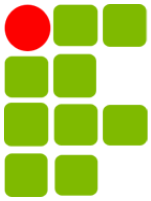


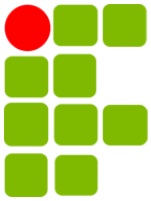
Instituto Federal de Educação, Ciência e Tecnologia da Paraíba
Campus Campina Grande
Coordenação do Curso Superior de Tecnologia em Telemática

MÉTODOS E TÉCNICAS DE SEGURANÇA PARA DISPOSITIVOS IOT: UMA REVISÃO SISTEMÁTICA DA LITERATURA

ALEX RODRIGUES ARAUJO

Orientador: ANDERSON FABIANO BATISTA FERREIRA DA COSTA

Campina Grande, Dezembro 2023



Instituto Federal de Educação, Ciência e Tecnologia da Paraíba
Campus Campina Grande
Coordenação do Cursos Superior de Tecnologia em Telemática

MÉTODOS E TÉCNICAS DE SEGURANÇA PARA DISPOSITIVOS IOT: UMA REVISÃO SISTEMÁTICA DA LITERATURA

ALEX RODRIGUES ARAUJO

Monografia apresentada à Coordenação do Curso Superior de Tecnologia em Telemática do IFPB - Campus Campina Grande, como requisito parcial para conclusão do curso Superior de Tecnologia em Telemática.

Orientador: ANDERSON FABIANO BATISTA FERREIRA DA COSTA

Campina Grande, Dezembro de 2023

A658m Araujo, Alex Rodrigues.
Métodos e técnicas de segurança para dispositivos iot: uma revisão sistemática da literatura / Alex Rodrigues Araujo. - Campina Grande, 2023.
43 f. : il.

Trabalho de Conclusão de Curso (Curso Superior de Tecnologia em Telemática) - Instituto Federal da Paraíba, 2023.
Orientador: Prof. Anderson Fabiano Batista Ferreira da Costa

1. Internet das coisas - IoT - segurança 2. Internet - segurança e privacidade 3. IoT - vulnerabilidades I. Costa, Anderson Fabiano Batista Ferreira da II. Título.

CDU 004.738

MÉTODOS E TÉCNICAS DE SEGURANÇA PARA DISPOSITIVOS IOT: UMA REVISÃO SISTEMÁTICA DA LITERATURA

ALEX RODRIGUES ARAUJO

Documento assinado digitalmente
gov.br
ANDERSON FABIANO BATISTA FERREIRA DA CO
Data: 25/01/2024 11:05:28-0300
Verifique em https://validar.iti.gov.br

Orientador

Documento assinado digitalmente
gov.br
PETRONIO CARLOS BEZERRA
Data: 25/01/2024 20:56:44-0300
Verifique em https://validar.iti.gov.br

Membro da Banca

Documento assinado digitalmente
gov.br
IANA DAYA CAVALCANTE FACUNDO PASSOS
Data: 26/01/2024 09:43:41-0300
Verifique em https://validar.iti.gov.br

Membro da Banca

Campina Grande, Paraíba, Brasil
Dezembro/2023

Dedicatória

Dedico este trabalho aos meus pais, pela constante inspiração e apoio incondicional ao longo da jornada acadêmica. Ao meu orientador Anderson, pela orientação valiosa, paciência e incentivo. A todos que, de alguma forma, contribuíram para a realização deste trabalho, meu sincero agradecimento.

"A verdadeira motivação vem de realização, desenvolvimento pessoal, satisfação no trabalho e reconhecimento."

Frederick Herzberg

Agradecimentos

Agradeço à minha família, em especial ao meu pai, **José Ari**, cujo apoio foi essencial ao longo desta jornada acadêmica. Sua presença constante e incentivo foram fontes de inspiração para superar desafios e alcançar este marco.

Aos dedicados professores do curso superior em telemática, que compartilharam conhecimento, desafios e inspiração. Suas aulas foram fundamentais para minha formação e para a compreensão mais profunda do vasto campo da telemática ao longo desses 3 anos e meio.

À professora **Iana Daya**, minha sincera gratidão pela sua ajuda incansável e pela paciência demonstrada em cada momento em que busquei ajuda.

Ao professor **David Candeia**, expresso minha profunda gratidão pela coorientação, fundamental nas fases iniciais deste trabalho. Seu valioso feedback desempenhou um papel crucial na elaboração e aprimoramento deste estudo.

Ao meu orientador, **Anderson Fabiano**, expresso minha sincera admiração e gratidão. Sua ajuda e comprometimento foram fundamentais para a concretização deste trabalho.

E, por último, gostaria de expressar meu sincero agradecimento ao professor **Katyusco Santos**, cujo papel foi fundamental no início deste projeto. Seus valiosos ensinamentos desempenharam um papel crucial na disciplina de projeto em telemática, contribuindo significativamente para o desenvolvimento deste trabalho.

Resumo

O propósito desta revisão sistemática da literatura foi identificar os principais elementos relacionados à segurança na Internet das Coisas (IoT), com a finalidade de identificar lacunas existentes e explorar soluções propostas como meios de mitigar eventuais problemas de segurança. O método empregado nesta revisão envolveu uma extensa busca na literatura acadêmica, por meio de bases de dados científicas e indexadores relevantes. Foram selecionados estudos que abordaram diretamente a segurança na IoT e que se enquadraram nos critérios de inclusão pré-definidos. A análise dos artigos selecionados foi realizada de forma sistemática, buscando extrair informações relevantes sobre protocolos de segurança, avaliação de vulnerabilidades, aprendizado de máquina, monitoramento de segurança, proteção de privacidade e detecção de intrusões.

Após leitura dos principais artigos que tratam sobre o tema proposto, os resultados obtidos revelaram uma diversidade de abordagens e soluções propostas para fortalecer a segurança na IoT. Foram identificados protocolos de segurança, como criptografia, autenticação e controle de acesso, que visam proteger as comunicações e os dados transmitidos entre dispositivos IoT. Além disso, técnicas de aprendizado de máquina foram exploradas para detecção de malware, intrusões e ataques de negação de serviço. O monitoramento contínuo do estado de segurança e a proteção da privacidade também foram abordados como aspectos fundamentais. Por fim, a detecção de intrusões mostrou-se como uma solução importante para identificar atividades suspeitas e mitigar ameaças.

