022)
	Tampering [9]	(Yaqoob <i>et al.</i> , 2019; Yaacoub <i>et al.</i> , 2020; Papaioannou <i>et al.</i> , 2022; Rasool <i>et al.</i> , 2022)
	Man In The Middle [5]	(Yaqoob <i>et al.</i> , 2019; Yaacoub <i>et al.</i> , 2020; Papaioannou <i>et al.</i> , 2022; Rasool <i>et al.</i> , 2022)
	Malware Attack [22]	(Hasan <i>et al.</i> , 2022; Yaacoub <i>et al.</i> , 2020; Papaioannou <i>et al.</i> , 2022; Rasool <i>et al.</i> , 2022; Kim <i>et al.</i> , 2015)
	Buffer Overflow [16]	(Yaqoob <i>et al.</i> , 2019; Rasool <i>et al.</i> , 2022)

Fonte: Elaborada pelo autor.

5.1.2.3 Classificação de ataques IoMT para a propriedade Repudiation

A Tabela 8 apresenta a classificação dos ataques de IoMT para a propriedade *repudiation*. Uma discussão sobre a classificação dos ataques é apresentada abaixo.

No ataque MITM, um agente malicioso intercepta e possivelmente modifica a comunicação entre duas partes sem que elas percebam. No caso de *Spoofing*, o ataque envolve a

falsificação de identidade, onde o atacante se faz passar por outra pessoa ou dispositivo, isso torna a identificação um grande desafio.

O ataque de *malware* por exemplo, pode alterar registros de atividades, logs de sistema e outros dados que possam ser utilizados para rastrear a origem de um ataque. Ao manipular esses registros, o atacante torna mais difícil a atribuição de responsabilidade. Além disso, o *malware* é por essência projetado para mascarar sua origem, dificultando a identificação do atacante.

No ataque *Grey Hole* e Sybil, o atacante cria uma ou várias identidades falsas para descartar pacotes ou influenciar a rede. Ao fazer isso, ele pode executar ações sob diferentes pseudônimos e negar o envolvimento em comportamentos maliciosos ao esconder-se atrás dessas identidades múltiplas.

Tabela 8 – Classificação de ataques IoMT para a propriedade Repudiation.

Categorias	Tipos de Ataques	Referências
STRIDE - Repudiation	Man In The Middle [5]	(Yaqoob <i>et al.</i> , 2019; Yaacoub <i>et al.</i> , 2020; Papaioannou <i>et al.</i> , 2022; Rasool <i>et al.</i> , 2022)
	Spoofing [7]	(Yaqoob <i>et al.</i> , 2019; Yaacoub <i>et al.</i> , 2020; Papaioannou <i>et al.</i> , 2022; Rasool <i>et al.</i> , 2022)
	Malware Attack [22]	(Hasan <i>et al.</i> , 2022; Yaacoub <i>et al.</i> , 2020; Papaioannou <i>et al.</i> , 2022; Rasool <i>et al.</i> , 2022; Kim <i>et al.</i> , 2015)
	Sybil Attack [19]	(Yaqoob <i>et al.</i> , 2019; Yaacoub <i>et al.</i> , 2020; Rasool <i>et al.</i> , 2022)
	Grey Hole [18]	(Yaqoob <i>et al.</i> , 2019; Rasool <i>et al.</i> , 2022)

Fonte: Elaborada pelo autor.

5.1.2.4 Classificação de ataques IoMT para a propriedade Information Disclosure

A Tabela 9 apresenta a classificação dos ataques de IoMT para a propriedade *information disclosure*. Uma discussão sobre a classificação dos ataques é apresentada abaixo.

O ataque de *eavesdropping*, envolve a escuta clandestina e não autorizada das comunicações entre dispositivos médicos, servidores, ou redes, a interceptação de informações pode levar à exposição de dados confidenciais (Papaioannou *et al.*, 2022; Yaqoob *et al.*, 2019; Yaacoub *et al.*, 2020; Rasool *et al.*, 2022; Ghubaish *et al.*, 2020; Hasan *et al.*, 2022).

O ataque de *sniffing* envolve a captura passiva e não autorizada de dados que trafegam na rede, permitindo que um atacante monitore e registre informações transmitidas entre dispositivos médicos, servidores, e redes de comunicação (Yaacoub *et al.*, 2020; Yaqoob *et al.*, 2019; Rasool *et al.*, 2022; Ghubaish *et al.*, 2020).

Segundo Yaqoob *et al.* (2019), *information disclosure* é um tipo de ataque que está relacionado à exposição de informações por uma entidade não autorizada, esse tipo de ataque ocorre devido a fraquezas no dispositivo ou meio de comunicação.

De acordo com Hasan *et al.* (2022), “ataques como o *man-in-the-middle* podem sabotar a integridade e a privacidade das redes IoMT ao intervir na comunicação para alterar os dados de troca entre duas partes sem serem notados”.

O *malware attack* pode expor informações sigilosas ou mesmo abrir um *backdoor* para posterior exploração. Esse tipo de ataque pode causar adulteração de dados clínicos, interrupção de serviços essenciais, e comprometimento da privacidade dos pacientes (Hasan *et al.*, 2022).

Segundo Yaqoob *et al.* (2019), “*replay attack* no contexto de dispositivos médicos consiste em obter dados de pacotes válidos transmitidos por esses dispositivos com a intenção de corrompê-los ou personificá-los”.

Os ataques de *side channel* geralmente exploram informações indiretas, como padrões de consumo de energia, tempo de resposta e emissões eletromagnéticas, para inferir informações sigilosas sem necessariamente estar conectado a a rede de dispositivos médicos.

Tabela 9 – Classificação de ataques IoMT para a propriedade Information Disclosure.

Categorias	Tipos de Ataques	Referências
STRIDE - Information Disclosure	Eavesdropping [2]	(Yaqoob <i>et al.</i> , 2019; Hasan <i>et al.</i> , 2022; Yaacoub <i>et al.</i> , 2020; Papaioannou <i>et al.</i> , 2022; Rasool <i>et al.</i> , 2022)
	Sniffing [3]	(Yaqoob <i>et al.</i> , 2019; Yaacoub <i>et al.</i> , 2020, 2020; Rasool <i>et al.</i> , 2022)
	Information Disclosure [4]	(Yaqoob <i>et al.</i> , 2019; Hasan <i>et al.</i> , 2022; Yaacoub <i>et al.</i> , 2020; Papaioannou <i>et al.</i> , 2022; Rasool <i>et al.</i> , 2022)
	Man In The Middle [5]	(Yaqoob <i>et al.</i> , 2019; Yaacoub <i>et al.</i> , 2020; Papaioannou <i>et al.</i> , 2022; Rasool <i>et al.</i> , 2022)
	Malware Attack [22]	(Hasan <i>et al.</i> , 2022; Yaacoub <i>et al.</i> , 2020; Papaioannou <i>et al.</i> , 2022; Rasool <i>et al.</i> , 2022; Kim <i>et al.</i> , 2015)
	Replay Attack [8]	(Yaqoob <i>et al.</i> , 2019; Yaacoub <i>et al.</i> , 2020; Papaioannou <i>et al.</i> , 2022; Rasool <i>et al.</i> , 2022)
	Side Channel Attack [14]	(Yaqoob <i>et al.</i> , 2019; Yaacoub <i>et al.</i> , 2020; Papaioannou <i>et al.</i> , 2022; Rasool <i>et al.</i> , 2022)

Fonte: Elaborada pelo autor.

5.1.2.5 Classificação de ataques IoMT para a propriedade Denial of Service

A Tabela 10 apresenta a classificação dos ataques de IoMT para a propriedade *denial of service*. Uma discussão sobre a classificação dos ataques é apresentada abaixo.

Ataques de negação de serviço como DoS, DDoS, *resource depletion* e *jamming attack*, têm como objetivo sobrecarregar dispositivos médicos com requisições constantes, consumindo sua capacidade de processamento, bateria e largura de banda de rede até que ele se torne incapaz de responder adequadamente às funções para as quais foi projetado (Yaqoob *et al.*, 2019).

A respeito de *ransomware DoS*, (Yaqoob *et al.*, 2019) cita que, “este ataque é possível em equipamentos médicos no local devido ao uso de um sistema operacional obsoleto e protocolos proprietários inseguros... usuários legítimos não conseguem acessar as instalações médicas até que a administração do hospital pague o resgate desejado”.

O *deauthentication attacks*, é uma forma de ataque de negação de serviço direcionado a rede sem fio, o atacante envia pacotes na tentativa de desautenticar um ou mais dispositivos, forçando-os a se desconectar da rede (Yaacoub *et al.*, 2020).

Tabela 10 – Classificação de ataques IoMT para a propriedade Denial of Service.

