PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
ESCOLA POLITÉCNICA E DE ARTES
GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

SIMULAÇÃO DE ATAQUES CIBERNÉTICOS NOS DISPOSITIVOS IOT EM AMBIENTES DE SAÚDE.

MATHEUS RODRIGUES TENAGLIA

GOIÂNIA
2023

MATHEUS RODRIGUES TENAGLIA

SIMULAÇÃO DE ATAQUES CIBERNÉTICOS NOS DISPOSITIVOS IOT EM AMBIENTES DE SAÚDE.

Trabalho de Conclusão de Curso apresentado à Escola Politécnica e de Artes, da Pontifícia Universidade de Goiás, como parte dos requisitos para obtenção do título de Bacharel em Ciência da Computação

Orientador (a):

Profª. Dr. Solange da Silva.

Banca examinadora:

Prof. Me. Aníbal dos Santos Jukemura

Profª. Ma. Lucilia Gomes Ribeiro

GOIÂNIA
2023

MATHEUS RODRIGUES TENAGLIA

SIMULAÇÃO DE ATAQUES CIBERNÉTICOS NOS DISPOSITIVOS IOT EM AMBIENTES DE SAÚDE.

Trabalho de Conclusão de Curso aprovado em sua forma final pela Escola Politécnica e de Artes, da Pontifícia Universidade Católica de Goiás, para obtenção do título de Bacharel em Ciências da Computação, em: __18__/__06__/__2024_____.

_____
Orientador (a): Profª. Dr. Solange da Silva.

_____
Prof. Me. Aníbal dos Santos Jukemura

_____
Profª. Ma. Lucilia Gomes Ribeiro

GOIÂNIA
2023

Dedico este trabalho para meus pais pelo apoio e carinho que sempre me proporcionaram até aqui.

AGRADECIMENTOS

À Deus por ter me dado forças.

Agradeço minha mãe por ajudar na minha formação e sempre me incentivar. Também sou grato ao meu pai pelo apoio nas decisões que tomei durante esses anos.

Um agradecimento especial à minha orientadora, Solange da Silva, pela sua paciência e ajuda com o meu TCC.

Por fim, agradeço a todos os meus professores e a todos que ajudaram de alguma forma no meu trabalho.

RESUMO

O objetivo geral foi realizar uma revisão bibliográfica para identificar os ataques e vulnerabilidades nos dispositivos IoT em ambientes de saúde, bem como simular um ataque cibernético para ilustrar esses pontos fracos e sugerir estratégias que garantam a privacidade e a segurança das informações dos pacientes. Durante o estudo, observou-se que as principais brechas identificadas na Internet das Coisas incluem senhas fracas, serviços de rede instáveis, interfaces inseguras, falta de mecanismos de atualização, uso de componentes defasados, proteção insuficiente de privacidade, transferência e armazenamento de dados precária, falta de controle de gerenciamento dos dispositivos, configuração padrão vulnerável e segurança física insuficiente. Ataques de clonagem e interferências no RFID, injeção de mensagem, DoS, DDoS e *spoofing* são ameaças reais e frequentes nesse contexto. Esses riscos, combinados com o aumento de coleta e análise de dados pessoais, tornam o desafio da proteção ainda maior. Isso é ainda mais crítico quando se trata de dispositivos conectados à saúde, uma vez que os dados envolvidos são altamente sensíveis. A simulação do ataque cibernético mostrou como essas fragilidades podem ser exploradas e quais são seus impactos em um ambiente de saúde conectado. Esse entendimento é fundamental para desenvolver estratégias de proteção eficazes. Com base ainda nos estudos conclui-se que garantir a privacidade e segurança dos pacientes requer: usar *firewalls* para bloquear acessos não autorizados e monitorar qualquer entrada suspeita na rede. Isso ajuda a criar uma barreira sólida contra possíveis ataques. Manter todos os dispositivos atualizados com as últimas correções de segurança para evitar que falhas conhecidas sejam exploradas por usuários mal-intencionados. Possuir sistemas fortes de autenticação e controle de acesso para garantir que só pessoas autorizadas acessem os dispositivos e dados. Monitorar a rede em tempo real e criptografar as comunicações ajuda a proteger a informação que circula, mantendo-a segura e privada. Realizar campanhas educativas aos funcionários e pacientes para ajudar a todos entender os riscos e a adotar práticas de segurança melhores.

Palavras chaves: Ataques Cibernéticos. Internet das Coisas. Segurança da Informação. Saúde. LGPD.

ABSTRACT

The general objective was to conduct a literature review to identify attacks and vulnerabilities in IoT devices in healthcare environments, as well as to simulate a cyberattack to illustrate these weaknesses and suggest strategies that ensure the privacy and security of patient information. During the study, it was observed that the main gaps identified in the Internet of Things include weak passwords, unstable network services, insecure interfaces, lack of update mechanisms, use of outdated components, insufficient privacy protection, poor data transfer and storage, lack of device management control, vulnerable default configuration, and insufficient physical security. Cloning and interference attacks on RFID, message injection, DoS, DDoS, and spoofing are real and frequent threats in this context. These risks, combined with the increase in the collection and analysis of personal data, make the challenge of protection even greater. This is even more critical when it comes to connected healthcare devices, as the data involved is highly sensitive. The cyberattack simulation showed how these vulnerabilities can be exploited and what their impacts are in a connected healthcare environment. This understanding is fundamental for developing effective protection strategies. Based on the studies, it is concluded that ensuring patient privacy and security requires: using firewalls to block unauthorized access and monitor any suspicious network entries. This helps create a solid barrier against potential attacks. Keeping all devices updated with the latest security patches to prevent known vulnerabilities from being exploited by malicious users. Having strong authentication and access control systems to ensure that only authorized people can access the devices and data. Monitoring the network in real-time and encrypting communications helps protect the information circulating, keeping it secure and private. Conducting educational campaigns for employees and patients to help everyone understand the risks and adopt better security practices.

Keywords: Cyber Attacks. Internet of Things. Information Security. Health. LGPD.

LISTA DE ILUSTRAÇÕES

LISTA DE SIGLAS E ABREVIATURAS

4G	*Fourth Generation*
5G	*Fifth Generation*
AES	*Advanced Encryption Standard*
ANDP	*Autoridade Nacional de Proteção de Dados*
API	*Application Programming Interface*
DoS	*Denial of Service*
DDoS	*Distributed Denial of Service*
EPC	*Electronic Product Codes*
GDPR	*General Data Protection Regulation*
IDE	*Integrated Development Environment* ou ambiente de desenvolvimento integrado
IoT	*Internet of Things ou* Internet das Coisas
IP	*Internet Protocol*
IPv4	*Internet Protocol version 4*
IPv6	*Internet Protocol version 6*
ISO	*International Organization for Standardization* ou Organização Internacional para Padronização
LGPD	Lei Geral de Proteção de Dados
MIT	Massachusetts Institute of Technology
OWASP	*Open Web Application Security Project*
RFID	*Radio Frequency Identification* ou identificação por radiofrequência
SI	Segurança da Informação
SSH	*Secure Shell*
uCode	*ubiquitous Code*
VMs	*Virtual Machines* ou máquinas virtuais
WIFI	*Wireless Fidelity*

SUMÁRIO

1 INTRODUÇÃO

Os dados são o ouro da era digital. As organizações que sabem como extrair valor dos dados são as que têm mais chances de sucesso (Botelho; Camargo, 2021). É nesse contexto de busca eficiente na manipulação e utilização de dados que surge a Internet das Coisas também conhecida como *Internet of Things* (IoT).

A IoT é o conjunto de objetos físicos conectados à rede que podem coletar e transmitir dados. Esses objetos podem ser usados para interagir e cooperar entre si para alcançar um objetivo comum (Marques; Pitarma, 2019). Essa integração do mundo físico e virtual é feita por meio da coleta, processamento e análise de dados gerados por dispositivos conectados à Internet (Rosa; Souza; Silva, 2020).

Essa ideia pode ser usada em diversos setores, desde aplicações simples em residências até avanços que trazem benefícios significativos para a sociedade, como o monitoramento da qualidade da água e a gestão remota de pragas na agricultura (Kinjo, 2022).

Considerando essa vasta gama de campos na qual a Internet das Coisas é usada, seu impacto na área da saúde é particularmente significativo. Dois exemplos notáveis são os *smartwatches* que verifica sinais vitais e a telemedicina (Kinjo, 2022).

Os dados gerados por essa tecnologia podem ser aplicados em diferentes áreas da medicina, desde monitoramento remoto de pacientes até identificação de causas das doenças, resultando em abordagens e tratamentos mais eficazes, que elevam a qualidade de vida da população (Salgado; Blank, 2020).

IoT de fato apresenta benefícios na saúde, mas também traz riscos e desafios que precisam ser considerados. Um dos principais desafios é a proteção da privacidade, pois é gerado grandes quantidades de dados pessoais que podem ser usados para fins maliciosos (Kinjo, 2022). Essa preocupação torna-se ainda mais crítica quando a maior parte dos dados na área médica são extremamente sensíveis (Botelho; Camargo, 2021).

Assim, a Lei Geral de Proteção de Dados (LGPD), sancionada no Brasil em 2018, tem como objetivo proteger os direitos relacionados aos dados pessoais dos indivíduos e regular a coleta e o processamento dessas informações. Portanto, é de extrema importância desenvolver um planejamento e gerenciamento de riscos para proteger as informações quando se usa IoT (Salgado; Blank, 2020).

Justifica-se pesquisar sobre este tema, pois existe uma necessidade de tratamento adequado e mais cauteloso dos dados de saúde nas instituições brasileiras que utilizam dispositivos IoT (Salgado; Blank, 2020). Esses aparelhos, ao mesmo tempo que oferecem avanços na medicina, também apresentam brechas que podem ser exploradas por atacantes, comprometendo a privacidade e segurança dos dados dos pacientes (Kinjo, 2022).

Diante deste contexto, esta pesquisa pretende responder a seguinte questão: - Quais são os ataques e vulnerabilidades nos dispositivos IoT em ambientes de saúde?

O objetivo geral é realizar uma revisão bibliográfica para identificar os ataques e vulnerabilidades nos dispositivos IoT em ambientes de saúde, bem como simular um ataque cibernético para ilustrar esses pontos fracos e sugerir estratégias que garantam a privacidade e a segurança das informações dos pacientes.

Os objetivos específicos são:

- Aprofundar o estudo de IoT;
- Estudar a Lei Geral de Proteção de Dados;
- Analisar brechas e possíveis ataques;
- Simular um ataque cibernético em um ambiente de saúde conectado para ilustrar as vulnerabilidades e os impactos potenciais;
- Sugerir estratégias de mitigação;

Espera-se que os resultados desta pesquisa possam auxiliar:

- Na identificação de melhores práticas para mitigação;
- Na detecção dos riscos específicos à privacidade e segurança que surgem quando dispositivos IoT são utilizados;
- Informando como as tecnologias IoT são empregadas na área da saúde brasileira;

2 REFERENCIAL TEÓRICO

Este capítulo divide-se em duas seções: uma abordando conceitos e definições e outra discutindo trabalhos relacionados.

2.1 Conceitos e definições

Dispositivos que antes não eram conectados à rede agora podem coletar dados, gerar informações para monitoramento, automatizar tarefas ou facilitar a vida do usuário, encaixando-se na ideia de IoT (Al-Fuqaha, 2015). A Figura 1 ilustra algumas dessas aplicações em setores que antes não estavam interconectados

Figura 1 - Aplicações IoT

Fonte: Adaptado de Thakor (2020)

A Internet das Coisas tem como objetivo preencher a lacuna entre o mundo virtual e físico usando os objetos, os conectando em uma rede de informações. Isso permite melhor capacidade de comunicação, interação e processamento de dados (Batista; Ramalho; Nader, 2021).

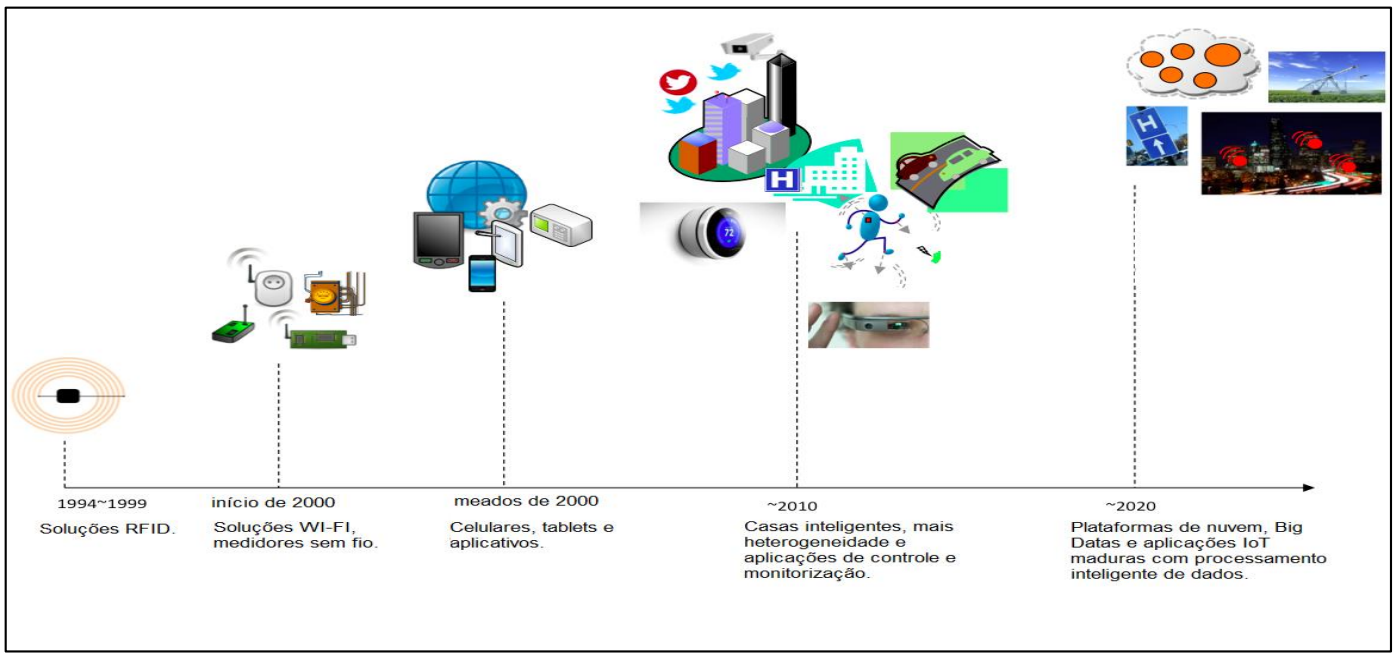
A tecnologia de *Radio Frequency Identification* (RFID) ou identificação por radiofrequência, é a base da Internet das Coisas. É usada em muitas aplicações, como etiquetas de identificação de caixas, roupas e outros objetos (Faccioni FIlho, 2016). Essa inovação surgiu na Segunda Guerra Mundial para identificar aviões aliados e inimigos. Os aviões, ao captar o sinal, deveria refletir ou emitir um novo sinal (Minerva; Biru; Rotondi, 2015).