Ao final desta revisão, baseada nos resultados alcançados, pode-se concluir que a segurança no âmbito da IoT representa um campo de pesquisa em constante evolução, repleto de desafios e oportunidades significativas. A implementação de protocolos de segurança adequados, juntamente com a avaliação sistemática de vulnerabilidades, a aplicação de técnicas de aprendizado de máquina, a adoção de monitoramento contínuo, a garantia da privacidade e a detecção de intrusões são elementos essenciais para assegurar a integridade dos dispositivos e sistemas relacionados à IoT.

Palavras-chave: Internet das Coisas, Segurança da IoT, Revisão Sistemática, Vulnerabilidades, Monitoramento de Segurança, Proteção de Privacidade, Detecção de Intrusões.

Abstract

This systematic literature review aims to identify key elements related to Internet of Things (IoT) security, with the goal of pinpointing existing gaps and exploring proposed solutions to mitigate potential security issues. The methodology employed in this review involved an extensive search in academic literature through relevant scientific databases and indexers. Studies directly addressing IoT security and meeting predefined inclusion criteria were selected. The analysis of selected articles was conducted systematically, aiming to extract relevant information on security protocols, vulnerability assessment, machine learning, security monitoring, privacy protection, and intrusion detection.

After reviewing key articles on the proposed topic, the obtained results revealed a diversity of approaches and proposed solutions to strengthen IoT security. Security protocols such as encryption, authentication, and access control were identified to safeguard communications and data transmitted between IoT devices. Additionally, machine learning techniques were explored for malware detection, intrusion detection, and denial-of-service attacks. Continuous security monitoring and privacy protection were also addressed as fundamental aspects. Finally, intrusion detection emerged as an important solution to identify suspicious activities and mitigate threats.

Based on the achieved results, it can be concluded that security in the realm of IoT represents a continuously evolving field of research, filled with challenges and significant opportunities. The implementation of appropriate security protocols, coupled with systematic vulnerability assessment, the application of machine learning techniques, continuous monitoring, ensuring privacy, and intrusion detection are essential elements to ensure the integrity of devices and systems related to IoT.

Keywords: Internet of Things, IoT Security, Systematic Review, Vulnerabilities, Security Monitoring, Privacy Protection, Intrusion Detection.

Lista de Siglas

ECC Criptografia de Curva Elíptica

GDPR Regulamento Geral de Proteção de Dados

IA Inteligência Artificial

IoHT Internet das Coisas para Saúde

IoT Internet das Coisas

IP Internet Protocol

LGPD Lei Geral de Proteção de Dados

ML Machine Learning

PC Computador Pessoal

RIM Métrica de Integridade de Referência

RSL Revisão Sistemática da Literatura

SDN Software Defined Network

SI Segurança da Informação

SSH Secure Shell

TCC Trabalho de Conclusão de Curso

TI Tecnologia da Informação

UIT União Internacional de Telecomunicações

UE União Europeia

Sumário

Lista de Siglas **ix**

1 Introdução **1**
1.1 Justificativa e Relevância do Trabalho 1
1.2 Objetivos 2
1.2.1 Objetivo Geral 2
1.2.2 Objetivos Específicos 2
1.3 Metodologia 2
1.4 Organização do Documento 3

2 Fundamentação Teórica **4**
2.1 Internet-of-Things: Conceitos Fundamentais 4
2.2 Cibersegurança: Fundamentos e Características 6
2.3 Desafios na Segurança da Internet das Coisas 7

3 Metodologia **8**
3.1 Procedimento metodológico 8
3.2 Formulação da questão a ser respondida 8
3.3 Definição dos termos de busca 8
3.4 Localização dos estudos 9
3.5 Protocolos de inclusão e exclusão de materiais 10
3.5.1 Finalidade dos protocolos 10
3.6 Critérios de Inclusão 10
3.7 Critérios de Exclusão 10
3.8 Triagem de seleção dos artigos 11

4 Resultados Obtidos **12**
4.1 Análise dos Dados Coletados 12
4.1.1 Número de Artigos Aceitos e Recusados em Cada Base de Dados . . . 13
4.1.2 Análise da Fase de Exclusão dos Artigos 13
4.1.3 Análise dos Artigos Selecionados na Segunda Etapa da RSL 14
4.2 Exploração Bibliográfica 15

4.3 Principais Tendências em Segurança para Dispositivos IoT 19
4.3.1 Blockchain 20
4.3.2 Machine learning 20
4.3.3 Autenticação 21
4.3.4 Criptografia 22
4.3.5 Inteligência Artificial (IA) 23
4.3.6 Controle de Acesso 24
4.3.7 Monitoramentos de Segurança e Detecção de Intrusão 25
4.3.8 Regulamentação para Proteção de Dados e Privacidade 26

5 Considerações Finais **28**

Referências Bibliográficas **30**

Capítulo 1

Introdução

1.1 Justificativa e Relevância do Trabalho

A rápida expansão da Internet das Coisas (IoT) nos últimos anos resultou em avanços significativos em várias áreas, como computação em névoa, cidades inteligentes e Indústria 4.0. Esses desenvolvimentos resultaram em um aumento substancial no processamento de dados sensíveis em diferentes setores, exigindo a implementação de medidas robustas de segurança cibernética para proteger as redes de computadores e os dispositivos conectados (Singh et al., 2020). Com o crescimento exponencial da quantidade de dados gerados por dispositivos IoT, a autenticação, segurança e privacidade emergem como preocupações críticas a serem abordadas. Consequentemente, a aplicação de métodos avançados de inteligência artificial (IA) tem ganhado destaque como uma abordagem eficaz para a detecção e prevenção de ataques cibernéticos nos dispositivos inteligentes de IoT.

Entretanto o rápido crescimento dessa tecnologia traz consigo vários desafios devido à proliferação cada vez mais evidente da Internet das Coisas, as inseguranças acerca de sua segurança têm se tornado amplamente reconhecidas na atualidade. Historicamente, os objetivos de segurança no âmbito da Tecnologia da Informação (TI) se preocupavam principalmente pela garantia da confidencialidade, integridade e responsabilidade dos sistemas e das comunicações. Contudo, essas abordagens convencionais demonstram limitações consideráveis quando aplicadas aos dispositivos IoT, devido, por exemplo, à sua capacidade de processamento muitas vezes insuficiente para tarefas mais prolongadas. Além disso, questões relacionadas à escalabilidade têm surgido devido à vasta interconexão de dispositivos dentro dos dispositivos da IoT.