Categorias	Tipos de Ataques	Referências
STRIDE - Denial of Service	DOS Attack [10]	(Yaqoob <i>et al.</i> , 2019; Hasan <i>et al.</i> , 2022; Yaacoub <i>et al.</i> , 2020; Papaioannou <i>et al.</i> , 2022; Rasool <i>et al.</i> , 2022)
	DDoS Attack [11]	(Yaacoub <i>et al.</i> , 2020; Rasool <i>et al.</i> , 2022)
	Resource Depletion [12]	(Yaqoob <i>et al.</i> , 2019; Rasool <i>et al.</i> , 2022)
	Jamming Attack [13]	(Yaqoob <i>et al.</i> , 2019; Yaacoub <i>et al.</i> , 2020; Rasool <i>et al.</i> , 2022)
	Ransomware DOS [15]	(Yaqoob <i>et al.</i> , 2019; Hasan <i>et al.</i> , 2022; Rasool <i>et al.</i> , 2022)
	Deauthentication Attacks [20]	(Yaacoub <i>et al.</i> , 2020; Rasool <i>et al.</i> , 2022)

Fonte: Elaborada pelo autor.

5.1.2.6 Classificação de ataques IoMT para a propriedade Elevation of Privilege

A Tabela 11 apresenta a classificação dos ataques de IoMT para a propriedade *elevation of privilege*. Uma discussão sobre a classificação dos ataques é apresentada abaixo.

O *brute Force attack*, busca comprometer sistemas de segurança através da tentativa exaustiva de combinações possíveis de credenciais, como senhas ou chaves de criptografia (Yaqoob *et al.*, 2019; Rasool *et al.*, 2022; Yaacoub *et al.*, 2020), dessa maneira o atacante consegue acender a funções restritas do sistema. De outra forma, o *malware attack* explora brechas em *firmware* ou software não atualizado, assim o atacante consegue adquirir permissões elevadas por meio de vulnerabilidades conhecidas.

Segundo Yaqoob *et al.* (2019), o *firmware modification attack* é um dos ataques mais frequentes em dispositivos de uso corporal. Além disso, a necessidade de atualizações

para melhoria do desempenho dos dispositivos é essencial para o seu adequado funcionamento e segurança, no entanto, à falta de mecanismos adequados de verificação de integridade do *firmware*, facilita a exploração maliciosa onde o atacante acaba por substituir o *firmware* legítimo do dispositivo por um malicioso passando a exercer controle parcial ou total do dispositivo.

O ataque de *buffer overflow* está diretamente relacionado as más práticas de programação, o problema ocorre devido a escrita de dados que ultrapassam os limites de *buffer*, esse tipo de problema pode resultar na execução de comando arbitrários (Yaqoob *et al.*, 2019).

Tabela 11 – Classificação de ataques IoMT para a propriedade Elevation of Privilege.

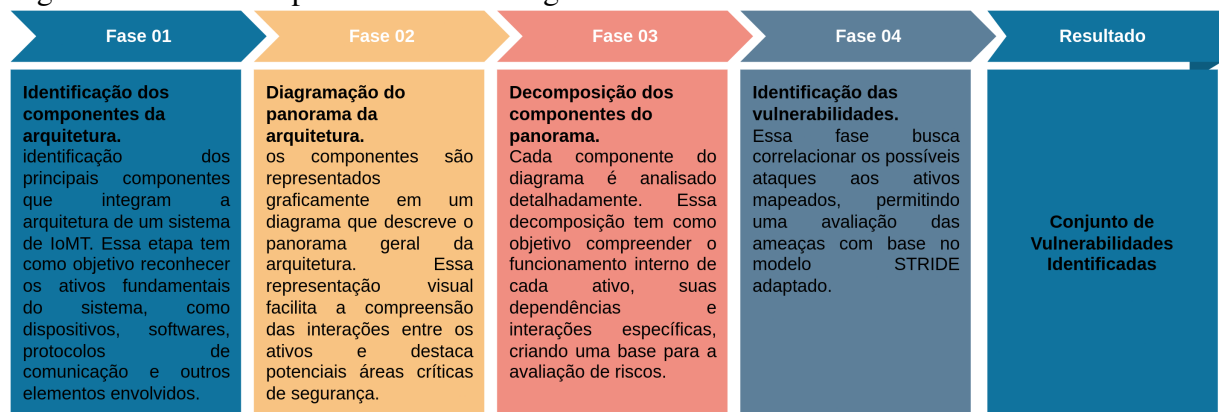
Categorias	Tipos de Ataques	Referências
STRIDE - Elevation of Privilege	Brute Force Attack [17]	(Yaqoob <i>et al.</i> , 2019; Rasool <i>et al.</i> , 2022)
	Unauthorized Access [6]	(Yaqoob <i>et al.</i> , 2019; Rasool <i>et al.</i> , 2022)
	Malware Attack [22]	(Hasan <i>et al.</i> , 2022; Yaacoub <i>et al.</i> , 2020; Papaioannou <i>et al.</i> , 2022; Rasool <i>et al.</i> , 2022; Kim <i>et al.</i> , 2015)
	Firmware Modification Attack [1]	(Yaqoob <i>et al.</i> , 2019; Papaioannou <i>et al.</i> , 2022; Rasool <i>et al.</i> , 2022)
	Buffer Overflow [16]	(Yaqoob <i>et al.</i> , 2019; Rasool <i>et al.</i> , 2022)

Fonte: Elaborada pelo autor.

5.1.3 Fases do Processo de Modelagem com MedSTRIDE

O MedSTRIDE é um *framework* desenvolvido para a modelagem de riscos em sistemas médicos conectados, com ênfase nas camadas física e de adaptação. Seu processo de modelagem é estruturado em quatro fases, concebidas para organizar e sistematizar a análise, desde a identificação dos componentes do sistema até a identificação de vulnerabilidades potenciais. Conforme ilustrado na Figura 13, cada fase gera insumos essenciais para a próxima, estabelecendo uma relação de dependência entre as etapas e garantindo a continuidade e a coerência do processo.

Figura 13 – Fases do processo de modelagem com MedSTRIDE.



Fonte: Elaborada pelo autor.

5.1.3.1 Identificação dos componentes do sistema

Na primeira fase que consiste na identificação dos componentes do sistema, é o ponto de partida do processo de modelagem de riscos no MedSTRIDE. Nesse momento, realiza-se o mapeamento de todos os ativos que compõem o sistema, incluindo dispositivos IoMT, gateways, softwares de gerenciamento, dispositivos móveis e quaisquer outros elementos críticos para o funcionamento do ambiente. Essa etapa é particularmente importante em sistemas que estão em desenvolvimento, pois permite definir de forma clara os componentes que serão integrados, assegurando uma base sólida para as fases subsequentes da análise.

Por outro lado, em sistemas já em operação, o nível de dificuldade dessa etapa varia conforme a complexidade da arquitetura. Em ambientes menores ou com poucos dispositivos conectados, a tarefa tende a ser mais simples e direta. Entretanto, em sistemas complexos, como os de grandes hospitais, o desafio aumenta significativamente. A existência de uma grande quantidade de dispositivos IoMT, *gateways* e dispositivos móveis para gerenciamento pode tornar o mapeamento uma tarefa árdua. Além disso, a falha em identificar qualquer componente, por menor que pareça, pode comprometer seriamente a segurança do sistema, abrindo brechas para vulnerabilidades não mapeadas.

Para grandes hospitais que possuem muitos equipamentos em operação, é essencial reconhecer que sistemas hospitalares estão em constante evolução, com a adição de novos dispositivos e tecnologias. Assim, o panorama criado deve ser atualizado regularmente para refletir essas mudanças. Sempre que um novo equipamento ou tecnologia for introduzido, ele deve ser integrado ao diagrama e submetido ao processo de modelagem de riscos. Essa abordagem não apenas garante que o panorama permaneça alinhado com a realidade do sistema, mas também possibilita a aplicação imediata da modelagem aos novos componentes, identificando possíveis vulnerabilidades antes que elas comprometam a segurança do ambiente.

Para realização da fase um, consideremos um sistema “simples” de bomba de infusão de insulina como o apresentado na Figura 14. De acordo com a fabricante Medtronic (2024), o sistema MiniMed 780G da Medtronic é uma solução avançada de gerenciamento de diabetes, composta por uma bomba de insulina e um monitor de glicose contínuo (MGC). A arquitetura do sistema inclui a bomba de infusão de insulina, que entrega insulina automaticamente com base nas leituras de glicose fornecidas pelo MGC. O monitor de glicose, conectado à bomba via *Bluetooth*, mede os níveis de glicose no sangue em tempo real e transmite essas informações para a bomba, que ajusta a dosagem de insulina de acordo com os valores observados. O

sistema também conta com um aplicativo para dispositivos móveis, permitindo que o usuário e os profissionais de saúde monitorem e ajustem o tratamento remotamente. Essa arquitetura integrada visa oferecer um controle mais preciso e dinâmico dos níveis de glicose, melhorando a qualidade de vida dos pacientes com diabetes.

Figura 14 – Bomba de infusão de insulina.



Fonte: (Medtronic, 2024).