Na virada do milênio, estudiosos reconheceram o potencial do RFID e começaram a explorar suas possibilidades. Em 1999, o Instituto de Tecnologia de Massachusetts (MIT) estabeleceu o *Auto-ID Center*, um centro de estudos que se dedicava à pesquisa e desenvolvimento de tecnologias para permitir que etiquetas RFID se comunicassem com a Internet (Minerva; Biru; Rotondi, 2015).

No mesmo ano, Neil Gershenfeld, outro pesquisador do MIT, publicou o livro *"When Things Start to Think"*, no qual sugeriu que os objetos não apenas seriam identificáveis, mas também teriam a capacidade de se comunicar diretamente com a Internet. Kevin Ashton, outro pesquisador do *Auto-ID Center*, consolidou essa visão em 2002, definindo o termo "Internet das Coisas" para descrever esse novo paradigma de objetos conectados e intercomunicáveis. (Faccioni FIlho, 2016).

Desde então, esse cenário é espaço para discussão e evoluções tecnológicas. A Figura 2 ilustra esse progresso ao longo dos anos.

Figura 2 - Evolução histórica do IoT



Fonte: Adaptado de Payam e Amit (2014)

Segundo Faccioni Filho (2016) o que difere IoT de outras redes de sistemas interconectados é a funcionalidade dos objetos, que podem ser físicos ou virtuais. Essas funcionalidades são divididas em nove características, conforme apresentado na Figura 3, e distribuídas em três conjuntos: características, relações e interface.

Figura 3 – Nove Características dos Objetos IoT

Fonte: Faccioni FIlho (2016)

No conjunto das **características**, existem as funcionalidades abaixo:

- **Processamento**: Referente a capacidade computacional de processamento do objeto;
- **Endereçamento**: Refere-se na capacidade o objeto ser localizado na rede por meio do roteamento, em resumo é seu endereço IP para comunicação em rede. Existem vários métodos de endereçamento, como *Internet Protocol version 4* (IPv4) e Internet Protocol version 6 (IPv6) (Marques; Pitarma, 2019);
- **Identificação**: Garante o correto reconhecimento dos objetos. Em resumo é o seu nome. Existem vários métodos de identificação, tais

como *Electronic Product Codes* (EPC) e *ubiquitous Code* (uCode) (Marques; Pitarma, 2019);

- **Localização**: É relacionada com a posição real que o objeto se encontra.

No conjunto das **relações** entre objetos IoT, são separadas as seguintes funcionalidades:

- **Comunicação**: É a capacidade do objeto de receber e enviar mensagens. É uma característica fundamental, porém limitada por fatores como duração de bateria e alcance de transmissão. Protocolos como *Wireless Fidelity* (WIFI), *Fourth Generation* (4G) e *Fifth Generation* (5G) proporcionam a comunicação entre os dispositivos (Marques; Pitarma, 2019);
- **Cooperação**: Visa o trabalho em conjunto entre os objetos;
- **Sensoriamento:** Refere-se aos dispositivos que coletam dados do ambiente e os enviam para uma base de dados, seja ela remota ou na nuvem. Os sensores inteligentes e os *wearable* são alguns exemplos de sensores usados na IoT (Marques; Pitarma, 2019);
- **Atuação**: É a capacidade do objeto se adaptar com o ambiente.

Por fim, o conjunto da **interface** é relacionada com a interação do usuário e o objeto, na qual é permitido ver as informações e realizar configurações se necessário.

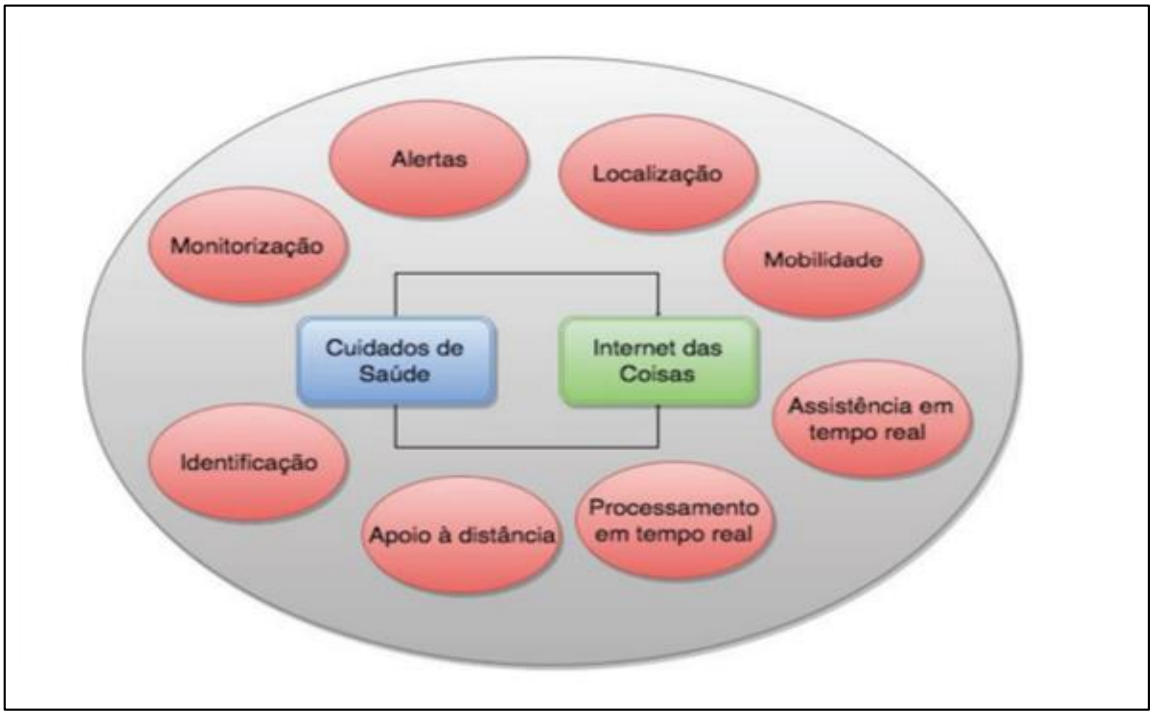
A saúde e medicina estão passando por uma revolução após a incorporação desse conceito, pois facilita processos, economiza tempo e recursos, minimiza erros humanos, personaliza tratamentos e fornece dados para prevenção de doenças (Rosa; Souza; Silva, 2020).

As principais inovações dessas áreas com o IoT podem ser divididas em três categorias essenciais. A primeira é marcada pelo uso de dispositivos vestíveis, os *wearables*, e sensores que coletam dados sobre o corpo e o comportamento das pessoas, permitindo diagnósticos remotos e acompanhamentos mais precisos, como pulseiras ou relógios que monitoram o batimento cardíaco do usuário. A segunda é relacionada com a telemedicina que possibilita consultas e tratamentos médicos sem descolamento físico. E, por último, surgem novas plataformas digitais com o objetivo de ajudar as pessoas a adotarem estilos de vida saudáveis, prevenindo doenças e promovendo o bem-estar. Por exemplo, aplicações de celulares para perda de peso e a desistência do tabagismo (Silva; Oliveira; 2017).

Esses avanços tecnológicos também se aplicam à utilização de aplicativos para verificar resultados de exames médicos e marcar consultas (Azevedo; Oliveira; Carneiro; 2021).

Essas categorias têm como finalidade tornar as informações mais acessíveis e acelerar sua aplicação em benefício dos pacientes. Além disso, elas contribuem para a diminuição de erros ligados a procedimentos manuais, o que possibilita a implementação de sistemas automatizados e que podem ser operados à distância (Silva; Oliveira; 2017). A Figura 4 destaca alguns desses benefícios à saúde gerados pelo IoT.

Figura 4 – Benefícios à saúde gerados pelo IoT



Fonte: Marques; Pitarma (2019)

Visto esses inúmeros benefícios, já existem casos concretos de uso do IoT na saúde como a empresa americana *Constant Health*, que usa celulares para avaliar a função cerebral, e a *Glooko*, também americana, que integra dispositivos médicos para acompanhar pacientes diabéticos (Maia; 2017).

Além disso, um relatório da *Grand View Research* (2023), uma organização respeitável no campo de pesquisa de mercado, revela que o mercado de IoT na área da saúde alcançou um valor impressionante de 252.1 bilhões de dólares em todo o

mundo em 2022. Com projeções indicando um crescimento ainda maior entre 2023 e 2030, o uso e confiança nas soluções de IoT estão crescendo.

À medida que os investimentos e as expectativas aumentam nesse setor, é crucial que a indústria desses aparelhos dê uma atenção redobrada na segurança da informação (SI) em seus dispositivos e soluções (De Paula, 2023).

De acordo com Pedra (2023) SI é definida como um conjunto de ações e procedimentos para proteger informações e conjuntos de dados, os preservando tanto para organizações quanto para pessoas individuais. Essas estratégias são implementadas para atingir os princípios essenciais da segurança da informação, que incluem:

- **Confidencialidade**: Garantir que apenas autorizados tenham acesso aos dados;
- **Integridade**: Manter a integridade dos dados, evitando alterações, danos ou comprometimento;
- **Disponibilidade**: Permitir que usuários legítimos tenham acesso a qualquer hora e dia;
- **Autenticidade**: Confirmar a veracidade dos dados e protege-los de falsificações;
- **Legalidade**: Garantir que todas as atividades estejam em conformidade com a lei.

Entretanto, como qualquer outro sistema, utilizar esses dispositivos IoT possui diversos desafios. Essas aplicações podem apresentar problemas de serviços de rede vulneráveis, falta de mecanismos seguros para atualização e falha na proteção e transferência não segura dos dados (OWASP, 2018).

No âmbito da saúde no Brasil, essas questões e fragilidades se tornam ainda mais alarmantes. A Lei Geral de Proteção de Dados demonstra essa preocupação ao classificar as informações relacionadas à saúde como dados sensíveis em seu artigo 5º, inciso II,

> “[...] dado pessoal sobre origem racial e étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural[...]” (Brasil, 2018, art. 5º, inciso II).

Essa questão sobre dados pessoais sensíveis já havia sido abordada na legislação brasileira através da Lei do Cadastro Positivo, também conhecida como Lei 12.414/11. Essa lei estabelece regras de acesso a bancos de dados com o objetivo de criar um histórico de crédito tanto para pessoas físicas e jurídicas. De acordo com o artigo 3º, é proibido consultar informações que não estejam diretamente relacionadas à análise de crédito.

Não é apenas a natureza confidencial dessas informações que as torna sensíveis. O modo como são utilizadas e o propósito de seu processamento desempenham um papel determinante. Dados que inicialmente são considerados comuns podem ser classificados como “sensíveis” quando tecnologias modernas estabelecem conexões entre eles (Salgado; Blank, 2020).

Apesar do país contar com mais de 40 regulamentos que visam, direta ou indiretamente, proteger a privacidade e os dados pessoais, a Lei nº 13.709/2018, conhecida como LGPD e sancionada em 14 de agosto de 2018, foi inspirada no Regulamento Geral de Proteção de Dados da Europa ou *General Data Protection Regulation* (GDPR) na forma de gerenciar as informações pessoais, tanto *online* quanto *offline*, abrangendo os setores público e privado (Brasil, 2018).

2.2 Princípios dos dados sensíveis de acordo com a LGPD.

Com o objetivo de garantir uma gestão eficiente de dados sensíveis, a legislação estabelece diretrizes claras, oferece proteções adicionais e impõe regulamentações rigorosas sobre dados pessoais. Como representado na Figura 5.

Figura 5 – Principais pontos da LGPD

Fonte: Serpro (2018)

2.2.1 Tratamento de Dados

O processamento de dados envolve uma série de ações realizadas com informações pessoais, como coleta, retenção, processamento, compartilhamento e exclusão. Esse processo deve ser finalizado quando não for mais necessário ou caso seja solicitado pelas autoridades, garantindo respeito e a integridade das informações manipuladas (Serpro,2018).

2.2.2 Direitos do Titular

É estabelecido pela Lei que o titular, pessoa à qual as informações se referem, deve ter conhecimento da finalidade da coleta de seus dados, como são tratados e quais medidas serão abordadas para garantir a integridade deles. Existem exceções para esse consentimento, como obrigação jurídica, execução de contratos e proteção da vida (Serpro,2018).