A complexidade inerente à natureza distribuída da IoT, onde múltiplas entidades heterogêneas em diferentes contextos interagem, acentua ainda mais a necessidade de implementar métodos e técnicas de segurança eficazes, interoperáveis e escaláveis para proteger a integridade e a confidencialidade das operações em toda a rede interconectada. A compreensão aprofundada das peculiaridades e desafios da segurança na IoT é crucial para o desenvolvimento de estratégias abrangentes e robustas de segurança que atendam às exigências dessa

infraestrutura em constante expansão (Roman et al., 2013).

A segurança da IoT revela-se de grande importância no contexto das aplicações exemplificadas anteriormente, uma vez que a ausência de modelos de segurança apropriados para a IoT pode comprometer a plena aceitação por parte dos usuários. Desta forma, o estudo sobre os métodos e as técnicas usadas para garantir a segurança dos dispositivos inteligentes se faz crucial para se propor soluções inteligentes para a crescente demanda desses dispositivos juntamente com os desafios gerados.

Esta revisão sistemática da literatura tem como objetivo discutir os métodos e técnicas de segurança disponíveis para dispositivos IoT, abordando os principais desafios enfrentados pela IoT em relação à segurança e privacidade. Será fornecida uma visão geral das técnicas e métodos de segurança existentes para proteger dispositivos IoT, com o intuito de contribuir para o avanço do conhecimento nessa área e para a promoção de um ambiente mais seguro e confiável para a IoT.

1.2 Objetivos

1.2.1 Objetivo Geral

Realizar uma revisão sistemática abrangente da literatura existente sobre métodos e técnicas de segurança para dispositivos de Internet das Coisas, com o objetivo de identificar os principais desafios de segurança, as práticas recomendadas, e tendências emergentes nesse campo.

1.2.2 Objetivos Específicos

Abordar as tendências emergentes em segurança de IoT, incluindo inovações tecnológicas recentes e abordagens de segurança inovadoras, com o objetivo de prever o desenvolvimento futuro nesse campo.

Avaliar os métodos e técnicas de segurança existentes utilizados para proteger os dispositivos IoT, destacando suas vantagens, limitações e casos de uso mais adequados.

1.3 Metodologia

Com o propósito de conduzir a presente investigação, o autor optou pela realização de uma Revisão Sistemática da Literatura (RSL). Tal escolha fundamentou-se na elevada robustez metodológica desse tipo de estudo, bem como na possibilidade de especificação e reprodutibilidade dos métodos de seleção dos artigos.

Uma Revisão Sistemática da Literatura é um método de pesquisa que busca sintetizar o conhecimento existente em uma determinada área, de forma sistemática e transparente. Segundo Kitchenham et al. (2009), a importância da RSL está no fato de que ela permite

identificar e avaliar a qualidade dos estudos relevantes, além de fornecer uma síntese dos resultados encontrados, o que pode ajudar a orientar a tomada de decisão na área de estudo.

O objetivo da RSL é fornecer uma visão geral abrangente e objetiva do estado atual do conhecimento em um campo específico, permitindo que os pesquisadores identifiquem lacunas na pesquisa existente e áreas que precisam de mais investigação. A RSL é especialmente útil em áreas onde há um grande volume de pesquisa publicada, pois ajuda a identificar estudos que apresentam resultados inconsistentes ou conflitantes. A realização de uma RSL pode ajudar a identificar as melhores práticas e as áreas que necessitam de maior atenção por parte dos pesquisadores e profissionais da área.

1.4 Organização do Documento

Capítulo 1: Explicação da relevância do tema e os objetivos traçados para o desenvolvimento dessa revisão sistemática da literatura.
Capítulo 2: Apresenta uma discussão sobre os conceitos básicos de Internet da Coisas, cibersegurança e os desafios da segurança nos dispositivos de IoT.
Capítulo 3: Neste capítulo será tratado o aprofundamento da metodologia usada juntos com todos os protocolos de pesquisa usadas nessa revisão.
Capítulo 4: Apresentação dos resultados obtidos na literatura juntamente com discussões sobre os métodos e as técnicas usados para mitigar os problemas de segurança nos dispositivos IoT.
Capítulo 5: Apresentação das considerações finais abordando as principais descobertas e conclusões obtidas durante a revisão sistemática da literatura sobre métodos e técnicas de segurança para dispositivos IoT.

Capítulo 2

Fundamentação Teórica

2.1 Internet-of-Things: Conceitos Fundamentais

Conforme relatado por Bendavid et al. (2018), a definição da Internet das Coisas pela União Internacional de Telecomunicações (UIT) é de uma infraestrutura global que viabiliza a oferta de serviços avançados através da interconexão de objetos físicos e virtuais, baseada em tecnologias de informação e comunicação interconectáveis, tanto existentes quanto em evolução. A IoT, enquanto um novo paradigma tecnológico que busca permitir a conexão de qualquer coisa e pessoa a qualquer momento e em qualquer lugar, está se materializando com o surgimento de aplicativos habilitados pela IoT, os quais abrem diversas oportunidades de negócios e dão origem a novos modelos de negócios.

A Internet das Coisas emergiu como um campo de rápido crescimento, com uma vasta gama de aplicações que vão desde veículos autônomos até microrredes e drones em sistemas de vigilância e cidades inteligentes (Gubbi et al., 2013). Embora esses sistemas ofereçam inúmeras vantagens em termos de eficiência e funcionalidade, a segurança da IoT tem se revelado uma preocupação crucial, dada a interconexão complexa entre dispositivos e o ambiente circundante. A ausência de uma consideração adequada da segurança desde as fases iniciais do desenvolvimento tem exposto muitos sistemas de IoT a riscos substanciais (Gubbi et al., 2013).

De acordo com Bello e Zeadally (2019) a internet das coisas representa um ecossistema tecnológico em rápida evolução, caracterizado pela interconexão de dispositivos inteligentes e redes que trabalham em conjunto para oferecer serviços avançados em diversos setores, como conservação de energia, saúde, transporte e vida urbana. À medida que o conceito de IoT continua a se expandir, novos requisitos e demandas do usuário têm impulsionado o surgimento de novos domínios de aplicação, cada um buscando oferecer serviços inteligentes que aprimorem a qualidade de vida (Bello & Zeadally, 2019). Embora os focos específicos possam variar entre diferentes domínios de aplicação, todos compartilham o objetivo comum de aprimorar as atividades diárias por meio da prestação eficiente de serviços inteligentes (Bello & Zeadally, 2019).