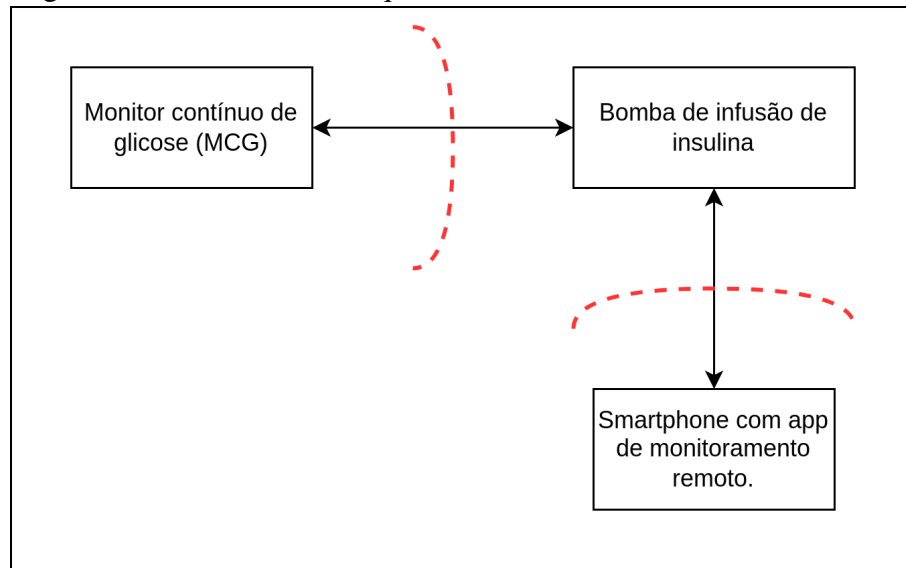
5.1.3.2 Criação do panorama da arquitetura

A Figura 15 apresenta uma visão simplificada da arquitetura do sistema MiniMed 780G, destacando três componentes principais: o monitor contínuo de glicose, a bomba de infusão de insulina e o *smartphone* com aplicativo de monitoramento remoto.

A construção desse panorama permite a identificação dos componentes do sistema, suas funções, e as interações entre eles. No caso do MiniMed 780G, o MGC monitora continuamente os níveis de glicose no corpo, transmitindo esses dados para a bomba de insulina. A bomba, por sua vez, ajusta automaticamente a dosagem de insulina com base nas informações recebidas, visando manter os níveis de glicose dentro da faixa desejada. O *smartphone*, ao se conectar à bomba de insulina, oferece ao usuário uma interface intuitiva para visualizar os dados de glicose, ajustar configurações do sistema e receber alertas sobre possíveis variações nos níveis de glicose ou necessidades de intervenção.

É crucial entender que, apesar da sofisticação do sistema, existem limites de confiança. A precisão dos dados do MGC pode ser afetada por diversos fatores, como a localização do sensor, atividade física e interferências eletromagnéticas. Além disso, a eficácia da bomba

Figura 15 – Panorama da arquitetura do sistema de infusão de insulina.



Fonte: Elaborada pelo autor.

de insulina depende da calibração correta e da resposta individual ao tratamento. As "linhas vermelhas" nesse contexto representam os limites críticos que, se ultrapassados, podem indicar problemas no sistema ou na saúde do paciente. Por exemplo, um nível de glicose extremamente baixo ou alto, ou um erro na comunicação entre os dispositivos, são situações que exigem atenção imediata.

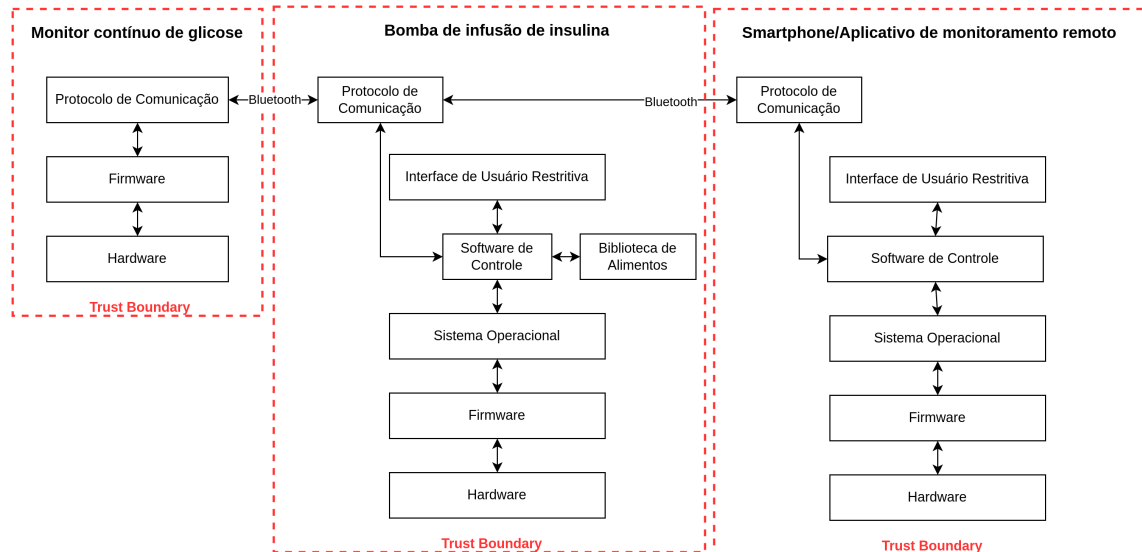
5.1.3.3 Decomposição dos componentes da arquitetura

Para a execução dessa fase, os modelos genéricos de decomposição de componentes apresentados na subseção 5.1.1 foram utilizados. A decomposição dos componentes de um sistema médico, como a bomba de infusão de insulina, é uma etapa crítica na modelagem de riscos, pois permite uma análise detalhada e específica das partes que compõem o dispositivo. Essa abordagem é particularmente importante porque cada componente do sistema pode apresentar vulnerabilidades únicas, sejam elas relacionadas ao protocolo de comunicação, *firmware*, hardware ou software de controle. A avaliação isolada de cada parte ajuda a identificar e mitigar riscos que poderiam ser negligenciados caso o sistema fosse analisado como um todo.

Ao analisar a Figura 16, o protocolo de comunicação *Bluetooth* utilizado para conectar o monitor de glicose, o *smartphone* e a bomba de insulina, pode estar suscetível a ataques como *sniffing* ou MITM. Ao mesmo tempo, o *firmware* do dispositivo, responsável por controlar as operações fundamentais, pode conter vulnerabilidades que, se exploradas, comprometeriam diretamente a administração de insulina, colocando a segurança do paciente em

risco. Analisar essas partes separadamente permite aplicar controles específicos e mais eficazes.

Figura 16 – Decomposição dos componentes da arquitetura.



Fonte: Elaborada pelo autor.

Além disso, essa decomposição possibilita a priorização dos esforços de segurança. Componentes com maior exposição ou impacto, como os que fazem interface direta com o usuário (ex.: aplicativo de monitoramento remoto), podem receber maior atenção durante a análise. Isso é essencial em sistemas hospitalares complexos, onde dispositivos IoMT são numerosos e interconectados. Sem essa abordagem estruturada, seria muito difícil identificar vulnerabilidades ocultas em dispositivos específicos ou em suas interações.

5.1.3.4 Aplicação da classificação STRIDE para identificação de vulnerabilidades

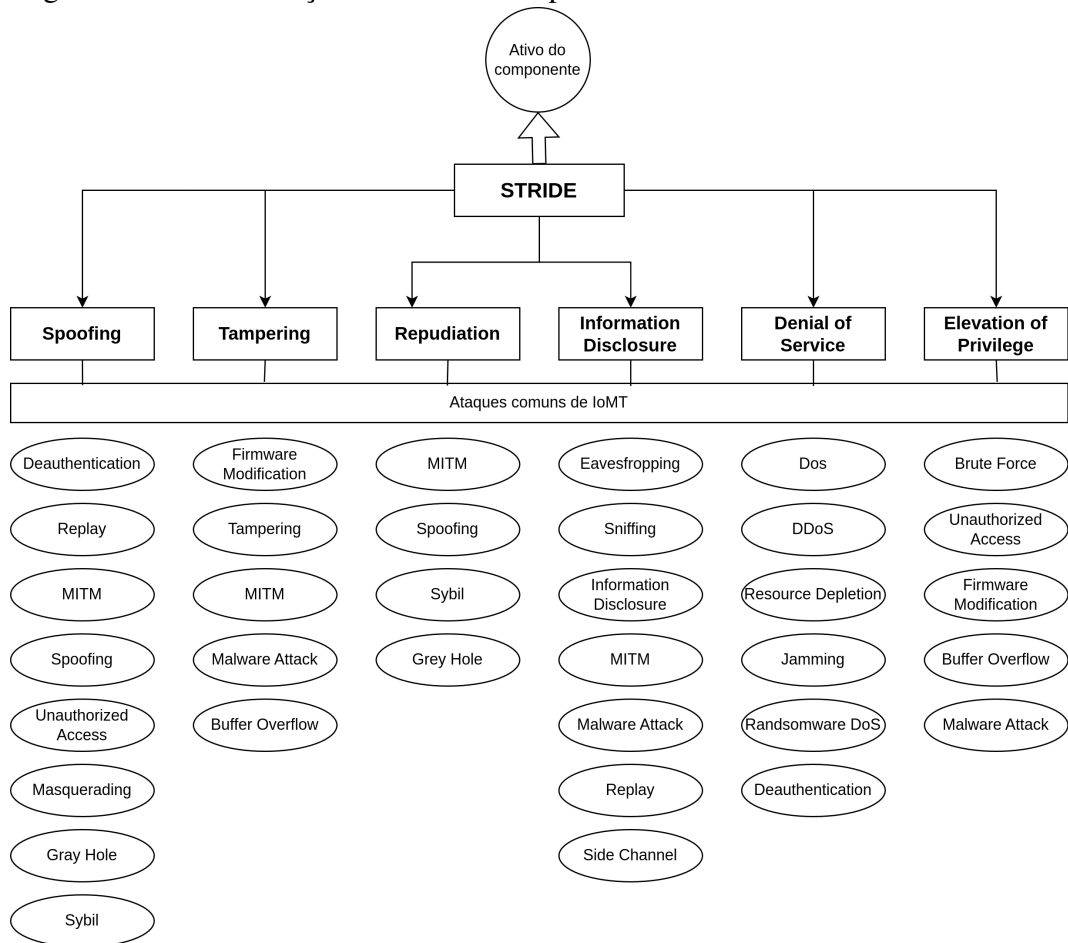
No modelo MedSTRIDE, a identificação de vulnerabilidades é realizada por meio de uma análise sistemática em todos os ativos do sistema. Cada ativo é submetido a uma avaliação que correlaciona potenciais ataques aos princípios de segurança definidos no STRIDE. Esse processo é essencial para identificar falhas de segurança e antecipar ameaças que possam comprometer a integridade, confidencialidade e disponibilidade dos dispositivos IoMT.