Quando um titular concorda em compartilhar suas informações, a empresa torna-se responsável pela segurança e pelo tratamento desses dados. No entanto, é crucial manter uma comunicação transparente entre essas entidades, proporcionando ao usuário o direito de acessar facilmente as informações que estão sendo utilizadas e de encerrar esse compartilhamento sem dificuldades (Serpro,2018).

2.2.3 Falhas na Segurança

No texto da legislação, é mencionado que os agentes de tratamento devem adotar medidas técnicas e administrativas de segurança para proteger os dados sensíveis, além de garantir a segurança da informação mesmo após o término do tratamento realizado.

Em casos de incidentes de segurança que comprometam o titular, é de extrema importância relatar a ocorrência à Autoridade Nacional de Proteção de Dados (ANPD).

No caso de ocorrer uma violação à lei, o artigo 52º da referida legislação trata das consequências. As punições são severas, pois os danos que a empresa pode sofrer não se limitam apenas ao aspecto financeiro, mas também afetam sua reputação devido à divulgação da infração cometida (Serpro,2018).

2.3 Trabalhos Relacionados

Esta seção apresenta alguns trabalhos relacionados ao tema em estudo.

2.3.1 Internet das Coisas (IoT): Vulnerabilidades de Segurança e Desafios

No contexto da rápida expansão da IoT, o estudo realizado por Leite (2019) analisou os desafios de segurança da informação gerados devido ao amplo uso

dessas aplicações. De acordo com o autor, esses dispositivos, que estão interconectados, são suscetíveis a vulnerabilidades que podem comprometer as informações, impactando a disponibilidade, integridade e confidencialidade dos dados.

O estudo foi dividido em três etapas: a primeira concentrou-se na identificação de vulnerabilidades, ameaças e tipos de ataques em dispositivos IoT; a segunda destacou incidentes de segurança envolvendo essas soluções, como invasões de câmeras inteligentes por *hackers*; e a terceira buscou medidas preventivas para reforçar a segurança.

Com base nas informações coletadas, foi constatado que ainda há muito a ser feito pelos fabricantes de *hardware* e desenvolvedores de *software* para resolver os diversos problemas relacionados à segurança da informação.

Alguns dos principais desafios encontrados nos dispositivos IoT incluem restrições de armazenamento, ameaças à segurança e privacidade dos dados transmitidos e armazenados, falta de padrão entre os fabricantes e brechas na segurança física dos equipamentos.

2.3.2 Saúde ocupacional e ambientes de vida melhorados com recurso à Internet

O artigo de Marques e Pitarma (2019) forneceu uma visão abrangente das tecnologias de Internet das Coisas, com foco especial na área da saúde. O objetivo é compreender como a IoT pode ser aplicada para melhorar esse setor e os serviços de assistência médica.

No trabalho, foi apresentado os conceitos fundamentais da IoT, como arquitetura e principais aplicações, especialmente em residências inteligentes e sistemas de saúde. O documento também explorou conceitos como a qualidade do serviço oferecido por esses aparelhos inteligentes e as questões de segurança relacionadas ao setor médico, incluindo análises robustas durante o planejamento e implementação, além do uso de técnicas de criptografia e mecanismos de proteção.

Foram discutidas diferentes soluções de IoT com base em diversos estudos que abordam desde o planejamento da infraestrutura até aspectos relacionados à segurança. Essas pesquisas analisaram vulnerabilidades e propuseram arquiteturas

inovadoras, como uma que se concentra na integração segura de sensores sem fio no contexto do IoT.

Os autores concluíram que privacidade, confidencialidade e segurança dos dados devem ser os pilares durante o desenvolvimento desses sistemas na área da saúde. Além disso, o documento pretende servir como um recurso valioso para pesquisas futuras nessa área.

2.3.3 Lei Geral de Proteção de Dados e segurança da informação na área da saúde

Devido à crescente utilização de tecnologia digital no campo da saúde, Salgado e Blank (2020) realizaram uma análise detalhada e explicativa da LGPD nesse contexto. A pesquisa teve o objetivo de mostrar como proteger as informações dos pacientes e garantir que as práticas de tratamento dos dados estejam em conformidade com os requisitos da lei.

Para atingir esse propósito, foi feito um detalhamento sobre o tratamento e a segurança dos dados pessoais sensíveis na área médica, como dados genéticos, condições de saúde e informações sexuais. Também, foi destacado a importância de implementar mecanismos e ferramentas eficazes de tecnologia em saúde que possam proteger esses dados, como por exemplo o uso de dispositivos IoT junto com Big Data.

Com base nos estudos os autores concluíram que é de extrema necessidade que o paciente permita o uso dos dados sensíveis para o tratamento de suas informações. Perceberam a importância de sistemas digitais seguros e em conformidade com a lei para proteger os direitos fundamentais das pessoas. Além disso, a proteção e segurança dos dados exigem uma gestão corporativa aprimorada, como o uso de melhores práticas para garantir a confiabilidade e prevenir comportamentos ilegais que possam resultar em sanções.

2.3.4 Segurança da Informação para Internet das Coisas (IoT): uma Abordagem sobre a Lei Geral de Proteção de Dados (LGPD)

Oliveira et al. (2019) abordam a importância de adaptar a SI em dispositivos IoT aos requisitos estabelecidas pela LGPD. A pesquisa lidou com o desafio de proteger informações pessoais em aplicações inteligentes, considerado suas

limitações significativas em termos de processamento, memória, largura de banda e energia.

O trabalho abordou os princípios de SI e IoT, mencionado as normas da série ISO 27000 como base para gerenciar a segurança de dados em organizações, ressaltando a importância de práticas para evitar perdas e promover melhorias. Além disso, enfatizam o papel da LGPD na proteção e transparência dos dados pessoais, destacando suas diretrizes para a coleta, armazenamento, processamento e compartilhamento das informações.

Conseguiram concluir que as soluções propostas pela pesquisa envolvem adaptar as práticas de SI para atender aos requisitos da LGPD nos dispositivos IoT. Isso inclui implementar medidas de segurança durante a coleta, transmissão e armazenamento dos dados. A coleta deve ser transparente e baseada no consentimento do usuário. A transmissão deve ser feita com o uso de VPNs e protocolos criptografados. O armazenamento dos dados deve ser protegido por criptografia que utilizam algoritmos leves.

2.3.5 Impactos da LGPD na Internet das coisas

A pesquisa realizada por Barbosa e Borin (2021) detalhou os impactos práticos da LGPD e GDPR no desenvolvimento de tecnologias IoT que trabalham com dados pessoais, por meio de uma revisão bibliográfica.

Reconheceram diversos obstáculos a serem enfrentados ao tentar ajustar as soluções baseadas em IoT para atender às exigências legais. Isso implica em obter o consentimento dos usuários de maneira clara, comunicar de forma transparente os procedimentos de tratamento de dados, assumir a responsabilidade e lidar efetivamente com possíveis falhas de segurança.

Também foram mencionadas algumas medidas importantes para garantir a segurança dos dados pessoais, como a importância de produtos e serviços com design que respeitam a privacidade, enfatizando a gestão do ciclo de vida dos dados, as limitações técnicas e os custos associados à implementação dessas soluções, efetivamente com possíveis falhas de segurança.

Os autores concluíram que a conformidade com a LGPD no contexto da IoT é um desafio complexo. Isso envolve não apenas ajustes técnicos, mas também mudar o jeito que as empresas pensam e agem com informações pessoais.

3 MÉTODO

Esta pesquisa quanto à natureza é um resumo de assunto, já que se baseia em apenas organizar uma área de conhecimento, indicando sua evolução histórica e estado de arte (Wazlawick, 2014).

Quanto aos objetivos, essa pesquisa é exploratória, na qual o autor não tem necessariamente uma hipótese ou objetivo definido em mente. Ela pode ser considerada, muitas vezes, como o primeiro estágio de um processo de pesquisa mais longo (Wazlawick, 2014).

Referente aos procedimentos técnicos, trata-se de uma pesquisa bibliográfica, documental e experimental.

A revisão bibliográfica envolve a análise de materiais já publicados, como livros, teses, recursos online e revistas, entre outros. Sua principal vantagem é permitir uma abordagem mais ampla de diversos fenômenos, além do que seria possível se pesquisasse diretamente (Gil, 2017).

De acordo com Gil (2017), as etapas da revisão bibliográfica são:

a) Escolha do tema: Ataques e vulnerabilidades nos dispositivos IoT em ambientes de saúde.

b) Revisão preliminar da literatura: Foi realizado o levantamento bibliográfico preliminar de periódicos e artigos relacionados ao assunto de pesquisa. No caso, sobre os ataques e riscos nos dispositivos IoT em ambientes de saúde - foram feitas na base de dados da CAPES, repositório da PUCGO e Google Acadêmico.

c) Formulação da pergunta de pesquisa: **Quais são os ataques e vulnerabilidades nos dispositivos IoT em ambientes de saúde?**

d) Identificação das fontes: Foram identificadas as fontes bibliográficas que forneçam informações relevantes para responder ao problema proposto, consultando dissertações, periódicos científicos, obras de referência, entre outros.

e) Análise do conteúdo: Foram examinados as informações e os dados coletados das fontes selecionadas, relacionando-os à pergunta de pesquisa e avaliando a consistência dos argumentos apresentados.

f) Fichamento: O fichamento foi realizado enfatizando os trabalhos relevantes para a pesquisa. No entanto, documentos com contribuições médias ou baixas também foram analisados para enriquecer as reflexões do autor. Essa abordagem permitiu que o TCC fosse escrito com uma base sólida.

g) Escrita do Trabalho de Conclusão de Curso.

A pesquisa documental é uma abordagem metodológica semelhante à pesquisa bibliográfica, mas se diferencia principalmente pelas fontes utilizadas. A pesquisa documental se concentra em materiais que já foram analisados anteriormente, mas podem ser reinterpretados com os objetivos específicos do estudo (Gil, 2017).

Segundo Gil (2017), a pesquisa documental também tem etapas. Entretanto, este estudo se concentrou em apenas uma delas, que é:

a) Análise e interpretação dos dados: foram analisados e interpretados os dados dos documentos da *Grand View Research* e OWASP, para assim descrever de forma objetiva, detalhada e com qualidade o conteúdo completo.

Pesquisas experimentais consistem em determinar o objeto de estudo, selecionar variáveis capazes de influenciá-lo e definir as formas de controle e de observação dos efeitos que a variável produz no objeto de estudo. (GIL, 2017). Logo, esta pesquisa experimental apresenta as seguintes etapas:

a) Formulação do problema: **Simular um ataque cibernético a um sistema de saúde conectado com IoT.**

b) Definição do plano experimental: Três máquinas virtuais ou em inglês *virtual machines* (VMs) foram configuradas com a ferramenta VMware para demonstrar diferentes aspectos de um sistema de saúde. A primeira máquina desempenhou o papel de um *hacker*. A segunda simulou o computador de um médico. Por fim, a terceira atuou como o *gateway* da rede, servindo como ponto de entrada. Além disso, foi criado um aplicativo móvel para ilustrar um *software* malicioso.

c) Determinação do ambiente: O ambiente virtual utilizado consistiu em três imagens de máquinas virtuais configuradas no VMware. A primeira, do Kali Linux, utilizou 2GB de RAM e 60GB de disco rígido. A segunda, com VyOS, alocou 2GB de RAM e 20GB de disco rígido. A terceira, uma imagem de *Windows* 10, também consumiu 2GB de RAM e 60GB de disco rígido. Essas três VMs utilizaram o adaptador de rede no modo *bridge.* Para o desenvolvimento do aplicativo móvel simulado, foi usado o ambiente de desenvolvimento integrado (IDE) *Android Studio*.

d) Análise e interpretação dos dados: A análise concentrou-se em como os invasores podem explorar as brechas em sistemas de saúde que utilizam IoT. As informações reunidas auxiliaram na compreensão mais aprofundada das falhas de segurança e na sugestão de ações para reforçar a proteção dos dados sensíveis.

4 RISCOS E AMEAÇAS À INTEGRIDADE DOS DADOS COM IOT

A grande quantidade e diversidade de dispositivos na IoT resultam em uma enorme coleta de dados dos usuários. Cada conjunto de dados representa uma possível falha para que criminosos cibernéticos possam violar a segurança. À medida que o número de dispositivos conectados aumenta, também crescem as oportunidades de invasões (Leite, 2019).

Neste contexto, a *Open Web Application Security Project* (OWASP), também conhecida como Projeto Aberto de Segurança em Aplicações Web é uma organização online que trabalha para melhorar a segurança de aplicações web. Em 2018, essa comunidade divulgou uma lista que descreve as 10 principais vulnerabilidades encontradas em dispositivos IoT, descritas a seguir.

- **Senhas fracas**: Uso de senhas que estão publicamente disponíveis ou são fáceis de adivinhar por meio de ataques de força bruta. Além disso, existe a preocupação com as falhas em *softwares* ou *firmwares*, que concedem acesso a sistemas por indivíduos não autorizados utilizando essas senhas vulneráveis.
- **Serviços de rede instáveis**: Serviços de rede não essenciais e vulneráveis ativos no dispositivo, e que podem ser acessados pela Internet, representam uma ameaça à privacidade, autenticidade e acessibilidade das informações, além de permitirem acessos remotos não autorizados.
- **Interface insegura**: Problemas de segurança em interfaces web, móveis, nuvem ou *Application Programming Interface* (API) que estão fora dos dispositivos e que podem comprometer o sistema.
- **Falta de mecanismo de atualização**: Falta de validação do firmware, envio sem criptografia, falta de mecanismos para evitar retrocessos e ausência de alertas sobre mudanças de segurança após as atualizações.
- **Uso de componentes defasados**: O uso de componentes ou bibliotecas de *software* desatualizados e possivelmente inseguros pode colocar o dispositivo em risco. Isso inclui personalizações vulneráveis do sistema operacional e a utilização de *software* ou *hardware* fornecidos por terceiros que possam estar comprometidos.
- **Proteção insuficiente de privacidade**: As informações pessoais do usuário armazenadas no dispositivo ou no ambiente em que estão

integradas podem ser utilizadas de maneira insegura, inadequada ou sem autorização.