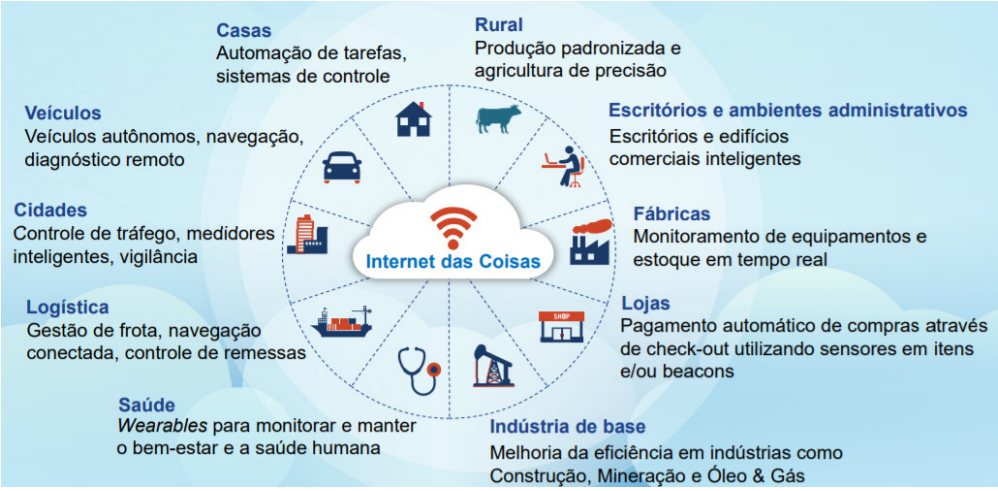
Essa rápida expansão alinhada com uma constante evolução da Internet das Coisas, tem impulsionado uma gama diversificada de domínios de aplicação, cada um com sua própria estrutura, escala e requisitos específicos. Conforme observado por Gubbi et al. (2013), essas aplicações podem ser classificadas com base em fatores como a disponibilidade de rede, cobertura, escala, heterogeneidade, repetibilidade, envolvimento do usuário e impacto. A categorização dessas aplicações abrange quatro domínios principais, incluindo (1) Pessoal e Residencial; (2) Empresarial; (3) Utilitários; e (4) Móvel. A interseção desses domínios frequentemente impulsiona a geração de dados e informações que são compartilhadas entre os diversos atores, oferecendo oportunidades significativas de inovação e colaboração interdisciplinar.

Dentro do domínio Pessoal e Residencial, a IoT desempenha um papel crucial no desenvolvimento de soluções para cuidados de saúde contínuos e monitoramento remoto, como mencionado por Gubbi et al. (2013). A integração de sensores e dispositivos vestíveis coleta dados fisiológicos dos indivíduos, que podem ser posteriormente analisados para fornecer percepções valiosos sobre o bem-estar dos usuários. Além disso, a automação residencial habilitada por IoT oferece oportunidades para o controle remoto e otimização de vários dispositivos, como ar condicionados e geladeiras, resultando em eficiência energética e maior comodidade para os consumidores.

Outro que vale ressaltar é o setor empresarial, onde a IoT desempenha um papel de suma importância no monitoramento ambiental e no aprimoramento das operações de fabricação (Gubbi et al. 2013). O uso de sensores e dispositivos conectados em ambientes de trabalho ajuda a monitorar a ocupação e a eficiência dos serviços, proporcionando melhorias significativas na segurança e na produtividade do local de trabalho. Além disso, a implementação de ambientes inteligentes dentro de espaços comerciais apresenta várias oportunidades de melhoria e otimização em termos de eficiência energética, gerenciamento de recursos e conforto dos ocupantes. A Figura 2.1 ilustra de maneira abrangente a vastidão das aplicações da IoT, destacando sua presença em setores tão diversos quanto saúde, agricultura, manufatura, transporte e residências inteligentes.

Dentro do ambiente complexo da IoT, diversos padrões tecnológicos têm surgido para atender às demandas específicas de cada domínio de aplicação. Apesar das diferenças, todos os processos subjacentes de operação compartilham similaridades, incluindo a implantação de dispositivos sensores, o uso de redes de comunicação e a coleta e análise de dados por meio de tecnologias avançadas (Bello & Zeadally, 2019). A conectividade com a Internet desempenha um papel crucial na coleta e análise de dados, visando fornecer percepções valiosos para aprimorar os serviços oferecidos. A busca constante por uma interligação eficiente e por serviços de qualidade continua sendo uma prioridade central para atingir o principal propósito da IoT, que é melhorar continuamente a qualidade de vida das pessoas (Bello & Zeadally, 2019). A compreensão desses processos operacionais é essencial para o desenvolvimento e a implementação bem-sucedida de serviços inovadores e eficazes no ecossistema em expansão da IoT.

Figura 2.1: *Diversas Aplicações da Internet das Coisas*



Fonte: BNDES - Plano Nacional de IoT - Roadmap Tecnológico

2.2 Cibersegurança: Fundamentos e Características

A segurança cibernética é uma área que vem evoluindo consideravelmente com o passar do tempo. Inicialmente, as preocupações se concentravam principalmente na confidencialidade, disponibilidade e integridade da informação na década de 1980 (Voydock & Kent, 1983). No entanto, com os constantes avanços tecnológicos, essas definições foram ampliadas para incluir a responsabilidade, onde as partes envolvidas em uma comunicação devem ser capazes de demonstrar a origem e a autenticidade das mensagens (Federrath & Pfitzmann, 2000). A evolução dos objetivos de segurança reflete uma mudança na abordagem da segurança de TI, passando da mera disponibilidade para garantir também a confidencialidade, a integridade e a responsabilidade (Laudon, Laudon, & Schoder, 2015).

Segundo Shirley (2000), para entender a segurança cibernética, é crucial compreender o conceito de ameaças, vulnerabilidades e riscos. Uma ameaça é um evento que tem o potencial de violar a segurança e causar danos, enquanto a vulnerabilidade surge de falhas no design, implementação, operação ou gerenciamento do sistema. Quando esses elementos se combinam, o risco se manifesta, podendo resultar em ataques ativos ou passivos, tanto internos quanto externos, dependendo da intenção e da origem dos invasores (Do, Martini, & Choo, 2019).