Conforme o exposto na Figura 17, cada ataque listado no modelo é utilizado como referência para investigar como as vulnerabilidades podem se manifestar nos ativos avaliados. Por exemplo, ao analisar o protocolo de comunicação *Bluetooth*, que é amplamente usado em dispositivos médicos para transferir dados entre sensores e dispositivos de controle, é possível identificar vulnerabilidades relacionadas a ataques específicos.

Por exemplo, o ataque de *eavesdropping* (classificado como *information disclosure*)

pode explorar comunicações desprotegidas, seja pela ausência de autenticação ou pelo uso de criptografia fraca, permitindo que o atacante intercepte e acesse informações sensíveis. Além disso, a falta de mecanismos robustos para defesa contra interferências torna o sistema vulnerável a ataques de negação de serviço (*Denial of Service*), que podem sobrecarregar o equipamento com múltiplas solicitações, resultando na interrupção deliberada de sua funcionalidade.

Figura 17 – Classificação MedSTRIDE aplicada aos ativos.



Fonte: Elaborada pelo autor.

O protocolo *Bluetooth*, assim como outros ativos, deve ser analisado quanto à sua resiliência frente a cada categoria de ataque do modelo MedSTRIDE, garantindo que um conjunto de vulnerabilidades seja previamente identificado por fabricantes e profissionais de cibersegurança. Esse conjunto de vulnerabilidades será utilizado por fabricantes e profissionais de cibersegurança que classificarão, priorizarão e, posteriormente, adotarão medidas para mitigar os riscos associados.

6 ANÁLISE DOS RESULTADOS E DISCUSSÕES

A avaliação do framework MedSTRIDE foi conduzida por meio de um experimento com 26 alunos de graduação dos cursos de Sistemas de Informação e Engenharia da Computação, distribuídos entre os sextos, oitavos e décimos semestres. O experimento foi organizado em três etapas principais: formação dos grupos; apresentação do estudo de caso e dos modelos (STRIDE e MedSTRIDE); execução do experimento.

A nossa hipótese é que, se o MedSTRIDE apresenta maior precisão e cobertura na identificação de ameaças, combinado com uma taxa reduzida de falsos positivos e erros de classificação em comparação ao STRIDE, isso indicará sua superioridade como ferramenta para modelagem de riscos em sistemas de IoMT.

6.1 Apresentação do Estudo de Caso

Para validar a modelagem de risco proposta, foi utilizado um estudo de caso baseado em um sistema típico de bomba de infusão de medicamentos em ambientes hospitalares. Este sistema é composto por três principais componentes: uma bomba de infusão de medicamentos, um servidor central para controle e monitoramento das bombas, e um dispositivo móvel (smartphone ou tablet) utilizado pelos profissionais de saúde para gerenciar as infusões. A seguir, detalham-se as características de cada componente.

A bomba universal de infusão de medicamentos (Figura 18) é um dispositivo médico projetado para administrar fluidos, como medicamentos e nutrientes, diretamente na corrente sanguínea do paciente de forma precisa e controlada. Este equipamento desempenha um papel crucial em tratamentos que exigem infusões graduais ao longo do tempo, sendo amplamente utilizado em ambientes hospitalares. As principais características da bomba são:

- **Tela sensível ao toque:** facilita a interação e a programação por parte do usuário.
- **Software avançado:** permite a configuração da terapia com acesso a uma biblioteca de medicamentos, definindo limites seguros de dosagem.
- **Conexão de rede Wi-Fi:** possibilita integração com o servidor central para envio e recepção de informações em tempo real.
- **Bateria de longa duração:** autonomia de até 8 horas com carregamento automático, garantindo operação contínua mesmo em caso de falha de energia.
- **Sistema de alarmes:** oferece alertas sonoros diferenciados conforme a criticidade, aju-

dando a priorizar ações corretivas de maneira eficaz.

Figura 18 – Bomba de infusão de medicamentos.



Fonte: LIFEMED. Lifeview. Disponível em: <https://www.lifemed.com.br/produto/smart-touch->. Acesso em: 2 nov. 2024.

O servidor central (Figura 19) é o núcleo de controle do sistema, responsável por monitorar e gerenciar as bombas de infusão conectadas. Este componente é essencial para garantir a supervisão eficiente e a segurança do tratamento intravenoso. Principais características:

- **Alta capacidade de gerenciamento:** suporta até 64 leitos em uma única unidade de processamento.
- **Monitoramento abrangente:** exibe valores numéricos, traçados gráficos e tendências de até 96 horas para cada paciente conectado.
- **Conectividade flexível:** suporta comunicação via Ethernet e Wi-Fi, adaptando-se às necessidades de infraestrutura do hospital.
- **Integração com bombas de infusão:** as informações sobre infusões, alarmes e alertas em tempo real são centralizadas para facilitar o acompanhamento.
- **Controle de acesso:** o sistema permite a auditoria de atividades por meio de credenciais exclusivas para cada usuário.

O dispositivo móvel complementa o sistema, permitindo aos profissionais de saúde acessar informações e gerenciar as infusões de maneira remota e prática. Principais características:

- **Aplicativo dedicado:** a comunicação com o servidor central é feita via aplicativo, ativado por QR-code.

Figura 19 – Sistema Lifeview para gerenciamento de bombas de infusão de medicamentos.



Fonte: LIFEMED. Lifeview. Disponível em: <https://www.lifemed.com.br/produto/lifeview>. Acesso em: 2 nov. 2024.

- **Informações em tempo real:** o aplicativo exibe dados sobre infusões, além de alarmes e alertas críticos.
- **Facilidade de uso:** o gerenciamento da terapia pode ser feito diretamente pelo profissional, otimizando o tempo e reduzindo deslocamentos desnecessários.

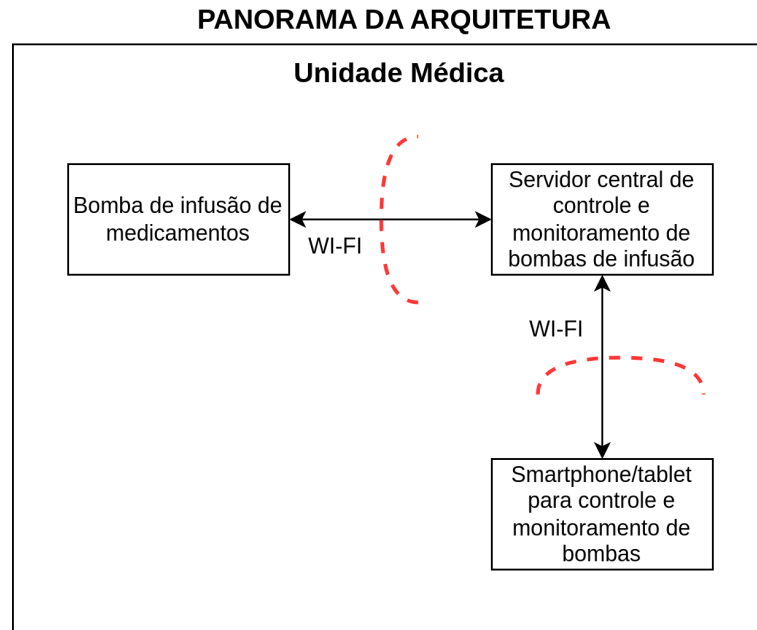
Esse sistema foi utilizado como base para a modelagem de risco, considerando as interações entre os componentes, os potenciais vetores de ataque e os ativos críticos identificados. O panorama da arquitetura é apresentado na Figura 20.

6.2 Execução do Experimento

Na primeira etapa, foram formados dois grupos, denominados Grupo-A e Grupo-B (grupo STRIDE e grupo MedSTRIDE, respectivamente), sendo cada grupo composto por 13 participantes. Ademais, os grupos foram formados de maneira equilibrada, respeitando o número de alunos por semestre do curso.

Antes da execução do experimento, ambos os grupos participaram de uma oficina com o objetivo de fornecer uma visão geral da área de IoMT e modelagem de risco, na qual os modelos STRIDE e MedSTRIDE foram apresentados. Para assegurar a aplicação correta das metodologias e a assimilação dos conceitos, os participantes realizaram uma pequena atividade prática ao final.

Figura 20 – Panorama da arquitetura do estudo de caso.