- **Transferência e armazenamento de dados precária:** A falta de criptografia ou mecanismos de controle de acesso para informações confidenciais no ambiente, seja para dados armazenados, em trânsito ou em processamento.
- **Falta de controle de gerenciamento dos dispositivos**: A falta de medidas de segurança nos dispositivos lançados para produção envolve a gestão de ativos, a administração de atualizações, a desativação adequada, a supervisão dos sistemas e as funcionalidades de resposta.
- **Configuração padrão vulnerável**: Dispositivos possuem uma configuração padrão pouco segura ou sem a possibilidade de torná-lo mais seguro.
- **Segurança física insuficiente**: A falta de medidas de segurança adequadas para proteger fisicamente os dispositivos pode permitir que *hackers* acessem informações sensíveis, que podem ser usadas em ataques remotos futuros ou para controlar o dispositivo localmente.

A Internet das Coisas é basicamente uma fusão de várias tecnologias de rede e, como resultado, enfrenta as fragilidades e ameaças inerentes a cada uma delas. A ausência de padrões unificados torna desafiadora a tarefa de integrar e analisar os dados coletados por diferentes dispositivos (Chanal; Kakkasageri, 2020).

4.1. Principais ataques em aplicações IoT da saúde

Com essa carência de padrão para guiar desenvolvedores e fabricantes na implementação de medidas de segurança, as redes se tornam alvos frequentes para *hackers*. Esses invasores, ao identificarem dispositivos com vulnerabilidades, como *gateway* e roteadores, podem comprometer a integridade da rede por completo podendo acessar outros dispositivos (Lulka, Pratt, 2023).

De acordo com o estudo de Firouzi et al. (2018), os principais ataques desses dispositivos levando em consideração o campo da saúde são:

4.1.1 Clonagem de RFID

A clonagem de RFID é um procedimento que consiste em copiar as informações armazenadas em uma etiqueta RFID para outra etiqueta. Isso é realizado lendo as informações da etiqueta original e, em seguida, gravando essas informações na etiqueta de destino (Leite, 2019).

O processo inicia com a análise da etiqueta original usando um dispositivo de leitura de RFID. Esse dispositivo decodifica as informações armazenadas, capturando os sinais de ondas de rádio. Após a captura dessas informações, elas são armazenadas usando softwares especializados e estão prontas para serem transferidas para um novo chip ou cartão RFID em branco (Roger, 2021).

A etapa final consiste na gravação dessas informações na etiqueta de destino, tornando-a uma cópia exata do original. Com essa cópia em mãos, os criminosos podem realizar atividades que normalmente seriam reservadas ao dono original da etiqueta (Roger, 2021).

Funcionários podem utilizar cartões ou pulseiras RFID para entrar em áreas restritas, como salas cirúrgicas, laboratórios de pesquisa e estoques de medicamentos controlados (Firouzi et al, 2018).

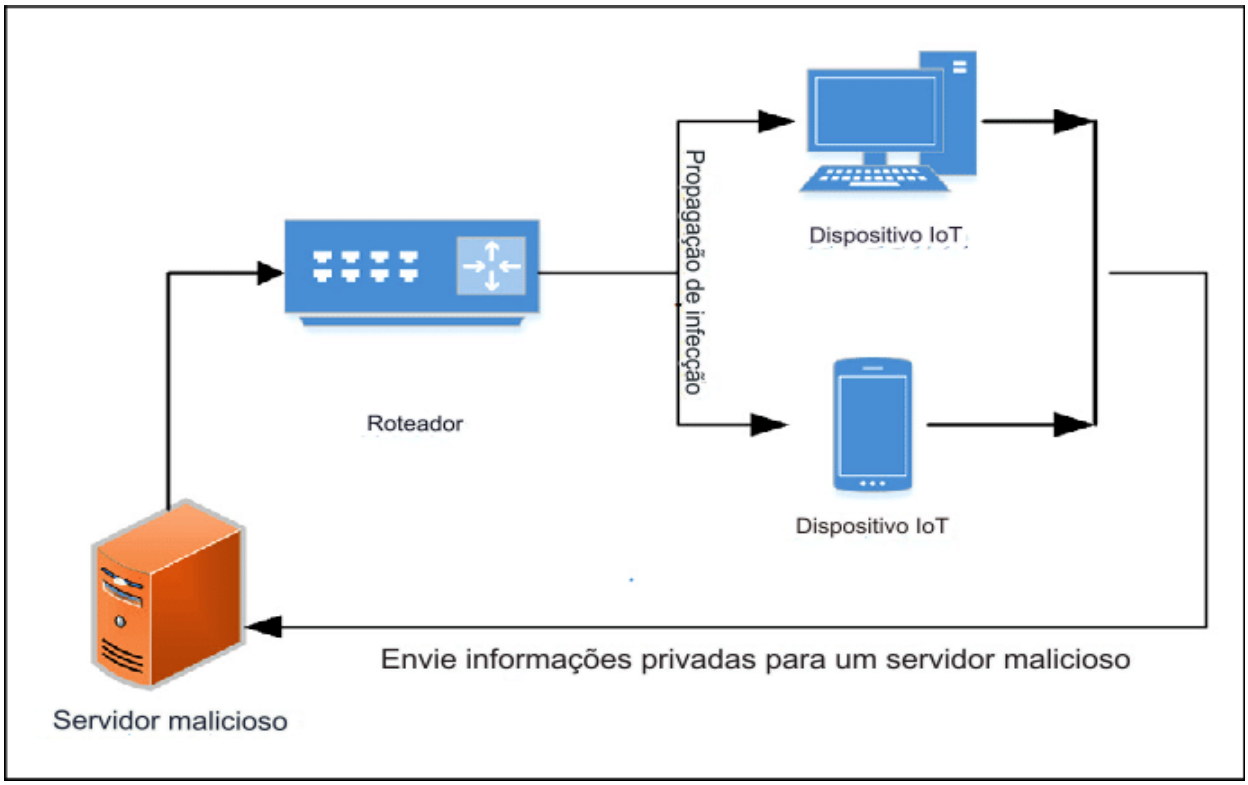
4.1.2 Spoofing

Spoofing se refere à ação de se disfarçar ou simular. É uma técnica de falsificação tecnológica que visa enganar redes ou indivíduos, permitindo que o agressor controle e envie e-mails, mensagens ou faça ligações usando o número de outras pessoas (Ribeiro, 2019).

Ataques de *spoofing* têm um impacto prejudicial tanto em redes com fio quanto sem fio. Um indivíduo mal-intencionado consegue acessar o dispositivo ao manipular as informações de identificação do usuário alvo, como endereços MAC ou IP (Khan et al, 2022).

No contexto de IoT na saúde, um invasor que consegue acessar a rede sem autorização pode espalhar *softwares* maliciosos em aparelhos conectados. Isso abrange tanto celulares quanto computadores usados por profissionais e pacientes, como ilustrado na Figura 6.

Figura 6 – Fluxo de *spoofing* em IoT



Fonte: Traduzido de Aydos, Vural e Tekerek (2020)

4.1.3 Interferência por radiofrequência em sistemas RFIDs

Um ataque de Negação de Serviço, também conhecido *como Denial of Service* (DoS), pode ser direcionado especificamente a sistemas RFID. Quando esse sistema é alvo de um ataque, o agressor intencionalmente cria e transmite sinais de ruído que são essencialmente sinais indesejados ou perturbadores (Leite, 2019).

Esses sinais são enviados pela mesma frequência de rádio usada pelo sistema RFID para suas operações normais. Como resultado, os sinais de ruído causam interferências, perturbando o processo normal de comunicação. Isso dificulta a capacidade do sistema em identificar ou rastrear objetos corretamente, comprometendo sua eficiência (Leite, 2019).

Esse ataque pode ser especialmente preocupante em ambientes hospitalares, nos quais equipamentos como máquinas de ultrassom e monitores de pacientes são equipados com RFID (Firouzi et al, 2018).

4.1.4 Injeção de mensagens

Nesse tipo de ataque, ocorre um redirecionamento no tráfego para permitir a inserção de comandos diretamente em um dispositivo específico. Isso resulta na capacidade de manipular ou controlar o fluxo de dados da rede, comprometendo assim a integridade das comunicações (Lulka, Pratt, 2023).

Quando uma resposta é gerada, o dispositivo malicioso captura esses dados e os envia de volta à fonte. Esse método cria uma falsa impressão de que a transmissão dos dados está ocorrendo como esperado, mas na realidade as informações estão sendo manipuladas ou comprometidas (Oliveira et al., 2019).

4.1.5 Negação de Serviço (Dos)

Um ataque de Negação de Serviço (DoS) ocorre quando um invasor sobrecarrega um alvo, esgotando seus recursos para impedir seu funcionamento adequado. O objetivo é desativar ou atrasar um serviço, prejudicando sua confidencialidade, integridade e disponibilidade (Hostinger, 2023).

Por outro lado, existe uma versão mais abrangente desse tipo de ataque chamada Negação Distribuída de Serviço ou em inglês *Distributed Denial of Service* (DDos). Aqui, a agressão não vem apenas de uma única fonte, mas sim de vários dispositivos diferentes. Para esse ataque o invasor segue três etapas: inicialmente, ele faz uma varredura para identificar computadores vulneráveis; em seguida, recruta esses computadores para gerar um fluxo constante de pacotes que, eventualmente, estabelece comunicação com o alvo (Džaferović et al., 2019).

Com o aumento da adoção dos dispositivos IoT, esses ataques têm se tornado mais variados, afetando várias camadas de protocolo nas redes desses dispositivos (Džaferović. et al., 2019).

Uma abordagem frequente para lidar com DoS é a redundância, que consiste em utilizar vários dispositivos interconectados, duplicando os recursos. Entretanto, em ambientes clínicos, implementar essa solução nem sempre é possível pois alguns desses dispositivos são responsáveis por sustentar funções vitais (Zeadally et al., 2019).

5 SIMULAÇÃO DE ATAQUE CIBERNÉTICO A UM AMBIENTE DE SAÚDE CONECTADO

Embora nos capítulos anteriores desse trabalho tenham sido discutidas as principais vulnerabilidades e ameaças à segurança de dados no ambiente de saúde conectado, para compreensão completa desses riscos é necessária uma abordagem mais prática e ilustrativa.

Assim, esse capítulo tem como objetivo fornecer uma representação detalhada de um ataque cibernético a um sistema de saúde conectado. O estabelecimento de saúde simulado faz uso da telemedicina e possui um aplicativo para pacientes verem resultados de exames. Dessa forma, é ilustrado as falhas e como invasores podem se aproveitar delas para comprometer os dispositivos, com foco particular na infraestrutura de telemedicina e no aplicativo de celulares.

Para montar esse cenário, foi utilizado o VMware, um programa que permite criar e gerenciar máquinas virtuais. Três VMs foram estabelecidas para simular diferentes componentes da simulação. A primeira máquina virtual rodando Kali Linux, para representar o hacker, equipada com ferramentas para testar a segurança e buscar brechas. A segunda VM operando o *Windows* 10, sendo o computador de um médico, mostrando como dispositivos individuais numa rede de saúde podem ser vulneráveis a ataques. A terceira VM tem o VyOS, um sistema operacional para redes, usado para configurar o *gateway*.

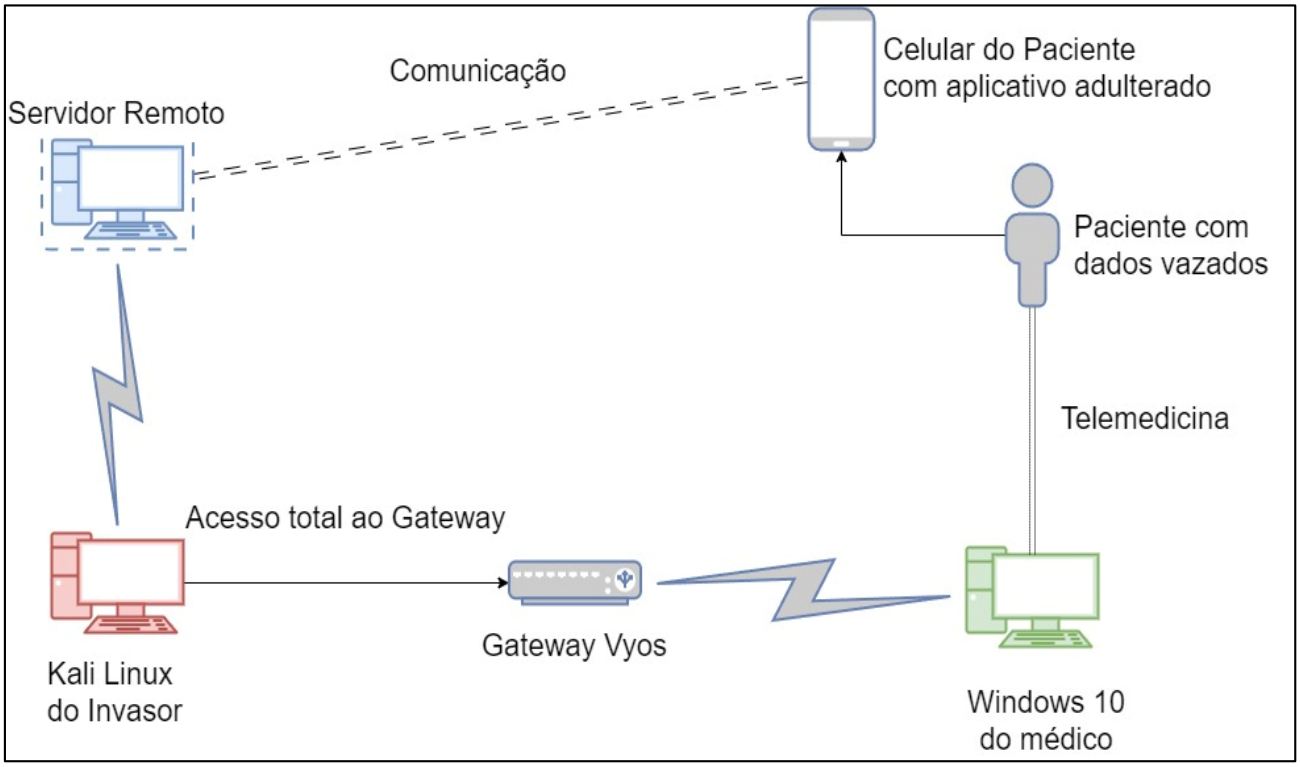
Essas três VMs foram conectadas numa rede modo *bridge*, o que permitiu que elas se comunicassem entre si, facilitando a exploração da rede pelo invasor fictício em busca de acessar os sistemas indevidamente.