Quando fala-se em segurança cibernética, é essencial compreender termos como "adversário" e "*malware*". Um adversário é uma entidade que acessa recursos de um sistema de forma ilícita, enquanto o *malware* é um *software* desenvolvido com o objetivo de comprometer a segurança de um sistema (Do, Martini, & Choo, 2019; Ngo et al., 2020). Compreender essa relação entre ameaças, vulnerabilidades e riscos é crucial para implementar estratégias eficazes de segurança cibernética, a fim de minimizar o impacto de potenciais ataques e garantir a integridade dos sistemas de informação.

Outro ponto importante a destacar são as guerras cibernéticas que junto com as operações

de informação emergem como componentes fundamentais em um cenário global cada vez mais conectado e digitalizado. Essas operações não se limitam apenas a atos de violação da segurança digital, mas integram diversas capacidades de guerra eletrônica e de rede de computadores que visam interferir, destruir ou sequestrar processos de tomada de decisão em nível nacional (Hart et al., 2020). No âmbito da cibersegurança, armadilhas e capturadores desempenham papéis significativos como ferramentas de espionagem cibernética, permitindo o acesso não autorizado a *softwares* e a captura de credenciais de usuários (Liu et al., 2021; Karbasi e Farhadi, 2021). A crescente sofisticação dessas práticas ressalta a importância de abordagens proativas e eficazes na proteção de redes e sistemas contra tais ameaças em evolução constante.

2.3 Desafios na Segurança da Internet das Coisas

A segurança e privacidade dos dispositivos IoT são frequentemente colocadas em risco devido à sua natureza conectada e à falta de padrões de segurança abrangentes (Yang et al., 2017). Os dispositivos IoT estão frequentemente expostos a diferentes tipos de ameaças, incluindo ataques de negação de serviço, invasões de privacidade e roubo de dados (Yang et al., 2017). Além disso, os dispositivos IoT são frequentemente projetados com recursos limitados de segurança, tornando-os vulneráveis a ataques sofisticados. Para proteger os dispositivos IoT e seus usuários, é fundamental implementar técnicas de segurança eficazes em diferentes camadas da arquitetura da IoT (Yang et al., 2017).

De acordo com Kamble e Bhutad (2018), a vulnerabilidade dos dispositivos, a privacidade dos usuários e a segurança dos dados transmitidos representam as principais preocupações no que diz respeito à segurança de dispositivos IoT. Desta forma, são objeto de estudo diversas técnicas de segurança que podem ser empregadas para proteger dispositivos IoT, abrangendo áreas como criptografia, autenticação, controle de acesso e detecção de intrusões (Yang et al., 2017).

A criptografia, de acordo com Laudon e Laudon (2014), refere-se a um processo fundamental que transforma informações em texto ou dados para um formato criptografado, acessível apenas pelo remetente e pelo destinatário desejado. Seu objetivo central é evitar que terceiros não autorizados acessem o conteúdo, assegurando um nível de confidencialidade dos dados transmitidos entre dispositivos. A implementação efetiva da criptografia tornou-se essencial no atual cenário tecnológico, onde a proteção da privacidade e a segurança da informação são de grande importância.

A autenticação é usada para verificar a identidade dos dispositivos IoT e garantir que apenas dispositivos autorizados possam acessar a rede. O controle de acesso é usado para limitar o acesso a recursos de rede específicos com base em regras predefinidas. A detecção de intrusões é usada para identificar e responder a ataques em tempo real (EL-HAJJ et al., 2019).

Capítulo 3

Metodologia

3.1 Procedimento metodológico

A metodologia utilizada nesta revisão sistemática da literatura sobre "Métodos e técnicas de segurança para dispositivos IoT" envolveu uma pesquisa bibliográfica em diversas bases de dados, com o objetivo de identificar os artigos relevantes para a análise e síntese dos dados. As etapas dessa pesquisa serão descritas detalhadamente a seguir.

3.2 Formulação da questão a ser respondida

A questão de pesquisa foi definida como "Quais são as técnicas de segurança mais usadas para dispositivos IoT?". Essa questão foi escolhida com base na importância crescente da IoT no cotidiano e na necessidade de proteger a privacidade e a integridade dos dados dos usuários.

3.3 Definição dos termos de busca

Para a realização da busca bibliográfica na revisão sistemática da literatura sobre métodos e técnicas de segurança para dispositivos IoT, foram definidos os seguintes termos de busca.

I. **Segurança de IoT (*IoT security*)** - Essa palavra-chave foi escolhida para encontrar artigos que abordem os aspectos gerais de segurança em dispositivos IoT, incluindo vulnerabilidades, ameaças e soluções de segurança;

II. **Privacidade de IoT (*IoT privacy*)** - Essa palavra-chave foi escolhida para encontrar artigos que abordem a proteção da privacidade em dispositivos IoT, incluindo o gerenciamento de dados pessoais e a conformidade com regulamentações de privacidade;

III. **Criptografia de IoT (*IoT cryptography*)** - Essa palavra-chave foi escolhida para encontrar artigos que abordem as técnicas de criptografia utilizadas para proteger a comunicação entre dispositivos IoT e a transferência de dados;

IV. **Técnicas de segurança de IoT (*IoT security techniques*)** - Essa palavra-chave foi escolhida para encontrar artigos que descrevam as diversas técnicas de segurança utilizadas para proteger dispositivos IoT, incluindo autenticação, criptografia, controle de acesso, monitoramento e detecção de ameaças.

A seleção das palavras-chave envolveu um processo que demandou um investimento significativo de tempo, com múltiplas combinações sendo consideradas antes de se chegar a uma definição final. Isso se deveu, em parte, às restrições impostas por uma das fontes de busca em relação ao uso de operadores lógicos na formulação da *string* de busca. Para contornar possíveis problemas com os operadores lógicos em algumas pesquisas foi necessário o uso do filtro do tipo "Assunto relacionado" que serviu de base para o aprimoramento dos resultados obtidos.