Fonte: Elaborada pelo autor.

Para a execução do experimento, foi aplicado o estudo de caso baseado em um sistema real de IoMT, conforme apresentado na Subseção 6.1. Ambos os grupos foram solicitados a realizar a modelagem de risco do sistema utilizando o *framework* de modelagem correspondente a cada grupo. Para isso, foram destinados uma hora para cada uma das oficinas e o exercício de fixação, trinta minutos para a fase de decomposição do sistema e uma hora para a fase de identificação de vulnerabilidades, conforme demonstrado na Subseção 5.1.3.

Ainda sobre a realização do experimento, cada participante recebeu um documento contendo toda a descrição do estudo de caso e um resumo dos processos de modelagem a serem executados. Além disso, foi fornecido um arquivo para a criação do diagrama da arquitetura, que continha o panorama da arquitetura (Figura 20) médica utilizada para a decomposição dos componentes. Para o Grupo-B, no entanto, além do panorama, também foram entregues os modelos genéricos de ativos apresentados na Subseção 5.1.1, que serviram como referência para a decomposição dos componentes do sistema médico.

Para a última fase do processo de modelagem, fornecemos a cada participante três planilhas, correspondentes aos três componentes da arquitetura: bomba de infusão, *gateway* médico e dispositivo móvel para gerenciamento de bombas de infusão. Essas planilhas foram utilizadas no processo de identificação de vulnerabilidades dos ativos definidos na etapa anterior. Cada planilha do Grupo-A (STRIDE) contém dez tabelas, cuja estrutura está ilustrada na Figura 21. Por sua vez, o Grupo-B (MedSTRIDE) também recebeu três planilhas contendo dez tabelas

cada; entretanto, as tabelas contidas seguem a estrutura apresentada na Figura 22.

Figura 21 – Planilha STRIDE para identificação de vulnerabilidades.

ATIVO 01	SPOOFING	TAMPERING	REPUDIATION	INFORMATION DISCLOSURE	DENIAL OF SERVICE	ELEVATION OF PRIVILEGE
Nome do Ativo						

Fonte: Elaborada pelo autor.

Figura 22 – Planilha MedSTRIDE para identificação de vulnerabilidades.

ATIVO 01	PROPRIEDADES STRIDE	ATAQUES IOMT	RISCOS IDENTIFICADOS
Nome do Ativo	SPOOFING	Deauthentication Attacks	
		Grey Hole	
		Replay Attack	
		Man In The Middle	
		Spoofing	
		Unauthorized Access	
		Masquerading Attacks	
		Sybil Attack	
	TAMPERING	Firmware Modification Attack	
		Tampering	
		Man In The Middle	
		Malware Attack	
		Buffer Overflow	
	REPUDIATION	Man In The Middle	
		Spoofing	
		Sybil Attack	
		Grey Hole	
	INFORMATION DISCLOSURE	Eavesdropping	
		Sniffing	
		Information Disclosure	
		Man In The Middle	
		Malware Attack	
		Replay Attack	
	DENIAL OF SERVICE	Side Channel Attack	
		DoS Attack	
		DDoS Attack	
		Resource Depletion	
		Jamming Attack	
	ELEVATION OF PRIVILEGE	Ransomware DOS	
		Deauthentication Attacks	
		Brute Force Attack	
		Unauthorized Access	
		Firmware Modification Attack	
		Buffer Overflow	
		Malware Attack	

Fonte: Elaborada pelo autor.

6.3 Discussão dos Resultados e Ameaças a Validade

A análise comparativa entre os *frameworks* STRIDE e MedSTRIDE permitiu avaliar a eficácia de cada abordagem no contexto específico de sistemas IoMT. Enquanto o STRIDE, amplamente utilizado em modelos de segurança tradicionais, oferece uma base sólida para identificar ameaças, o MedSTRIDE foi projetado para atender às particularidades de dispositivos médicos conectados, incorporando características adaptadas às vulnerabilidades e ativos dessa

área. A discussão dos resultados obtidos no experimento busca evidenciar como essas adaptações influenciaram na identificação de ameaças, a cobertura dos ativos mapeados e a usabilidade do *framework* em cenários médicos reais, fornecendo percepções relevantes para aprimoramentos futuros.

Os resultados são discutidos a partir de duas perspectivas. A primeira é a decomposição da arquitetura, que avalia a capacidade de identificar ativos críticos de um componente, considerando que esses ativos serão utilizados para a identificação de vulnerabilidades. A não identificação de um ativo pode resultar em vulnerabilidades não detectadas. A segunda perspectiva é a identificação de vulnerabilidades, visto que, sem o conhecimento prévio dos problemas, é difícil esperar que um dispositivo IoMT possua os mecanismos de segurança adequados.

Com relação à fase de decomposição dos componentes do sistema, 9 participantes do Grupo-B conseguiram entregar o diagrama com todos os ativos mapeados. No entanto, nenhum participante do Grupo-A conseguiu mapear 100% dos ativos da arquitetura. A partir desse resultado, podemos inferir que o modelo genérico para decomposição de ativos facilitou o processo de identificação dos ativos que compõem os elementos da arquitetura. Além disso, foi possível observar que os integrantes do Grupo-B levaram menos tempo para execução dessa fase do que os integrantes do Grupo-A.

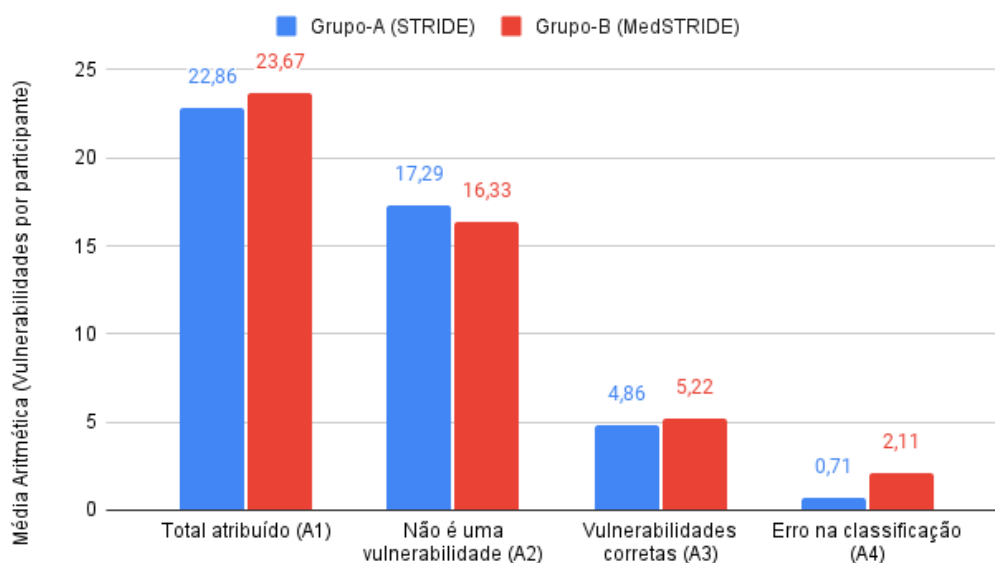
Após a fase de decomposição dos componentes do sistema, iniciamos a fase de identificação de ameaças, nessa fase todos (total de 26 participantes) os participantes iniciaram a atividade, sendo 13 pertencentes ao Grupo-A e 13 ao Grupo-B. No entanto, 6 participantes do Grupo-A e outros 4 do Grupo-B declinaram na fase de identificação de vulnerabilidades ao alegarem dificuldades na realização. Diante disso, apenas 7 participantes do Grupo-A conseguiram finalizar o experimento, enquanto que o Grupo-B alcançou 9 entregas. Nessa etapa do processo, também foi possível observar que os integrantes do Grupo-A concluíram a fase de identificação mais rapidamente. Entendemos que isso ocorreu porque o MedSTRIDE conta com um conjunto de 22 tipos de ataques, o que levou os participantes a analisarem todas as possibilidades, aumentando, como consequência, o tempo necessário para a realização da atividade.

Ao analisarmos os resultados do experimento, conforme demonstrado na Figura 23, realizamos a comparação dos modelos considerando quatro aspectos identificados nas entregas. Os aspectos usados para comparação serão identificados por siglas.

- **Total atribuído (A1):** Total de possíveis vulnerabilidades atribuídas;

- **Não é uma vulnerabilidade (A2):** atribuições inválidas como descrições e consequências de ataques que foram considerados como vulnerabilidades (fraquezas);
- **Vulnerabilidades corretas (A3):** vulnerabilidades corretamente atribuídas aos seus ativos e classes de ataques;
- **Erros na classificação (A4):** vulnerabilidades erroneamente atribuídas aos seus ativos e classes de ataques.

Figura 23 – Comparação dos resultados do experimento.



Fonte: Elaborada pelo autor.

No aspecto de avaliação (A1), que considera o total de vulnerabilidades atribuídas, o Grupo-B (MedSTRIDE) apresentou uma média maior por participante (23,67) em comparação ao Grupo-A (STRIDE), com 22,86. Essa diferença sugere que o MedSTRIDE pode estimular uma análise mais detalhada e abrangente. No entanto, essa maior quantidade de atribuições também pode refletir a maior complexidade da metodologia, que abrange 22 tipos de ataques, o que pode aumentar a probabilidade de erros quando se trata de profissionais menos experientes aplicando o modelo.