Além disso, foi criado um aplicativo móvel usando o *Android Studio*, uma ferramenta de desenvolvimento bastante utilizada para criar aplicativos no sistema operacional *Android*. O programa se conecta a um servidor remoto configurado no Kali Linux para demonstrar como as comunicações entre os aplicativos dos pacientes e os servidores podem ser interceptadas e comprometidas por indivíduos mal-intencionados.

A etapa inicial dessa estrutura virtual envolveu a configuração do *gateway* no Vyos, definindo as bases para o planejamento e a execução do ataque. Em seguida, o invasor procurou por vulnerabilidades nesse dispositivo e conseguiu acessar a rede do centro de saúde sem autorização. Após ter acesso à rede, a simulação demonstrou

como o intruso poderia obter os dados sensíveis através dos dispositivos conectados. Esse fluxo é representado na Figura 7.

Figura 7 – Fluxo do cenário simulado

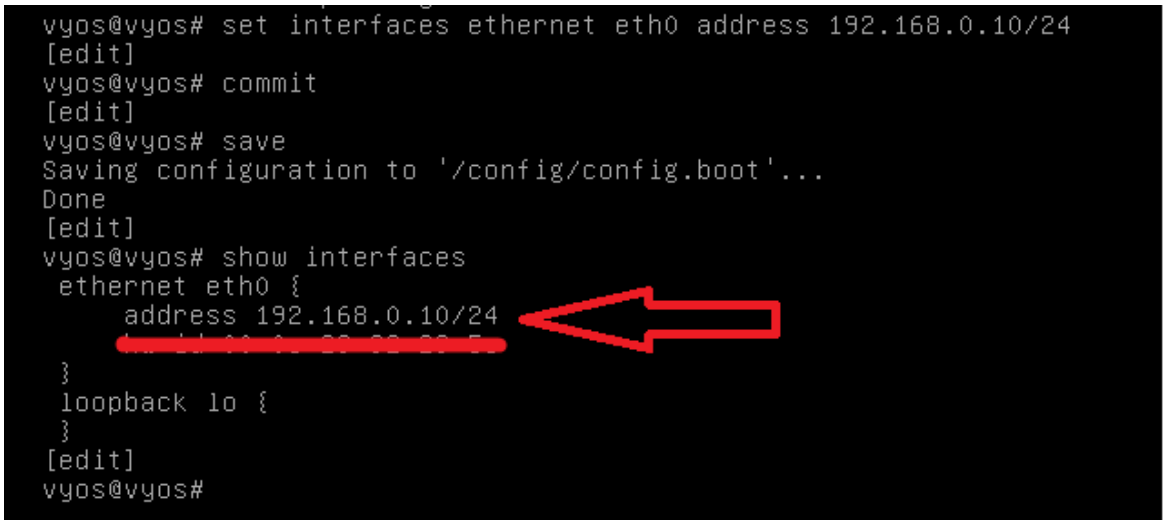


Fonte: Autoria própria (2024)

5.1. Configurando o *gateway*

Para garantir uma comunicação segura entre os dispositivos do hospital, foi instalado um *gateway* VyOS. Esse ponto de entrada não só controla o tráfego de rede, mas também permite conexões SSH seguras para a administração remota do sistema. Sua configuração inicial envolveu a definição de um endereço IP ao aparelho, um ponto crucial que estabelece a capacidade de enviar e receber tráfego tanto na rede local quanto na Internet. A Figura 8 ilustra como foi feita essa estrutura.

Figura 8 – Definição de IP ao *gateway*

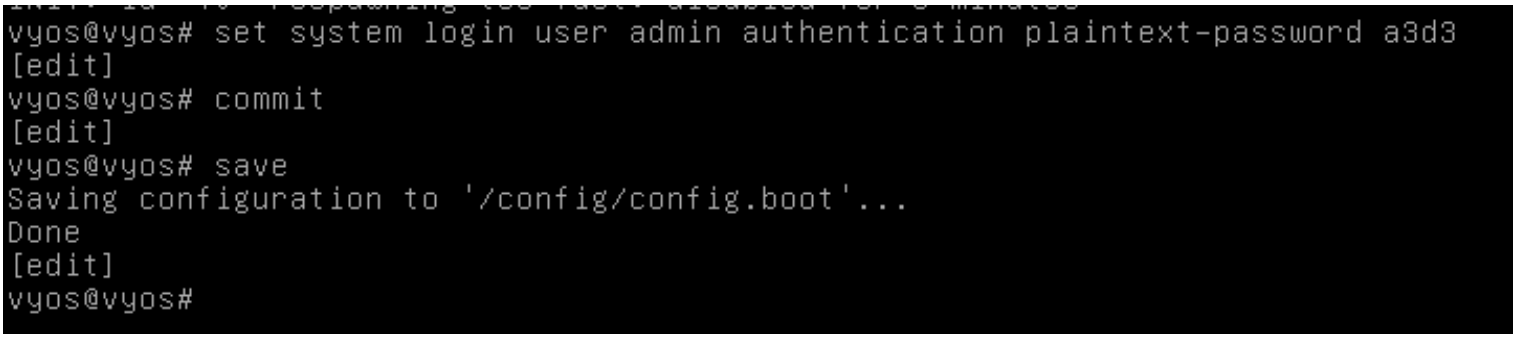


Fonte: Autoria própria (2024)

Para habilitar o serviço de SSH no VyOS, foi utilizado o comando "*set service ssh"*, que ajusta as configurações do SSH com os padrões estabelecidos, possibilitando conexões remotas seguras ao dispositivo.

Por fim, foi criado uma conta de usuário para a administração do sistema, usando o comando "*set system login user admin authentication plaintext-password a3d3"*, conforme mostrado na Figura 9. A escolha da senha "*a3d3*" foi feita para destacar um ponto crítico identificado pela OWASP: dispositivos IoT frequentemente têm senhas fracas. Essa questão enfatiza a importância de implementar políticas de senha mais robustas e considerar a utilização de uma camada adicional de autenticação.

Figura 9 – Definição de senha ao *gateway*



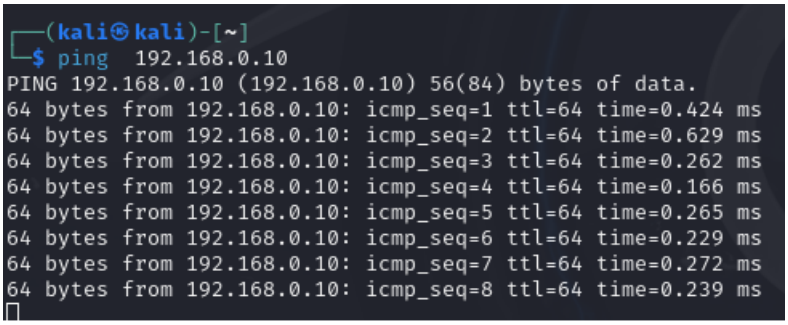
Fonte: Autoria própria (2024)

5.2. Acessando o *gateway* através de ataque DoS

O objetivo do invasor é ganhar acesso não autorizado no *gateway* para conseguir explorar a rede interna do hospital. Uma vez dentro, é possível perturbar dispositivos IoT críticos para saúde, roubar dados sensíveis ou até implantar *software* maliciosos, causando caos nos serviços de saúde.

Inicialmente foi feito um teste de rede com um simples comando de *ping*, ilustrado na Figura 10. Esse comando foi direcionado ao IP do *gateway*, com o intuito de verificar a presença do dispositivo na rede.

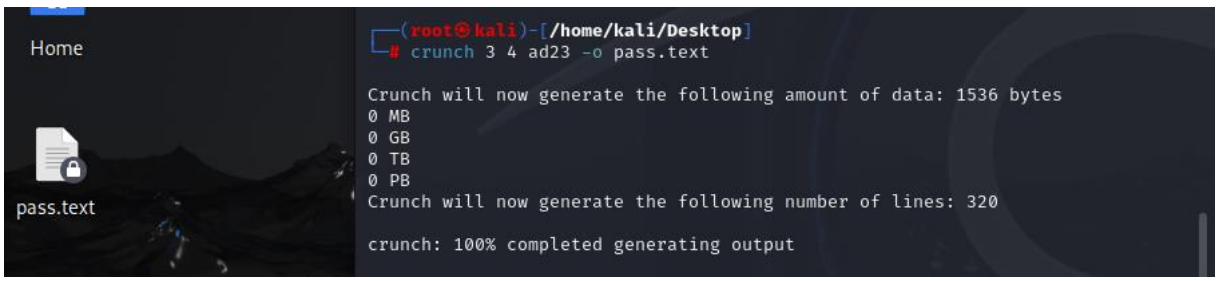
Figura 10 – Teste de *ping* ao *gateway*



Fonte: Autoria própria (2024)

Vendo a acessibilidade do dispositivo, foi desenvolvido uma lista de possíveis combinações de senhas. O invasor se limitou aos caracteres 'a', 'd', '2', e '3', para assim criar todas as sequências possíveis com tamanhos variando entre três e quatro caracteres. O comando utilizado foi "*crunch 3 4 ad23*", como representado na Figura 11, o que resultou em uma lista que começa com sequências como 'aaa', 'aad' e 'aa2' e evolui gradativamente até alcançar as combinações de quatro caracteres como '3d2a', '2a3d', entre outras.

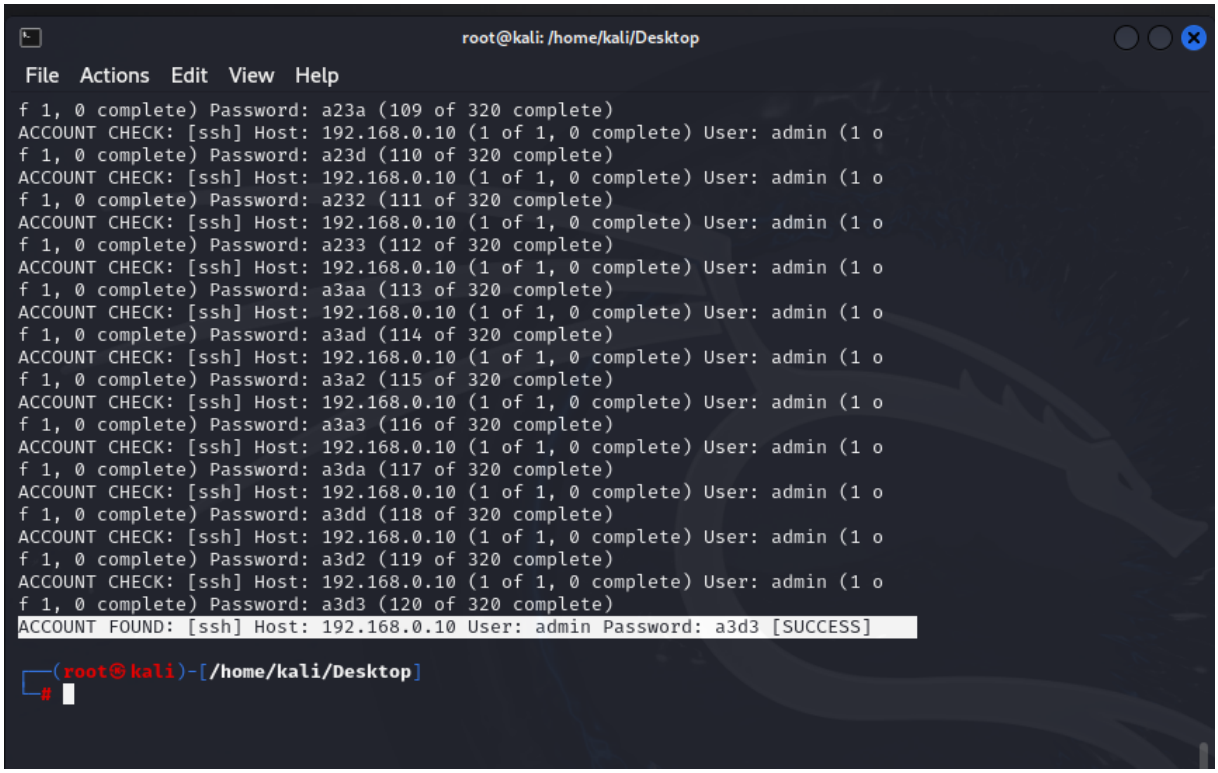
Figura 11 – Criação de lista com sequências de senhas



Fonte: Autoria própria (2024)

Com a lista feita, o invasor utilizou uma ferramenta de ataque de DoS e de força bruta chamada Medusa. Configurando o *software* para utilizar múltiplas *threads* para acelerar o processo de teste das combinações. Após inúmeras tentativas, foi revelado que a combinação ‘a3d3’ é a senha de administrador do *gateway*, como mostrado na Figura 12.