Uma vez que as palavras-chave e as fontes de busca foram devidamente definidas, foi possível especificar quais serão as *strings* de busca. A estratégia final consistiu em combinar as palavras-chave e seus sinônimos, incorporando operadores lógicos apropriados. Além disso, foi estabelecido que a busca deveria ser realizada nos títulos, resumos e palavras-chave dos artigos. Dado que cada fonte de busca apresentava requisitos específicos para a formatação da *string*, ajustes personalizados foram necessários. Os detalhes específicos dessas configurações para cada fonte podem ser encontrados no Quadro 3.3.

Quadro 3.3: Strings de buscas

Seção	String de busca
I	("técnicas de segurança" OR *"security techniques"*) AND ("dispositivos IoT" OR *"IoT devices"*)
II	("proteção de dados" OR *"IoT data protection"*) AND ("dispositivos IoT" OR *"IoT devices"*)
III	("segurança de rede" OR *"IoT network security"*) AND ("dispositivos IoT" OR *"IoT devices"*)
IV	("vulnerabilidades de segurança" OR *"IoT security vulnerabilities"*) AND ("dispositivos IoT" OR *"IoT devices"*)
V	("soluções de segurança" OR *"IoT security solutions"*) AND ("dispositivos IoT" OR *"IoT devices"*)

3.4 Localização dos estudos

A busca bibliográfica foi realizada em diversas bases de dados, incluindo IEEE Xplore (https://ieeexplore.ieee.org/Xplore/home.jsp), DOAJ Directory of Open Access Journals

(https://doaj.org/) e o ScienceDirect (https://www.sciencedirect.com/). Utilizando os termos de pesquisa “segurança de IoT”, “privacidade de IoT”, “criptografia de IoT” e “técnicas de segurança de IoT”. Os resultados da busca foram importados para o *software* Mendeley (gerenciador de referências bibliográficas) para gestão dos artigos.

3.5 Protocolos de inclusão e exclusão de materiais

3.5.1 Finalidade dos protocolos

O objetivo dos protocolos descritos a seguir é estabelecer critérios claros para a inclusão e exclusão de artigos na revisão sistemática da literatura sobre métodos e técnicas de segurança para dispositivos IoT. O protocolo visa garantir a seleção de estudos relevantes que abordem diretamente o tema proposto.

3.6 Critérios de Inclusão

I. Os artigos devem abordar diretamente métodos ou técnicas de segurança relacionadas a dispositivos IoT ou Cibersegurança no contexto de IoT;

II. Os artigos devem ser relevantes para a compreensão e exploração das técnicas de segurança utilizadas em dispositivos IoT;

III. Os artigos devem ser publicados em periódicos científicos revisados por pares ou conferências.

3.7 Critérios de Exclusão

I. Os artigos que não abordarem diretamente os métodos ou técnicas de segurança para dispositivos IoT ou Cibersegurança relacionados ao ambiente IoT serão excluídos;

II. Artigos que apresentem conteúdo duplicado ou sobreposto serão excluídos, priorizando a inclusão do estudo mais recente ou mais completo;

III. Artigos que não atenderem a critérios mínimos de qualidade, como falta de embasamento teórico, metodologia inadequada, falta de dados empíricos ou análise insuficiente, serão excluídos;

IV. Artigos escritos em idiomas diferentes do inglês ou português serão excluídos devido a restrições de compreensão e recursos de tradução.

3.8 Triagem de seleção dos artigos

I. Durante 8 meses, foram pesquisados artigos publicados em periódicos já mencionados anteriormente;

II. O autor desta RSL se propôs a identificar os materiais relevantes na presente pesquisa;

III. De forma individual, o autor analisou os títulos e resumos dos artigos para verificar a relevância preliminar e a adequação aos critérios de inclusão;

IV. Artigos que não atendem aos critérios de inclusão serão excluídos nessas etapas iniciais;

V. Os artigos selecionados na triagem inicial serão lidos integralmente para uma avaliação mais detalhada, de acordo com os critérios de inclusão e exclusão já estabelecidos;

VI. Após a leitura dos artigos selecionados na triagem inicial, serão abordados nesta RSL os artigos que se fazem relevantes para esse estudo.

Capítulo 4

Resultados Obtidos

Neste capítulo, serão abordadas todas as informações e análises derivadas dos artigos identificados conforme o protocolo aplicado durante a condução desta revisão sistemática da literatura. Posteriormente, são apresentados os resultados e discussões pertinentes a cada questão de pesquisa.

Com o objetivo de estabelecer a presente Revisão Sistemática da Literatura sobre Métodos e Técnicas de Segurança para Dispositivos IoT, foi realizada uma pesquisa inicial exclusivamente por meio de termos de busca presente na metodologia deste trabalho. Os resultados obtidos estão dispostos no Quadro 4, a qual reflete a quantidade de material encontrado inicialmente nas bases de buscas anteriormente mencionadas, sem a aplicação momentaneamente dos critérios de inclusão e exclusão estabelecidos na metodologia deste estudo.

Quadro 4: Resultados das buscas

ID	Base de Dados	Quantidade de artigos encontrados
1	IEEE Xplore	93
2	ScienceDirect	496
3	DOAJ Directory of Open Access Journals	30

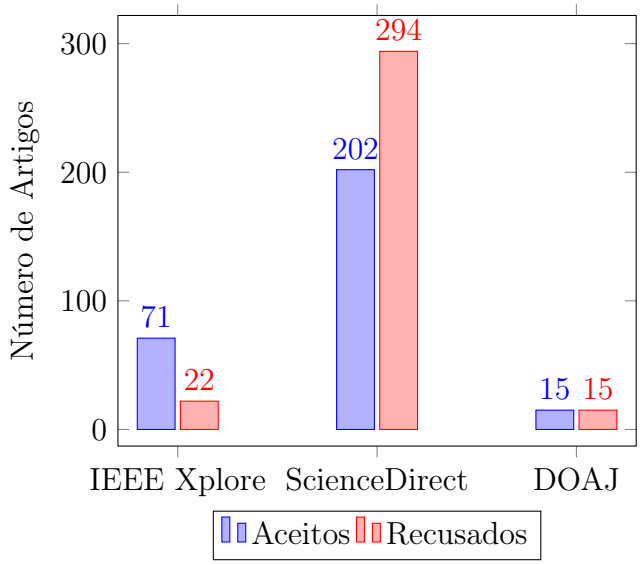
4.1 Análise dos Dados Coletados

Nesta seção, apresentamos uma análise dos dados coletados durante a Revisão Sistemática da Literatura sobre métodos e técnicas de segurança para dispositivos IoT. Os resultados foram obtidos de três fontes principais: IEEE Xplore, ScienceDirect e DOAJ Directory of Open Access Journals.