O Grupo-A apresentou uma média maior de atribuições inválidas (A2) (17,29) em comparação ao Grupo-B, que teve uma média de 16,33. Isso sugere que, embora o MedSTRIDE possua maior complexidade devido ao número de tipos de ataques considerados, ele pode oferecer uma estrutura mais clara ou intuitiva, ajudando os participantes a evitar identificações inválidas de vulnerabilidades.

A respeito do aspecto (A3), o Grupo-B (MedSTRIDE) teve maior sucesso na identi-

ificação de vulnerabilidades corretas, com uma média de 5,22 por participante, em comparação ao Grupo-A (STRIDE), que apresentou uma média de 4,86. Esses dados reforçam que o MedSTRIDE pode ser mais eficaz em destacar ameaças relevantes, ainda que isso venha acompanhado de maior esforço cognitivo por parte dos participantes.

No aspecto (A4), o número de erros na classificação foi mais alto no Grupo-B, com uma média de 2,11 por participante, em comparação ao Grupo-A, que apresentou uma média de 0,71. Esse resultado corrobora a ideia de que a maior complexidade do MedSTRIDE pode levar a confusões entre participantes com pouca experiência em modelagem de risco, aumentando a chance de erros ao associar vulnerabilidades a ativos ou classes de ataques.

A desistência de participantes durante a fase de identificação (6 no Grupo-A e 4 no Grupo-B) pode refletir dificuldades específicas de cada abordagem. O maior número de desistentes no Grupo-A (6) pode sugerir que o STRIDE oferece menos suporte estruturado ou clareza para orientar os participantes na tarefa. O Grupo-B, com 9 entregas, teve uma base de participantes ligeiramente maior. Ademais, ao analisar o aspecto (A2), observa-se que tanto o STRIDE quanto o MedSTRIDE apresentam desafios para os participantes na distinção entre vulnerabilidades reais e falsas, sendo o STRIDE o mais impactado nesse quesito.

Contudo, é importante considerar que a eficácia percebida na utilização do MedSTRIDE para a identificação de vulnerabilidades corretas pode refletir mais a estrutura detalhada do método do que a habilidade dos participantes em compreender as ameaças. Isso se torna ainda mais evidente ao levar em conta que os participantes não são especialistas em modelagem de risco ou em cibersegurança.

Por fim, é importante destacar que os resultados podem não ser diretamente aplicáveis a profissionais experientes, que provavelmente teriam maior facilidade em lidar com a complexidade do MedSTRIDE e a simplicidade do STRIDE. Além disso, o contexto acadêmico, por oferecer um ambiente controlado e sem a pressão de aplicações práticas, pode ocultar desafios reais, como a limitação de tempo para análises em cenários do mundo real.

7 CONCLUSÕES E TRABALHOS FUTUROS

7.1 Conclusões

Esta dissertação apresentou uma contribuição para o campo da segurança em sistemas da IoMT ao propor um método sistemático para a modelagem de risco específico para esse contexto. A proposta do modelo de risco apresentado nesta dissertação não só contribui para a segurança dos sistemas IoMT, mas oferece uma ferramenta útil e adaptável para pesquisadores e profissionais da área, permitindo uma melhor compreensão dos riscos associados à implementação e operação desses sistemas. As metodologias desenvolvidas e os ativos identificados formam a base para futuras pesquisas e podem ser adaptados para cenários emergentes da tecnologia IoMT, garantindo que as medidas de segurança evoluam conforme as ameaças e desafios se tornem mais sofisticados.

Quanto aos objetivos específicos, pode-se afirmar que todos foram plenamente atendidos no decorrer deste trabalho, com cada um deles desempenhando um papel crucial na construção da proposta apresentada.

O primeiro objetivo, de analisar as características e peculiaridades da IoMT para identificar os principais desafios relacionados à segurança nas camadas física e de adaptação, foi alcançado por meio de uma revisão detalhada da literatura e da discussão teórica presente nos capítulos iniciais. A pesquisa permitiu mapear vulnerabilidades críticas, como falhas em protocolos de comunicação, ataques ao *firmware* e problemas na heterogeneidade dos dispositivos conectados. Essa análise estabeleceu a base necessária para a proposta do *framework*, contextualizando os riscos e desafios específicos da IoMT.

No que diz respeito ao segundo objetivo, que buscava elaborar um modelo genérico de ativos para a IoMT, descrevendo componentes críticos das camadas física e de adaptação, sua realização foi consolidada na formulação do MedSTRIDE. Este modelo identificou e detalhou ativos essenciais, como hardware, *firmware*, sistemas operacionais e protocolos de comunicação, fornecendo um arcabouço estruturado para a modelagem de risco. A generalização desses ativos foi essencial para garantir a aplicabilidade do modelo em diferentes cenários de IoMT.

Ademais, o objetivo de classificar os ataques mais comuns na IoMT com base no *framework* STRIDE foi também atingido com êxito. A adaptação do *framework*, apresentada no Capítulo 5, categorizou ataques relevantes, como *side channel*, *gray hole* e *replay attack*, associando-os às respectivas categorias de ameaça. Essa abordagem ampliou a capacidade de

identificação e mapeamento de vulnerabilidades, alinhando o MedSTRIDE às peculiaridades dos dispositivos médicos conectados.

Por fim, a validação da extensão proposta do *framework* STRIDE, comparando sua eficácia na identificação de vulnerabilidades em relação ao modelo clássico, foi realizada com sucesso por meio de um estudo de caso e um experimento prático. Oferecendo uma avaliação inicial sobre a eficácia da metodologia de modelagem de risco aplicada aos sistemas IoMT. A análise dos resultados revelou a aplicabilidade do modelo, demonstrando sua capacidade de identificar e classificar os riscos associados aos 22 tipos de ataques identificados na literatura. Além disso, o modelo proposto demonstrou uma melhoria moderada na identificação de vulnerabilidades em comparação ao *framework* clássico. No entanto, acredita-se que sua eficácia será ainda mais evidenciada quando submetido a análises e testes conduzidos por especialistas da área, permitindo uma validação mais aprofundada e refinada de sua aplicabilidade no contexto da IoMT.

7.2 Limitações e Trabalhos Futuros

Uma das principais limitações deste trabalho refere-se à potencial carga cognitiva gerada pelo uso dos modelos STRIDE e MedSTRIDE, especialmente para usuários sem experiência prévia em cibersegurança ou modelagem de risco. A inclusão de 22 tipos de ataques do MedSTRIDE, ainda que amplie a abrangência e detalhamento da identificação de vulnerabilidades, pode tornar o processo mais desafiador para esses usuários. Essa complexidade adicional pode acarretar um maior tempo necessário para realizar as análises, impactando a eficiência do processo de identificação de vulnerabilidades.

Além disso, tanto no MedSTRIDE quanto no STRIDE clássico, observou-se uma taxa de desistência durante a fase de identificação de vulnerabilidades, destacando a dificuldade inerente da tarefa. Isso sugere que a modelagem de risco, como proposta, pode ser desmotivadora para indivíduos sem formação específica na área, reforçando a necessidade de abordagens mais intuitivas e ferramentas de suporte que reduzam essa barreira de entrada.

Outro aspecto importante é a ausência de experimentação com especialistas na área de cibersegurança. A validação do modelo foi realizada em um ambiente acadêmico controlado, utilizando participantes que, embora capacitados, não possuem a mesma experiência prática que profissionais atuantes no mercado. Essa limitação restringe a capacidade de avaliar a aplicabilidade dos modelos em cenários reais e sob as pressões características de ambientes

médicos conectados, como a necessidade de respostas rápidas e a alta criticidade dos sistemas envolvidos.

Ademais, o contexto acadêmico do experimento apresenta limitações adicionais. Embora o ambiente controlado ofereça vantagens em termos de organização e análise sistemática dos resultados, ele não reflete completamente as complexidades enfrentadas em sistemas reais de saúde conectada, onde fatores como recursos limitados, variabilidade tecnológica e pressão por decisões rápidas podem impactar a eficácia do modelo.

Portanto, futuras pesquisas poderiam abordar essas limitações, explorando formas de tornar o MedSTRIDE mais acessível a usuários inexperientes, ampliando a validação com especialistas e testando sua aplicação em cenários reais. Essas iniciativas permitiriam avaliar e aprimorar ainda mais o modelo, fortalecendo sua contribuição para a segurança na IoMT.

A colaboração com especialistas poderia também contribuir para a calibração do modelo e a identificação de potenciais melhorias, tornando-o ainda mais robusto e alinhado às necessidades do setor. A realização de experimentos com esse público em futuras pesquisas pode ser uma etapa crucial para a validação final da metodologia proposta e sua adaptação a contextos específicos da indústria de saúde conectada.

Uma outra proposta para trabalhos futuros seria o desenvolvimento de uma ferramenta web interativa para modelagem de ameaças baseada no *framework* MedSTRIDE, com a capacidade de relacionar ativos específicos com ataques e identificar riscos de maneira dinâmica e acessível. Essa ferramenta poderia fornecer uma interface intuitiva para profissionais e pesquisadores da área de segurança em IoMT, permitindo a criação e visualização de modelos de risco em tempo real. Ao integrar funcionalidades que conectam ativos críticos com os tipos de ataques específicos identificados, a ferramenta permitiria uma análise mais profunda dos riscos e vulnerabilidades dos sistemas IoMT.