Figura 12 – Revelação da senha do *gateway*



Fonte: Autoria própria (2024)

Com acesso total ao dispositivo de rede, o invasor obteve uma posição privilegiada dentro da infraestrutura do hospital. Isso abriu a porta para ataques subsequentes a outros dispositivos conectados à mesma rede.

5.3. Ataque direcionado

Após realizar uma varredura na rede para identificar os dispositivos conectados, o invasor preparou um cavalo de troia destinado à coleta de dados e espionagem, com o objetivo de infectar esses aparelhos.

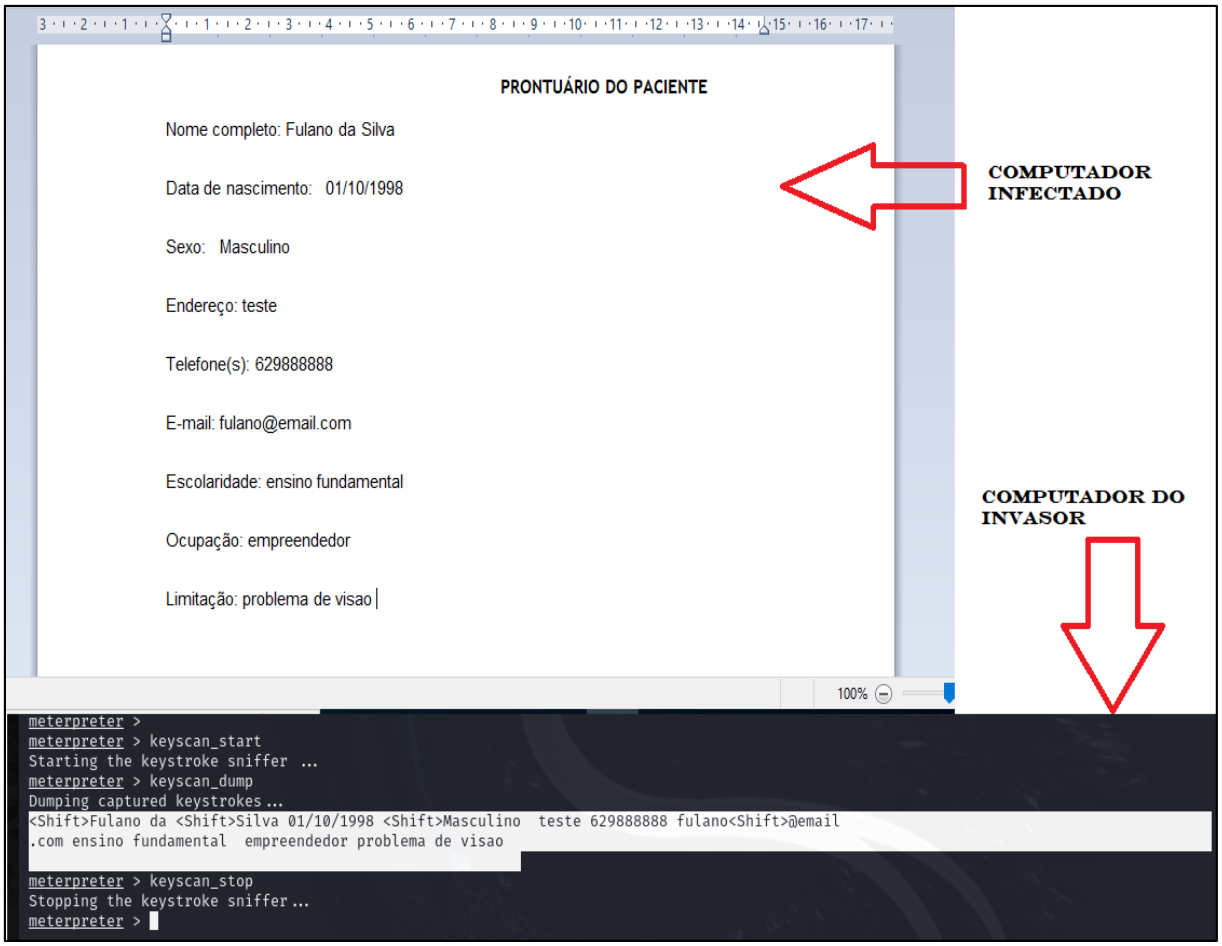
Possuindo as credenciais de administrador do *gateway*, o *hacker* tinha a capacidade de manipular o tráfego de rede conforme desejar. Isso incluía a interceptação, modificação ou redirecionamento de pacotes de dados.

Utilizando esse controle, o invasor executou uma injeção de mensagem no computador de um médico que realizava consultas remotas. Algumas das solicitações legítimas do médico foram interceptadas e substituídas pelo cavalo de troia.

Desconhecendo o perigo, o médico baixou e executou o *software* malicioso, concedendo assim acesso total ao seu dispositivo. Sem saber, ele passava a enviar informações sensíveis diretamente para o intruso.

Controlando o dispositivo, era possível capturar todas as informações digitadas durante as consultas online, desde diagnósticos até dados pessoais dos pacientes. A Figura 13 ilustra simultaneamente o médico preenchendo o prontuário eletrônico e, ao mesmo tempo, mostra o que era registrado no terminal do *hacker*, evidenciando a interceptação das informações.

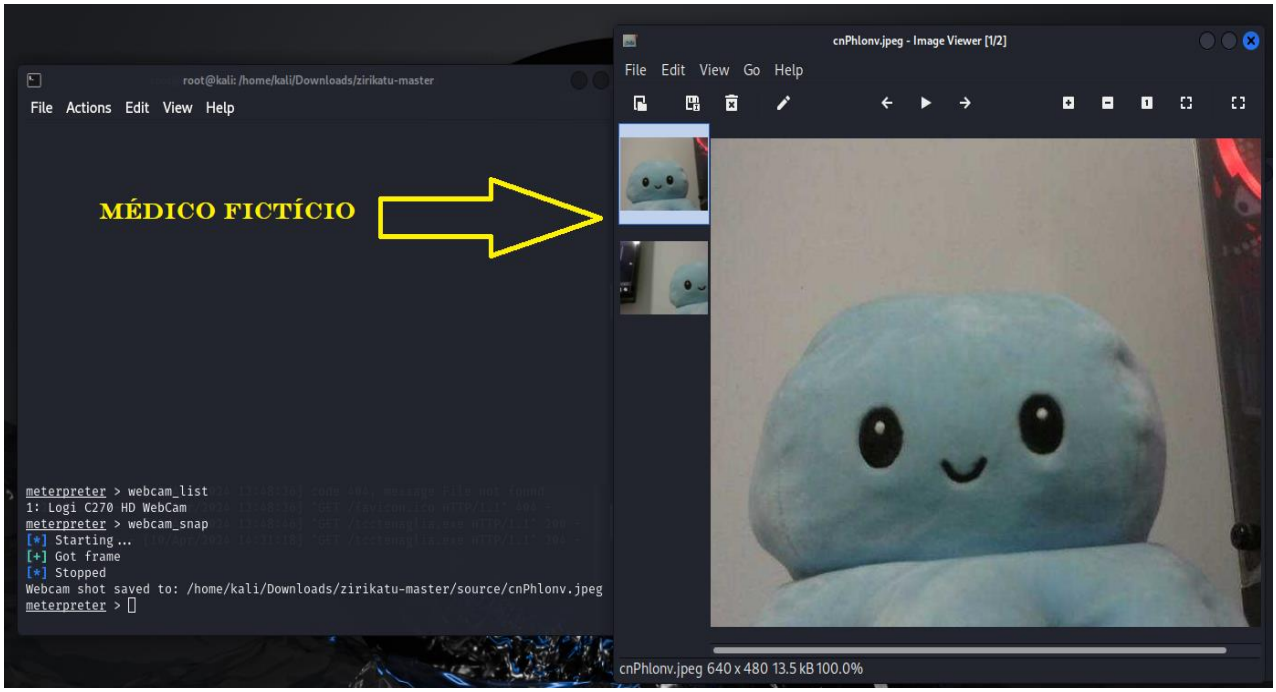
Figura 13 – Invasor coletando dados sensíveis



Fonte: Autoria própria (2024)

Além de ver as teclas digitadas, era possível acessar a webcam do médico. Esse acesso permitiu que o intruso observasse visualmente as consultas, capturando imagens sem que percebessem qualquer sinal de invasão. Essa clara violação da privacidade é exemplificada na Figura 14, que mostra a perspectiva do invasor através da webcam ativado.

Figura 14 – Capturando imagem do médico



Fonte: Autoria própria (2024)

Colocando assim, não só em risco a privacidade dos dados dos pacientes, mas o ataque também compromete a segurança dos profissionais de saúde.

5.4. Extensão ao paciente

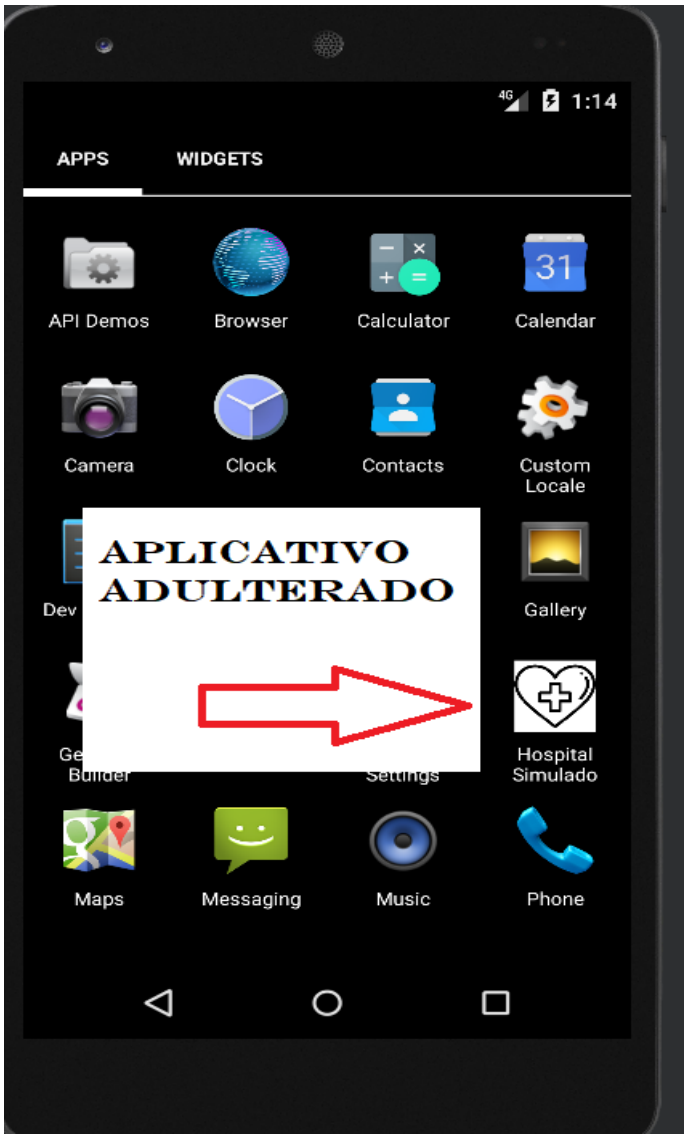
Utilizando técnicas de engenharia reversa, o invasor direcionou seus esforços para o aplicativo móvel usado pela instituição de saúde. Com o *Android Studio* ele analisou o código-fonte do aplicativo original e inseriu um código malicioso, criando uma “porta dos fundos” que se comunicava silenciosamente com um servidor remoto sob seu controle.

Com o novo código em vigor e com acesso aos dados confidenciais do paciente, o *hacker* elaborou um e-mail convincente, fazendo-se passar por uma

comunicação oficial da instituição de saúde. Na mensagem, ele alertava sobre uma suposta atualização crítica de segurança para o aplicativo, destacando a importância urgente da instalação para proteger os dados pessoais do usuário.

Interessado na aparente preocupação com sua segurança, o paciente seguiu as orientações do e-mail e baixou a “atualização de segurança". Sem desconfiar de nada, ele prosseguiu com a instalação, ilustrado na Figura 15.