4.1.1 Número de Artigos Aceitos e Recusados em Cada Base de Dados

Após a fase inicial de seleção dos artigos, realizada com base nos critérios de análise dos títulos e resumos, os resultados obtidos são apresentados na Figura 4.1.1, na qual foi realizada a separação entre os artigos aceitos e recusados em cada base de dados.

Figura 4.1.1: Resultados Obtidos



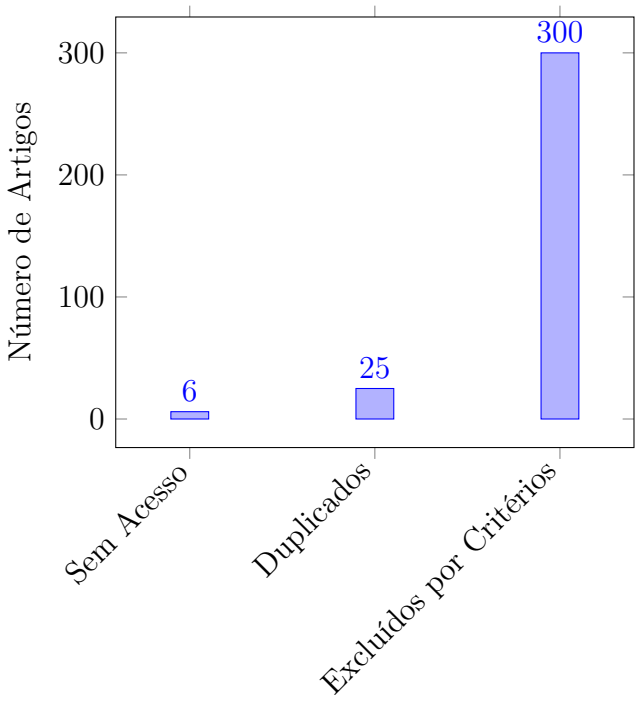
4.1.2 Análise da Fase de Exclusão dos Artigos

Além de categorizar os artigos como aceitos ou recusados, conduziu-se uma análise mais aprofundada da etapa de exclusão de materiais durante a RSL. Os resultados estão resumidos na Figura 4.1.2.

Observou-se que, dentre os artigos coletados por meio das *strings* de busca, 6 artigos não tinham acesso ao documento completo, enquanto 25 artigos estavam duplicados. A etapa inicial de inclusão de material resultou na exclusão de 300 artigos que não atenderam aos critérios de inclusão previamente estabelecidos nesta RSL, totalizando 331 artigos excluídos na primeira fase.

Após examinar os títulos seguidos dos resumos (*abstracts*) dos artigos identificados pelas *strings* de busca, os principais motivos de exclusão foram a falta de abordagem direta sobre métodos ou técnicas de segurança para dispositivos IoT, ou a ausência de enfoque em cibersegurança relacionada ao ambiente IoT.

Figura 4.1.2: Resultados da Fase de Exclusão de Artigos

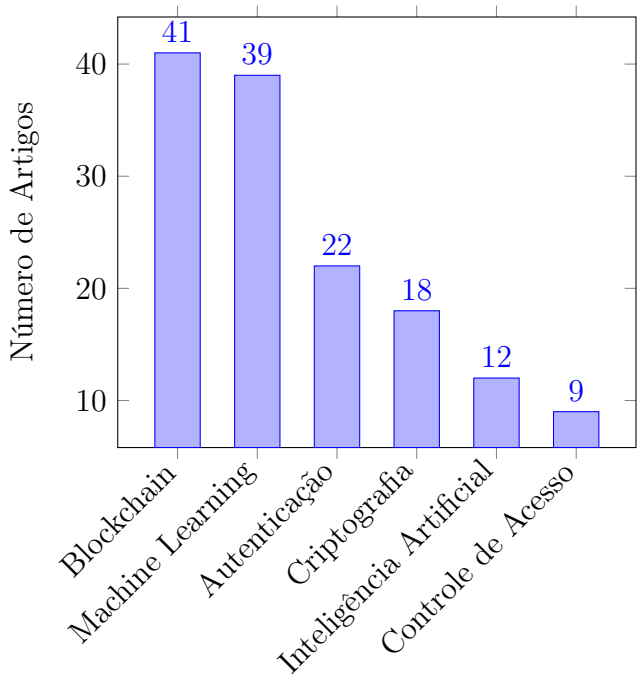


4.1.3 Análise dos Artigos Selecionados na Segunda Etapa da RSL

Nesta etapa da RSL, foram analisados os títulos, resumos e introduções dos 288 artigos que avançaram para a segunda fase de seleção. Após essa análise, com o objetivo de responder às questões inicialmente levantadas durante a condução desta RSL, obtivemos alguns resultados, como demonstrado na figura 4.1.3.

Foram identificados os assuntos mais recorrentes como tema central dos artigos que abordavam a segurança em dispositivos IoT. Realizou-se uma verificação para identificar a interseção desses assuntos, buscando apenas aqueles que eram os temas centrais dos artigos. Embora a maioria dos autores tenha abordado brevemente cada método e técnica de segurança para dispositivos IoT, observa-se uma tendência crescente ao uso de ferramentas correlacionadas, como *blockchain*, *machine learning* e inteligência artificial, para desenvolver novas estratégias de segurança.

Figura 4.1.3: Assunto Central Abordado sobre Segurança IoT



4.2 Exploração Bibliográfica

Com o objetivo de proporcionar uma compreensão mais clara para o leitor, será apresentada um quadro contendo as referências bibliográficas utilizadas na elaboração dos resultados obtidos desta RSL. O quadro fornecerá informações como base de dados de onde cada artigo foi obtido, o título, os autores, o ano de publicação e o assuntro central abordado em cada artigo. Essa abordagem visa oferecer uma visão organizada e acessível das fontes bibliográficas essenciais que fundamentam os resultados desta revisão.