REFERÊNCIAS

- AIRCRAK-NG Documentation. Disponível em: <https://www.aircrack-ng.org/documentation.html>. Acesso em: 02 dez 2023.
- ALMOHRI, H.; CHENG, L.; YAO, D.; ALEMZADEH, H. On threat modeling and mitigation of medical cyber-physical systems. In: **2017 IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE)**. [S. l.]: IEEE, 2017. p. 114–119.
- ALSUBAEI, F.; ABUHUSSEIN, A.; SHIVA, S. Security and privacy in the internet of medical things: taxonomy and risk assessment. In: IEEE. **2017 IEEE 42nd conference on local computer networks workshops (LCN workshops)**. [S. l.], 2017. p. 112–120.
- ANALYTICS, I. **State of IoT 2022**: Number of connected iot devices growing 18% to 14.4 billion globally. 2022. Disponível em: <https://iot-analytics.com/number-connected-iot-devices/>. Acesso em: 08 mai. 2023.
- ANALYTICS, I. **State of IoT 2023**: Number of connected iot devices growing 16% to 16.7 billion globally. 2023. Disponível em: <https://iot-analytics.com/number-connected-iot-devices/>. Acesso em: 06 jun. 2024.
- ANJIELO. **What is Wi-Fi HaLow? Tuya Wi-Fi HaLow IP Camera**. 2022. Disponível em: <https://anjielo.com/blogs/anjielo/what-is-wi-fi-halow-tuya-wifi-halow-ip-camera>. Acesso em: 02 dez 2023.
- ARRIETA, A.; BATTELINO, T.; SCARAMUZZA, A. E.; SILVA, J. D.; CASTAÑEDA, J.; CORDERO, T. L.; SHIN, J.; COHEN, O. Comparison of minimed 780g system performance in users aged younger and older than 15 years: Evidence from 12,870 real-world users. **Diabetes, Obesity and Metabolism**, Wiley Online Library, v. 24, n. 7, p. 1370–1379, 2022.
- ASIF, M. R. A.; HASAN, K. F.; ISLAM, M. Z.; KHONDOKER, R. Stride-based cyber security threat modeling for iot-enabled precision agriculture systems. In: IEEE. **2021 3rd International Conference on Sustainable Technologies for Industry 4.0 (STI)**. [S. l.], 2021. p. 1–6.
- BEARDSLEY, T. **R7-2016-07**: Multiple vulnerabilities in animas onetouch ping insulin pump. 2016. Disponível em: <https://www.rapid7.com/blog/post/2016/10/04/r7-2016-07-multiple-vulnerabilities-in-animas-onetouch-ping-insulin-pump/>. Acesso em: 16 set. 2024.
- BIOSPACE. **IoT in Healthcare Market To Reach USD 260.75 Billion By 2027– Reports and Data**. 2021. Disponível em: <https://www.biospace.com/article/iot-in-healthcare-market-to-reach-usd-260-75-billion-by-2027-reports-and-data/>. Acesso em: 24 out. 2023.
- BISDIKIAN, C. An overview of the bluetooth wireless technology. **IEEE Communications magazine**, IEEE, v. 39, n. 12, p. 86–94, 2001.
- BOCHNIEWICZ, E.; CHASE, M.; COLEY, S. C.; WALLACE, K.; WEIR, M.; ZUK, M. **Playbook for Threat Modeling Medical Devices**. 2021. Disponível em: <https://www.mitre.org/news-insights/publication/playbook-threat-modeling-medical-devices>. Acesso em: 27 out. 2024.

BRANQUINHO, T.; BRANQUINHO, M. **Segurança cibernética industrial**: as infraestruturas críticas mundiais correm perigo. aprenda a proteger redes e sistemas de controle com uma metodologia comprovada na prática. Rio de Janeiro: Alta Books, 2021. E-book. ISBN 978-65-5520-466-7. Acesso em: 1 dez. 2023.

CAGNAZZO, M.; HERTLEIN, M.; HOLZ, T.; POHLMANN, N. Threat modeling for mobile health systems. In: IEEE. **2018 IEEE Wireless Communications and Networking Conference Workshops (WCNCW)**. [S. l.], 2018. p. 314–319.

CHALLOO, R.; OLADEINDE, A.; YILMAZER, N.; OZCELIK, S.; CHALLOO, L. An overview and assessment of wireless technologies and co-existence of zigbee, bluetooth and wi-fi devices. **Procedia Computer Science**, Elsevier, v. 12, p. 386–391, 2012.

CHANTZIS, F.; STAIS, I.; CALDERON, P.; DEIRMENTZOGLOU, E.; WOODS, B. **Practical IoT hacking: the definitive guide to attacking the internet of things**. [S. l.]: No Starch Press, 2021.

CHOWDHURY, S. N.; KUHIKAR, K. M.; DHAWAN, S. Iot architecture: A survey. **International Journal of Industrial Electronics and Electrical Engineering (IJIEEE)**, v. 3, n. 5, May 2015.

COPPENS, D.; SHAHID, A.; LEMEY, S.; HERBRUGGEN, B. V.; MARSHALL, C.; POORTER, E. D. An overview of uwb standards and organizations (ieee 802.15. 4, fir, apple): Interoperability aspects and future research directions. **IEEE Access**, IEEE, v. 10, p. 70219–70241, 2022.

DAVITEQ. **Temperature Monitoring Solution for Vaccine Cabinet**. Disponível em: <https://www.daviteq.com/en/use-cases/monitoring-use-case-for-vaccine-pharmaceutical-warehouse/>. Acesso em: 07 nov. 2023.

DIVISION, F. C. **Unpatched and Outdated Medical Devices Provide Cyber Attack Opportunities**. 2022. Disponível em: <https://www.aha.org/system/files/media/file/2022/protect-penalty-\@M09/fbi-pin-ttp-white-unpatched-and-outdated-medical-devices-\protect-penalty-\@Mprovide-cyber-attack-opportunities-sept-12-2022.pdf>. Acesso em: 09 nov. 2023.

EARLE, N. **IoT Tech News**. 2022. Disponível em: <https://www.iottechnews.com/news/2022/jul/12/iot-drives-rapid-growth-in-uk-digital-healthcare/>. Acesso em: 09 mai. 2023.

ELLOUZE, N.; ALLOUCHE, M.; AHMED, H. B.; REKHIS, S.; BOUDRIGA, N. Securing implantable cardiac medical devices: Use of radio frequency energy harvesting. In: **Proceedings of the 3rd International Workshop on Trustworthy Embedded Devices**. [S. l.]: IEEE, 2013. p. 35–42.

Food and Drug Administration (FDA). **Digital Health Center of Excellence - Cybersecurity**. 2024. Disponível em: <https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity>. Acesso em: 27 de outubro de 2024.

FOROUZAN, B. A.; MOSHARRAF, F. **Redes de Computadores**: uma abordagem top-down. Porto Alegre, RS: Grupo A, 2013. E-book. ISBN 9788580551693. Disponível em: <https://app.minhabiblioteca.com.br/#/books/9788580551693/>. Acesso em: 20 nov. 2023.

GEELHOED-DUIJVESTIJN, P.; VEGELYTE, D.; KOWNACKA, A.; ANTON, N.; JOOSSE, M.; WILSON, C. **Performance of the Prototype NovioSense Noninvasive Biosensor for Tear Glucose in Type 1 Diabetes**. 2020. Disponível em: <https://journals.sagepub.com/doi/10.1177/1932296820964844>. Acesso em: 30 out. 2023.

GHUBAISH, A.; SALMAN, T.; ZOLANVARI, M.; UNAL, D.; AL-ALI, A.; JAIN, R. Recent advances in the internet-of-medical-things (iomt) systems security. **IEEE Internet of Things Journal**, IEEE, v. 8, n. 11, p. 8707–8718, 2020.

HANDS, C. H. S. **REDUCE INFECTIONS By Improving Hand Hygiene**. 2018. Disponível em: <https://cleanhands-safehands.com/wp-content/uploads/2018/10/CHSH-Brochure-1018.pdf>. Acesso em: 30 out. 2023.

HASAN, M. K.; GHAZAL, T. M.; SAEED, R. A.; PANDEY, B.; GOHEL, H.; ESHMAWI, A.; ABDEL-KHALEK, S.; ALKHASSAWNEH, H. M. A review on security threats, vulnerabilities, and counter measures of 5g enabled internet-of-medical-things. **IET communications**, Wiley Online Library, v. 16, n. 5, p. 421–432, 2022.

HASSAN, W. H. *et al.* Current research on internet of things (iot) security: A survey. **Computer networks**, Elsevier, v. 148, p. 283–294, 2019.

INDUSTRIES, G. **Innovative Measurement Tools**. 2017. Disponível em: <https://www.gojo.com/en/Electronic-Monitoring-Systems/Healthcare-EMS/SMARTLINK-Technology>. Acesso em: 30 out. 2023.

INSTITUTE, P. **The Impact of Ransomware on Healthcare During COVID-19 and Beyond**. [S. l.], 2021. Disponível em: https://assets-global.website-files.com/63bc855e7cb1897eeb806ea7/6532d7b6718a3de763b9cbd1_Ponemon%20Research%20Report%20-%20The%20Impact%20of%20Ransomware%20on%20Healthcare%20During%20COVID-19%20and%20Beyond.pdf. Acesso em: 08 mai. 2023.