Figura 15 – Aplicativo adulterado no aparelho do paciente

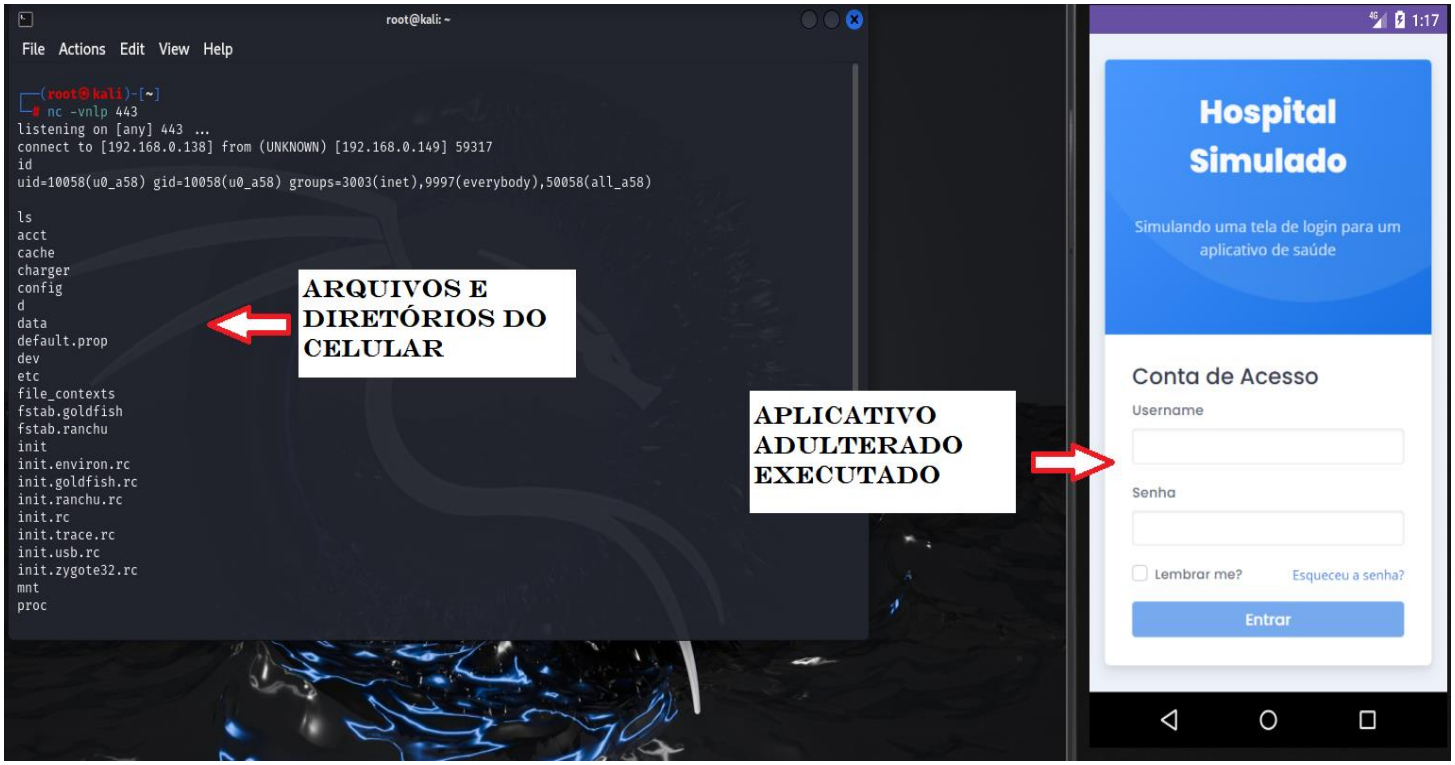


Fonte: Autoria própria (2024)

Com o aplicativo adulterado instalado e executado no celular do paciente, o invasor obteve acesso total ao dispositivo. Agora, ele podia ver não apenas os

registros médicos do paciente, mas também outras informações armazenadas no aparelho, a Figura 16 demostra o acesso do aparelho pelo servidor remoto.

Figura 16 – Acesso do aparelho do paciente pelo servidor remoto



Fonte: Autoria própria (2024)

Esse caso simulado mostrou a importância de boas medidas de segurança cibernética, especialmente em hospitais e clínicas onde as informações dos pacientes precisam ser bem protegidas. A instituição de saúde que foi atacada precisa agir rápido, avisando os pacientes que foram afetados, tirando de circulação as versões do aplicativo que foram comprometidas e melhorando suas medidas de segurança para evitar que isso aconteça de novo.

6 ESTRATÉGIAS COM IOT E LGPD PARA PROTEGER OS DADOS PESSOAIS

A obtenção de informações, como batimentos cardíacos, biometria, localização e padrões de rotina, é algo comum no contexto da IoT na saúde. Qualquer dispositivo que coleta esses tipos de dados está sujeito à LGPD (Barbosa; Borin, 2021).

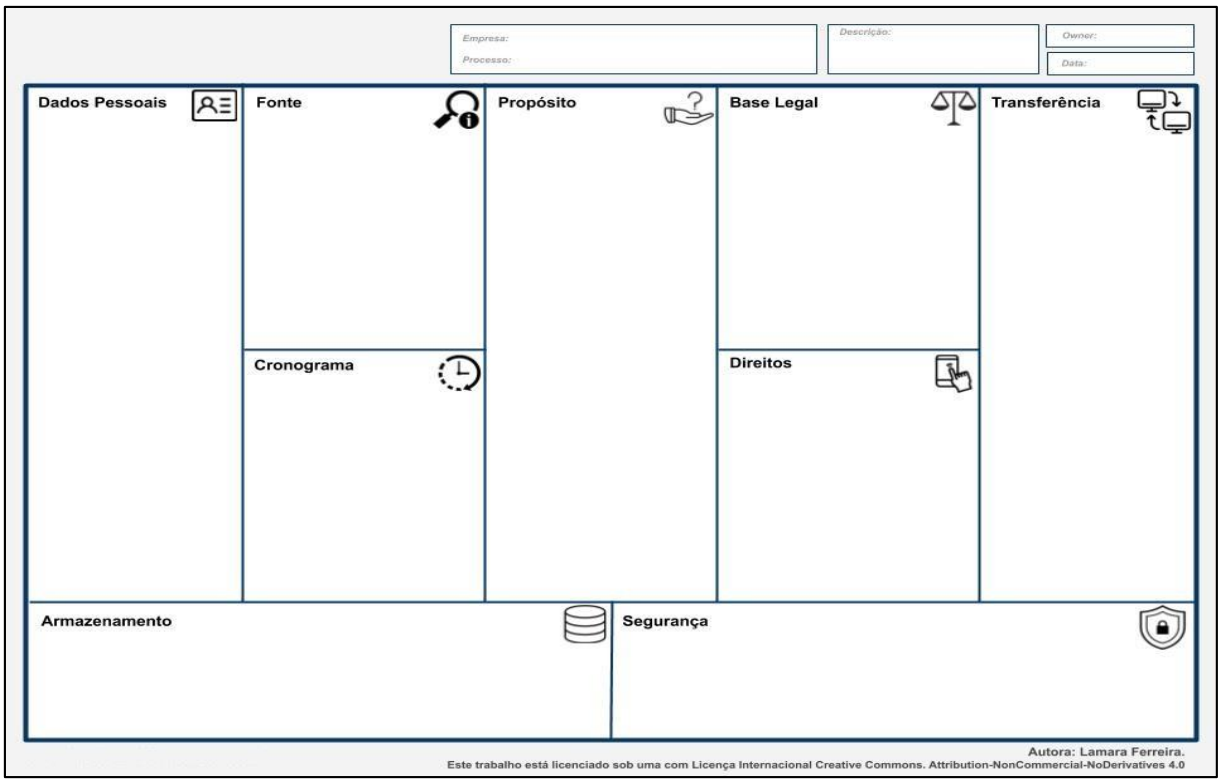
Portanto, em primeiro lugar, é fundamental que a empresa de saúde identifique e mapeie os dados que possui. Essa documentação das informações é extremamente importante quando se trata de cumprir as leis de proteção de dados. Essa documentação deve mostrar o caminho dos dados pessoais dentro da empresa, abrangendo todos os processos e etapas pelos quais eles passam.

A elaboração de um mapeamento de dados deve ser feita entre os vários setores da corporação, com apoio de especialistas técnicos e jurídicos para identificar possíveis falhas (JusBrasil, 2020). Com base no artigo da JusBrasil (2020), alguns elementos chaves que devem ser incluídos nesse mapeamento são:

- **Classificação dos titulares dos dados**: Pode ser clientes, fornecedores, colaboradores, etc;
- **Identificação dos dados coletados**: Nomes, endereços, formas de contato e documentos;
- **Local de armazenamento dos dados**: Onde os dados estão sendo armazenados;
- **Métodos de coleta de dados**: Como os dados são coletados;
- **Finalidade da coleta de dados**: Explicar o motivo da coleta de dados;
- **Definição dos colaboradores autorizados para acessar os dados**: Quem tem permissão para acessar os dados;
- **Determinação da sensibilidade dos dados**: Identificar o quão sensível é o dado;
- **Destino dos dados em caso de compartilhamento**: Para onde os dados vão se forem compartilhados;
- **Período de retenção dos dados**: Por quanto tempo os dados serão mantidos;
- **Procedimentos de exclusão de dados**: Como os dados são excluídos quando não são mais necessários.

Com as informações coletadas é possível gerar um fluxograma das informações e elaborar documentos como planilhas ou modelos disponibilizados na Internet como mostrado na Figura 17.

Figura 17 – Exemplo modelo para mapeamento de dados



Fonte: Adaptado de Leite Júnior (2020)

É essencial realizar esse procedimento, uma vez que o artigo 37º da LGPD estipula que tanto o controlador quanto o operador devem manter um registro das atividades relacionadas ao processamento de dados sensíveis (Barbosa; Borin, 2021).

A transparência também é crucial. É necessário garantir que os dispositivos IoT possuam ferramentas e opções de privacidade intuitivas, compreensíveis e fáceis de usar. É fundamental que os pacientes tenham conhecimento claro sobre quais dados estão sendo coletados e por qual motivo (Oliveira et al., 2019).

É importante criar campanhas de conscientização sobre segurança para os funcionários e pacientes. Essas iniciativas ajudam a entender os riscos associados aos IoTs e ensinam as melhores práticas de segurança. A conscientização desempenha um papel fundamental na prevenção de falhas na segurança, pois indivíduos bem-informados tendem a evitar erros que poderiam comprometer a confidencialidade e integridade dos dados (Barbosa; Borin, 2021).

Além disso, as empresas responsáveis pelo desenvolvimento desses dispositivos devem implementar mecanismos para garantir a segurança e a privacidade dos dados sensíveis, como realizar ações com base em regras e alertas, considerando endereços IP de destino, protocolos, portas e até mesmo números de identificação (Cryptoid, 2021).

A implementação de *firewalls* nos sistemas que se comunicam com os aparelhos é necessária, pois filtram o tráfego não autorizado e monitoram tentativas de acesso, estabelecendo uma defesa sólida contra invasões externas. Outro ponto importante é a de manter todos os dispositivos atualizados com as últimas correções de segurança, reduzindo vulnerabilidades que poderiam ser exploradas por invasores (Cryptoid, 2021).

Um outro ponto importante é a adoção de medidas fortes de autenticação e controle de acesso. Isso implica que o acesso aos dispositivos e aos dados deve ser cuidadosamente regulado, autorizando somente as funções e pessoas essenciais para suas respectivas operações ou manipulação (Firouzi et al, 2018).

Além de monitorar a rede em tempo real e supervisionar cada ponto de conexão em busca de problemas, como picos repentinos no tráfego, o uso de criptografia nas comunicações é uma medida crucial para garantir a segurança dos dados transmitidos (Cryptoid, 2021).

O processo de criptografia no contexto IoT, se inicia com um sensor executando uma operação de varredura para coletar dados. Esses dados podem incluir informações diretamente capturadas pelo sensor ou outras informações relevantes de dispositivos conectados na mesma rede. Após a coleta, o sensor processa os dados e os criptografa usando uma chave específica. Quando os dados criptografados são enviados pela rede, eles chegam a um servidor que decifra a mensagem seja usando a mesma chave ou uma chave diferente para então interpretar as informações recebidas e tomar decisões automatizadas (Pauferro; Paiva; Lessa, 2020).

7.CONCLUSÃO

Este projeto teve o intuito de responder a seguinte questão de pesquisa: Quais são os ataques e vulnerabilidades nos dispositivos IoT em ambientes de saúde?

O objetivo geral foi realizar uma revisão bibliográfica para identificar os ataques e vulnerabilidades nos dispositivos IoT em ambientes de saúde, bem como simular um ataque cibernético para ilustrar esses pontos fracos e sugerir estratégias que garantam a privacidade e a segurança das informações dos pacientes.

Durante o estudo, observou-se que as principais brechas identificadas na Internet das Coisas incluem senhas fracas, serviços de rede instáveis, interfaces inseguras, falta de mecanismos de atualização, uso de componentes defasados, proteção insuficiente de privacidade, transferência e armazenamento de dados precária, falta de controle de gerenciamento dos dispositivos, configuração padrão vulnerável e segurança física insuficiente.

Ataques de clonagem e interferências no RFID, injeção de mensagem, DoS, DDoS e *spoofing* são ameaças reais e frequentes nesse contexto. Esses riscos, combinados com o aumento de coleta e análise de dados pessoais, tornam o desafio da proteção ainda maior. Isso é ainda mais crítico quando se trata de dispositivos conectados à saúde, uma vez que os dados envolvidos são altamente sensíveis.

A simulação do ataque cibernético mostrou como essas fragilidades podem ser exploradas e quais são seus impactos em um ambiente de saúde conectado. Esse entendimento é fundamental para desenvolver estratégias de proteção eficazes.

Com base ainda nos estudos conclui-se que garantir a privacidade e segurança dos pacientes requer:

- Usar *firewalls* para bloquear acessos não autorizados e monitorar qualquer entrada suspeita na rede. Isso ajuda a criar uma barreira sólida contra possíveis ataques.
- Manter todos os dispositivos atualizados com as últimas correções de segurança para evitar que falhas conhecidas sejam exploradas por usuários mal-intencionados.
- Possuir sistemas fortes de autenticação e controle de acesso para garantir que só pessoas autorizadas acessem os dispositivos e dados.
- Monitorar a rede em tempo real e criptografar as comunicações ajuda a proteger a informação que circula, mantendo-a segura e privada.

- Realizar campanhas educativas aos funcionários e pacientes para ajudar a todos entender os riscos e a adotar práticas de segurança melhores.

Para continuidade desta pesquisa, sugere-se como trabalhos futuros:

- Realizar ataques RFID em um ambiente médico (simulado) e identificar as melhores estratégias para preveni-los.
- Desenvolver estudos que integrem as melhores práticas de segurança para dispositivos IoT em conformidade com a Lei Geral de Proteção de Dados.

REFERÊNCIAS:

AL-FUQAHA, Ala et al**. Internet of Things: A Survey on Enabling Technologies, Protocols and Applications**. IEEE Communications Surveys & Tutorials, 2015. Disponível em: https://ieeexplore.ieee.org/document/7123563. Acesso em: 17 set. 2023.

AYDOS, M.; VURAL, Y.; TEKEREK, A. **Assessing risks and threats with layered approach to Internet of Things security**. Measurement and Control, 2019. Disponível em: https://doi.org/10.1177/0020294019837991. Acesso em: 20 out. 2023.