JAIN, R.; GAWRE, S. K. Monitoring and control of covid vaccine storage temperature using iot and machine learning. In: **2022 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS)**. [S. l.]: IEEE, 2022. p. 1–6.

JR., E. E. S.; BROWN, D. S.; LONGSTAFF, T. A. **Responding to computer security incidents: Guidelines for incident handling**. Livermore, CA, 1990. DOE Contract Number: W-7405-ENG-48. Acesso em: 09 mai. 2023.

KHAN, R.; MCLAUGHLIN, K.; LAVERTY, D.; SEZER, S. Stride-based threat modeling for cyber-physical systems. In: IEEE. **2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)**. [S. l.], 2017. p. 1–6.

KHANDELWAL, S. **Medtronic's Implantable Defibrillators Vulnerable to Life-Threatening Hacks**. 2019. Disponível em: <https://thehackernews.com/2019/03/hacking-implantable-defibrillators.html>. Acesso em: 07 nov. 2023.

KIM, Y.; LEE, W.; RAGHUNATHAN, A.; RAGHUNATHAN, V.; JHA, N. K. Reliability and security of implantable and wearable medical devices. In: **Implantable Biomedical Microsystems**. [S. l.]: Elsevier, 2015. p. 167–199.

KWAK, K. S.; ULLAH, S.; ULLAH, N. An overview of ieee 802.15. 6 standard. p. 1–6, 2010.

- LONZETTA, A. M.; COPE, P.; CAMPBELL, J.; MOHD, B. J.; HAYAJNEH, T. Security vulnerabilities in bluetooth technology as used in iot. **Journal of Sensor and Actuator Networks**, MDPI, v. 7, n. 3, p. 28, 2018.
- LU, Y.; PENG, H.; ZHAO, J.; DENG, Z.; HUANG, Z.; ZHANG, J.; DENG, J.; WANG, Z.; WEI, C. Ubiquitous blood pressure monitoring using eeg and ppg signals. In: **Proceedings of the 2017 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2017 ACM International Symposium on Wearable Computers**. New York, NY, USA: ACM, 2017. p. 257–260.
- MALAMAS, V.; CHANTZIS, F.; DASAKLIS, T. K.; STERGIOPOULOS, G.; KOTZANIKOLAOU, P.; DOULIGERIS, C. Risk assessment methodologies for the internet of medical things: A survey and comparative appraisal. **IEEE Access**, IEEE, v. 9, p. 40049–40075, 2021.
- MARTINO, B. D.; RAK, M.; FICCO, M.; ESPOSITO, A.; MAISTO, S. A.; NACCHIA, S. Internet of things reference architectures, security and interoperability: A survey. **Internet of Things**, Elsevier, v. 1, p. 99–112, 2018.
- MASCHIETTO, L. G.; VIEIRA, A. L. N.; TORRES, F. E.; AL. et. **Arquitetura e Infraestrutura de IoT**. Porto Alegre: SAGAH, 2021. E-book. p. Capa. ISBN 9786556901947. Disponível em: <https://app.minhabiblioteca.com.br/reader/books/9786556901947/>. Acesso em: 20 nov. 2023.
- MATHKOR, D. M.; MATHKOR, N.; BASSFAR, Z.; BANTUN, F.; SLAMA, P.; AHMAD, F.; HAQUE, S. Multirole of the internet of medical things (iomt) in biomedical systems for managing smart healthcare systems: An overview of current and future innovative trends. **Journal of infection and public health**, Elsevier, 2024.
- Medtronic. **MiniMed 780G System**. 2024. Disponível em: https://info.medtronicdiabetes.com/MiniMed780G_BR. Acesso em: 02 dez. 2023.
- MNJAMA, J.; FOSTER, G.; IRWIN, B. A privacy and security threat assessment framework for consumer health wearables. In: IEEE. **2017 Information Security for South Africa (ISSA)**. [S. l.], 2017. p. 66–73.
- MORAES, A. d.; HAYASHI, V. T. **Segurança em IoT**. Rio de Janeiro: Editora Alta Books, 2021. E-book. p. iii. ISBN 9788550816548. Disponível em: <https://app.minhabiblioteca.com.br/reader/books/9788550816548/>. Acesso em: 20 nov. 2023.
- MOUSSA, A.; JABRI, I. Impact of rts/cts jamming attacks in iee 802.11 ah dense networks. In: **2021 International Wireless Communications and Mobile Computing (IWCMC)**. N/A: IEEE, 2021. p. 1551–1556.
- OMOTOSHO, A.; HARUNA, B. A.; OLANIYI, O. M. Threat modeling of internet of things health devices. **Journal of Applied Security Research**, Taylor & Francis, v. 14, n. 1, p. 106–121, 2019.
- OWASP. **OWASP Firmware Security Testing Methodology**. 2024. Disponível em: https://owasp.org/owasp-istg/03_test_cases/firmware/index.html. Acesso em: 12 mar. 2024.

PAPAIIOANNOU, M.; KARAGEORGOU, M.; MANTAS, G.; SUCASAS, V.; ESSOP, I.; RODRIGUEZ, J.; LYMBERPOULOS, D. A survey on security threats and countermeasures in internet of medical things (iomt). **Transactions on Emerging Telecommunications Technologies**, Wiley Online Library, v. 33, n. 6, p. e4049, 2022.

PRODANOV, C. C.; FREITAS, E. C. D. **Metodologia do trabalho científico: métodos e técnicas da pesquisa e do trabalho acadêmico**. 2. ed. [S. l.]: Editora Feevale, 2013.

PULSE, I. **IoMT (Internet of Medical Things): Reducing Cost While Improving Patient Care**. 2023. Disponível em: <https://www.embs.org/pulse/articles/iomt-internet-of-medical-things-reducing-cost-while-improving-patient-care/>. Acesso em: 25 out. 2023.

QASEM, A.; SHIRANI, P.; DEBBABI, M.; WANG, L.; LEBEL, B.; AGBA, B. L. Automatic vulnerability detection in embedded devices and firmware: Survey and layered taxonomies. **ACM Computing Surveys (CSUR)**, ACM New York, NY, USA, v. 54, n. 2, p. 1–42, 2021.

QIAO, L.; ZHENG, Z.; CUI, W.; WANG, L. A survey on wi-fi halow technology for internet of things. In: **2018 2nd IEEE Conference on Energy Internet and Energy System Integration (EI2)**. [S. l.]: IEEE, 2018. p. 1–5.

RASOOL, R. U.; AHMAD, H. F.; RAFIQUE, W.; QAYYUM, A.; QADIR, J. Security and privacy of internet of medical things: A contemporary review in the age of surveillance, botnets, and adversarial ml. **Journal of Network and Computer Applications**, Elsevier, v. 201, p. 103332, 2022.

SHEVCHENKO, N.; CHICK, T. A.; O'RIORDAN, P.; SCANLON, T. P.; WOODY, C. Threat modeling: a summary of available methods. **Software Engineering Institutel Carnegie Mellon University**, 2018.

SHOSTACK, A. **Threat modeling: designing for security**. [S. l.]: John Wiley & Sons, 2014.

SILVA, F. R. d.; SOARES, J. A.; SILVA, L. P. C.; AL. et. **Redes sem fio**. Grupo A, 2021. E-book. ISBN 9786556901374. Disponível em: <https://app.minhabiblioteca.com.br/#/books/9786556901374/>. Acesso em: 13 nov. 2023.

SOUPPAYA, M.; SCARFONE, K. **Guide to data-centric system threat modeling**. [S. l.], 2016. Disponível em: <https://csrc.nist.gov/pubs/sp/800/154/ipd>. Acesso em: 26 mai. 2023.

SUN, Y.; LO, F. P.-W.; LO, B. Security and privacy for the internet of medical things enabled healthcare systems: A survey. **IEEE Access**, IEEE, v. 7, p. 183339–183355, 2019.

VODAFONE. **Vodafone claims Internet Of Things connected healthcare can improve millions of lives and save billions of dollars**. 2017. Disponível em: <https://www.vodafone.com/business/news-and-insights/press-release/vodafone-claims-internet-of-things-connected-healthcare>. Acesso em: 30 out. 2023.

YAACOUB, J.-P. A.; NOURA, M.; NOURA, H. N.; SALMAN, O.; YAACOUB, E.; COUTURIER, R.; CHEHAB, A. Securing internet of medical things systems: Limitations, issues and recommendations. **Future Generation Computer Systems**, Elsevier, v. 105, p. 581–606, 2020.

YAQOOB, T.; ABBAS, H.; ATIQUZZAMAN, M. Security vulnerabilities, attacks, countermeasures, and regulations of networked medical devices—a review. **IEEE Communications Surveys & Tutorials**, IEEE, v. 21, n. 4, p. 3723–3768, 2019.

ZUBAIR, M.; UNAL, D.; AL-ALI, A.; SHIKFA, A. Exploiting bluetooth vulnerabilities in e-health iot devices. In: **Proceedings of the 3rd international conference on future networks and distributed systems**. [*S. l.: s. n.*], 2019. p. 1–7.