AZEVEDO, Marco A. S.; OLIVEIRA, Vitor E. L. de; CARNEIRO, Tiago R. **Saúde e tecnologia: desenvolvimento de aplicativo para consulta**. 2021. Disponível em: https://ric.cps.sp.gov.br/bitstream/123456789/10141/1/sistemas_para_internet_2021_1_marco_antonio_siviero_azevedo_saude_e_tecnologia_desenvolvimento_de_aplicativo_para_consulta.pdf. Acesso em: 26 abril. 2024

BARBOSA, Alexandre Luciano; BORIN, Juliana Freitag. **Impactos da LGPD na internet das coisas**. Universidade Estadual de Campinas, Instituto De Computação, 2021.

BARNAGHI, Payam; SHETH, Amit. **The Internet of Things: The Story So Far**. IEEE - Internet of Things, 2014. Disponível em: http://iot.ieee.org/ newsletter/september-2014/theinternet-of-things-the-story-so-far.html. Acesso em: 12 set. 2023.

BATISTA DA SILVA, Eliel.; RAMALHO DE SOUZA, P. A..; NADER, Renato. **Tendências no âmbito internet das coisas: um estudo patentário**. Innovar, 2021. Disponível em: https://doi.org/10.15446/innovar.v31n81.95572. Acesso em: 12 set. 2023.

BOTELHO, M. C.; CAMARGO, E. P. do A. **A aplicação da Lei Geral de Proteção de Dados na saúde**. Revista de Direito Sanitário, 2021. Disponível em: https://www.revistas.usp.br/rdisan/article/view/168023. Acesso em: 2 set. 2023.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD)**. Diário Oficial da União, Brasília, DF, 2018. Disponível em: https:// www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 18 set. 2023.

CHANAL, Poornima; KAKKASAGERI, Mahabaleshwar. **Security and Privacy in IoT: A Survey**. Wireless Personal Communications, 2020. Disponível em: https://doi.org/10.1007/s11277-020-07649-9. Acesso em: 16 out. 2023.

CRYPTOID. **Importância da segurança dos dados em dispositivos IoT aumenta com a LGPD**. Cryptoid, 2021. Disponível em: https://cryptoid.com.br/iot-internet-das-coisas/importancia-da-seguranca-dos-dados-em-dispositivos-iot-aumenta-com-a-lgpd/. Acessado em: 25 out. 2023.

DE PAULA, Marcus Vinícius Cândido. **Segurança da informação e a internet das coisas**. Brasília: Faculdade de Tecnologia e Ciências Sociais Aplicadas – FATECS, 2023.

DŽAFEROVIĆ, E.; SOKOL, A.; ALMISREB, A. A.; MOHD NORZELI , S. **DoS and DDoS vulnerability of IoT: A review**. Sustainable Engineering and Innovation, 2019.

FACCIONI FILHO, Mauro. **Internet das coisas**. Unisul Virtual, 2016. Disponível em: https://www.researchgate.net/publication/319881659_Internet_das_Coisas_Internet_of_Things. Acesso em: 6 set. 2023.

FIROUZI, Farshad; FARAHANI, Bahar; IBRAHIM, Mohamed; CHAKRABARTY, Krishnendu. **Keynote Paper: From EDA to IoT eHealth: Promises, Challenges, and Solutions**. IEEE Communications Surveys & Tutorials, 2018. Disponível em: https://ieeexplore.ieee.org/document/8279520. Acesso em: 17 set. 2023.

GIL, Antônio Carlos. **Como Elaborar Projetos de Pesquisa**. 6. ed. São Paulo: Editora Atlas Ltda., 2017.

GONÇALVES, Vitor Hugo Pereira. **Marco Civil da Internet Comentado**. São Paulo: Atlas, 2017.

GRAND VIEW RESEARCH. **Internet of Things in Healthcare Market Size Report.** Grand View Research, 2023. Disponível em: https://www.grandviewresearch.com/industry-analysis/internet-of-things-iot-healthcare-market. Acesso em: 12 set. 2023.

HOSTINGER. **DDoS: O que é, Como funciona e Como se Proteger de Ataques Maliciosos na Internet**. Hostinger, 2023. Disponível em: https://www.hostinger.com.br/tutoriais/o-que-e-ddos-e-como-se-proteger-de-ataques. Acesso em: 20 out. 2023.

JUSBRASIL. **O que é o mapeamento de dados?**.JusBrasil, 2020. Disponível em: https://www.jusbrasil.com.br/artigos/o-que-e-o-mapeamento-de-dados/855783756. Acesso em: 5 nov. 2023.

KHAN, F. et al. **Development of a Model for Spoofing Attacks in Internet of Things**. Mathematics, 2022. Disponível em: https://doi.org/10.3390/math10193686. Acesso em: 20 out. 2023.

KINJO, Erika Midori; LIBRANTZ, André Felipe Henriques; DE SOUZA, Edson Melo; DOS SANTOS, Fábio Cosme Rodrigues. **Modelagem Bayesiana aplicada para cálculo da probabilidade de falha em Sistemas de Saúde IoT**. Revista Ibérica de Sistemas e Tecnologias de Informação, 2022. Disponível em: https://scielo.pt/pdf/rist/n47/1646-9895-rist-47-87.pdf. Acesso em: 10 set. 2023.

LEITE JÚNIOR, Nelson Corrêa. **LGPD MODEL CANVAS – MAPEAMENTO DE DADOS ÁGIL**. Ravel Tecnologia, 2020. Disponível em: https://ravel.com.br/blog/lgpd-model-canvas-mapeamento-de-dados-agil/. Acesso em: 5 nov. 2023.

LEITE, Leandro Rogério Corrêa. **Internet das Coisas (IoT): vulnerabilidades de segurança e desafios**. Faculdade de Tecnologia de Americana, Americana, 2019. Disponível em: https://ric.cps.sp.gov.br/handle/123456789/3978. Acesso em: 20 out. 2023.

LULKA, Jessica; PRATT, Mary K.. **Top 12 IoT security threats and risks to prioritize. TechTarget**, 2023. Disponível em: https://www.techtarget .com/iotagenda/tip/5-IoT-security-threats-to-prioritize. Acesso em: 20 out. 2023.

MARQUES, Gonçalo; PITARMA, Rui. **Saúde ocupacional e ambientes de vida melhorados com recurso à Internet das Coisas**. Revista RISTI, 2019. Disponível em: https://www.proquest.com/openview/841aa93ba3c3df4558018418916838ff/1?pq-origsite=gscholar&cbl=1006393. Acesso em: 12 set. 2023.

MAIA, Ubijara. **Como a IoT está mudando os hospitais e o mercado de saúde**. Instituto Information Management. Revista 81, 2017. Disponível em: https://docmanagement.com.br/03/02/2017/como-iot-esta-mudando-os-hospitais-e-o-mercado-de-saude/. Acesso em: 17 set. 2023.

MINERVA, Roberto; BIRU, Abyi; ROTONDI, Domenico. **Towards a Definition of the Internet of Things (IoT)**. SCRIBD, 2015. Disponível em: https://pt.scribd.com/doc/306069323/IEEE-IoT-Towards-Definition-Internet-of-Things-Revision1-27MAY15. Acesso em: 12 set. 2023.

MUNDO DA TI BRASIL. **Criptografia: Chaves simétricas e assimétricas**. 2017. Disponível em: https://mundodatibrasil.wordpress.com/2017/11/05/criptografia-chaves-simetrica-e-assimetrica/. Acesso em: 05 nov. 2023.

NOMAN, H. A.; ABU-SHARKH, O. M. F. **Code Injection Attacks in Wireless-Based Internet of Things (IoT): A Comprehensive Review and Practical Implementations**. Sensors, 2023. Disponível em: https://doi.org/ 10.3390/s23136067. Acesso em: 20 out. 2023.

OLIVEIRA, N. S.; GOMES, M. A.; LOPES, R.; NOBRE, J. C. **Segurança da Informação para Internet das Coisas (IoT): uma Abordagem sobre a Lei Geral de Proteção de Dados (LGPD)**. Universidade do Vale do Rio dos Sinos (UNISINOS), 2019.

OWASP. **OWASP Internet of Things**. OWASP, 2018. Disponível em: https://owasp.org/www-pdf-archive/OWASP-IoT-Top-10-2018-final.pdf. Acesso em: 25 set. 2023.

PAUFERRO, Gabriel Brogno Alcantara; PAIVA, Seila Vasti Faria de; LESSA, Nayari Marie. **IoT: conceitos de segurança de dados e criptografia**. Cogitare, 2020.

PEDRA, David. Segurança da informação: **o que é e como criar uma política para proteção de dados**. SiteWare. 2023. Disponível em: https://www.siteware.com.br/seguranca/seguranca-da-informacao/. Acesso em: 05 nov. 2023.

RIBEIRO, Felipe. **O que é spoofing? Conheça a técnica hacker utilizada contra o Ségio Moro**. Canaltech, 2019. Disponível em: https://canaltech.com.br/hacker/o-que-espoofing-conheca-a-tecnica-hacker-utilizada-contra-sergio-moro-144951/. Acesso em: 20 out. 2023.

ROGER. **É possível clonar cartões RFID? Um Guia de Segurança RFID Tudo Incluído**. WXR, 2021. Disponível em: https://www.rfidfuture.com/pt/clone- rfid-cards.html. Acesso em: 20 out. 2023.

ROSA, Claudia Marisa; SOUZA, Paulo Augusto Ramalho de; SILVA, Joaquim Manoel da. **Inovação em saúde e internet das coisas (IoT): Um panorama do desenvolvimento científico e tecnológico**. Perspectivas em Ciência da Informação, 2020. Disponível em: https://doi.org/10.1590/1981-5344/3885. Acesso em: 25 set. 2023

SALGADO LEME, R.; BLANK, M. **Lei Geral de Proteção de Dados e segurança da informação na área da saúde**. Cadernos Ibero-Americanos de Direito Sanitário, 2020. Disponível em: https://doi.org/10.17566/ciads.v9i3.690. Acesso em: 6 set. 2023.

SERVIÇO FEDERAL DE PROCESSAMENTO DE DADOS. **O que muda com a LGPD**. Serpro, 2018. Disponível em: https://www.serpro.gov.br/lgpd/menu/a-lgpd/oque-muda-com-a-lgpd. Acesso em: 18 out. 2023.

SILVA, Rogério Oliveira da; OLIVEIRA, José Lucas Sousa de. **A INTERNET DAS COISAS (IOT) COM ENFOQUE NA SAÚDE**. Tecnologia em Projeção, 2017. Disponível em: https:// revista.faculdadeprojecao.edu.br /index.php/Projecao4/ article/view/824. Acesso em: 14 out. 2023.

THAKOR, Vishal; RAZZAQUE, MOHAMMAD Abdur; KHANDAKER, Muhammad. **Lightweight Cryptography for IoT: A State-of-the-Art**. arXiv, 2020. Disponível em: https://doi.org/10.48550/arXiv.2006.13813. Acessado em: 12 set. 2023

WAZLAWICK, R. S. **Metodologia de Pesquisa para Ciência da Computação**. 2º ed. Rio de Janeiro: Elsevier, 2014. cap.4, p. 21 – 26.

ZEADALLY, S.; SIDDIQUI, F.; BAIG, Z.; Ibrahim, A. **Smart health care challenges and potential solutions using internet of things (IoT) and big data analytics**. PSU Research Review, 2019. Disponível em: https://www.emerald.com/ insight/content/doi/10.1108/PRR-08-2019-0027/full/html. Acesso em: 20 out. 2023

PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
GABINETE DO REITOR

Av. Universitária, 1069 ● Setor Universitário
Caixa Postal 86 ● CEP 74605-010
Goiânia ● Goiás ● Brasil
Fone: (62) 3946.1000
www.pucgoias.edu.br ● reitoria@pucgoias.edu.br

RESOLUÇÃO n° 038/2020 – CEPE

ANEXO I

APÊNDICE ao TCC

Termo de autorização de publicação de produção acadêmica

O estudante Matheus Rodrigues Tenaglia do Curso de Ciência da Computação, matrícula: 20191002800640, telefone: 62 985524863, e-mail: matheus12gyn@gmail.com, na qualidade de titular dos direitos autorais, em consonância com a Lei nº 9.610/98 (Lei dos Direitos do Autor), autoriza a Pontifícia Universidade Católica de Goiás (PUC Goiás) a disponibilizar o Trabalho de Conclusão de Curso intitulado SIMULAÇÃO DE ATAQUES CIBERNÉTICOS NOS DISPOSITIVOS IOT EM AMBIENTES DE SAÚDE, gratuitamente, sem ressarcimento dos direitos autorais, por 5 (cinco) anos, conforme permissões do documento, em meio eletrônico, na rede mundial de computadores, no formato especificado (Texto(PDF); Imagem (GIF ou JPEG); Som (WAVE, MPEG, AIFF, SND); Vídeo (MPEG, MWV, AVI, QT); outros, específicos da área; para fins de leitura e/ou impressão pela internet, a título de divulgação da produção científica gerada nos cursos de graduação da PUC Goiás.

Goiânia, 28 de MAIO DE 2024.

Assinatura do autor: _____ gov.br Documento assinado digitalmente MATHEUS RODRIGUES TENAGLIA Data: 19/06/2024 20:33:07-0300 Verifique em https://validar.iti.gov.br _____

Nome completo do autor: Matheus Rodrigues Tenaglia_____

Assinatura do professor–orientador: ___ gov.br Documento assinado digitalmente SOLANGE DA SILVA Data: 21/06/2024 16:23:50-0300 Verifique em https://validar.iti.gov.br __

Nome completo do professor-orientador: __ SOLANGE DA SILVA _____