Quadro 4.2: Quadro de artigos usados nesta RSL

ID	Base de Dados	Título	Autores	Ano	Assunto Central
1	DOAJ	Segurança da Informação para Internet das Coisas (IoT): uma Abordagem sobre a Lei Geral de Proteção de Dados (LGPD)	Nairobi Spiecker de Oliveira, Moises Alexandre Gomes, Ronaldo Lopes, Jéferson C. Nobre	2019	Lei Geral de Proteção de Dados

ID	Base de Dados	Título	Autores	Ano	Assunto Central
2	IEEE Xplore	A Survey on Security and Privacy Issues in Internet-of-Things	Yang Yuchen, Wu Longfei, Yin Guisheng, Li Lijie, Zhao Hongbin	2017	Autenticação
3	IEEE Xplore	Exploring Security and Authentication Issues in Internet of Things	Prathibha L, Kaleem Fatima	2018	Autenticação
4	IEEE Xplore	IoT Security Techniques Based on Machine Learning: How Do IoT Devices Use AI to Enhance Security?	Liang Xiao, Xiaoyue Wan, Xiaozhen Lu, Yanyoung Zhang, Di Wu	2018	Machine Learning
5	IEEE Xplore	Survey on Internet of Things (IoT) security issues e solutions	Kamble Ashvini, Bhutad Sonali	2018	Monitoramento de Segurança
6	IEEE Xplore	Enhanced Data Security and Authentication Techniques for IoT Devices on Cloud	Neha Kashyap, Ajay Rana, Vineet Kansal, Himdweep Walia	2021	Autenticação
7	IEEE Xplore	Security Threats and Artificial Intelligence Based Countermeasures for Internet of Things Networks: A Comprehensive Survey	Shakila Zaman, Khaled Alhazmi, Mohammed A. Aseeri, Muhammad Raisuddin Ahmed, Risala Tasin Khan, M. Shamim Kaiser, Mufti Mahmud,	2021	Inteligência Artificial

ID	Base de Dados	Título	Autores	Ano	Assunto Central
8	ScienceDirect	A blockchain future for internet of things security: a position paper	Mandrita Banerjee, Junghee Lee, Kim-Kwang Raymond Choo	2018	Blockchain
9	ScienceDirect	Blockchain mechanisms for IoT security	Daniel Minoli, Benedict Occhiogrosso	2018	Blockchain
10	ScienceDirect	IoT security: Review, blockchain solutions, and open challenges	Minhaj Ahmad Khan, Khaled Salah	2018	Blockchain
11	ScienceDirect	System Hardening and Security Monitoring for IoT Devices to Mitigate IoT Security Vulnerabilities and Threats	Choi S.-K, Yang C.-H, Kwak Jin	2018	Monitoramento de Segurança
12	ScienceDirect	BlockIoTIntelligence A Blockchain-enabled Intelligent IoT Architecture with Artificial Intelligence	Sushil Kumar Singh, Shailendra Rathore, Jong Hyuk Park	2020	Blockchain
13	ScienceDirect	Machine learning based solutions for security of Internet of Things (IoT): A survey	Syeda Manjia Tahsien, Hadis Karimipour, Petros Spachos	2020	Machine Learning

ID	Base de Dados	Título	Autores	Ano	Assunto Central
14	ScienceDirect	Authentication and Identity Management of IoHT Devices: Achievements, Challenges, and Future Directions	Moustafa Mamdouh, Ali Ismail Awad, Ashraf A.M. Khalaf, Hesham F.A. Hamed	2021	Autenticação
15	ScienceDirect	Landscape of IoT security	Eryk Schiller, Andy Aidoo, Jara Fuhrer, Jonathan Stahl, Michael Ziörjen, Burkhard Stiller	2022	Autenticação
16	ScienceDirect	Machine learning and the Internet of Things security: Solutions and open challenges	Umer Farooq, Noshina Tariq, Muhammad Asim, Thar Baker, Ahmed Al-Shamma	2022	Machine Learning
17	ScienceDirect	Access control in Internet of Things: A survey	Rahma Trabelsi, Ghofrane Fersi, Mohamed Jmaiel	2023	Controle de Acesso
18	ScienceDirect	Cryptography Algorithms for Enhancing IoT Security	Fursan Thabit, Ozgu Can, Asia Othman Aljahdali, Ghaleb H. Al-Gaphari, Hoda A. Alkhzaim	2023	Criptografia

ID	Base de Dados	Título	Autores	Ano	Assunto Central
19	ScienceDirect	Enhancement of IoT device security using an Improved Elliptic Curve Cryptography algorithm and malware detection utilizing deep LSTM	R. Aiyshwariya Devi, A.R. Arunachalam	2023	Criptografia
20	ScienceDirect	Towards SDN-based smart contract solution for IoT access control	Mizna Khalid, Sufian Hameed, Abdul Qadir, Syed Attique Shah, Dirk Draheim	2023	Controle de Acesso

A seleção dos artigos definitivos explorados nesta RSL é realizada exclusivamente com base no critério de relevância do tópico abordado e na incorporação de informações pertinentes, seguindo a perspectiva adotada pelo autor desta revisão.

4.3 Principais Tendências em Segurança para Dispositivos IoT

O propósito desta seção é conduzir uma análise detalhada para oferecer uma visão abrangente das tendências mais significativas em segurança para dispositivos IoT, evidenciando os temas centrais e os métodos preferidos pelos pesquisadores.

Durante a condução desta RSL, observou-se que temas como *blockchain*, aprendizado de máquina, criptografia e autenticação foram os mais frequentemente discutidos, conforme já destacado nos dados fornecidos anteriormente. Com o intuito de aprofundar o entendimento desses conceitos e sua interação com os métodos e técnicas de segurança aplicados a dispositivos IoT, será feito uma abordagem inicial com os temas predominantes identificados na pesquisa. Posteriormente, será apresentado uma visão abrangente sobre as demais técnicas identificadas.

4.3.1 Blockchain

Como enfatizado ao longo desta RSL, a *blockchain* surge como uma técnica de grande destaque nos estudos analisados. Esta tecnologia apresenta-se como uma solução promissora, oferecendo um paradigma descentralizado, distribuído e imutável para assegurar a integridade e autenticidade dos dados. De acordo com Khan e Salah (2018), a *Blockchain* opera como um livro-razão compartilhado, onde cada transação é verificada por consenso, proporcionando confiança distribuída sem depender de terceiros confiáveis. Inicialmente projetado para transações financeiras, o *blockchain* se revela robusto para aprimorar a segurança na IoT (Banerjee et al., 2018). O modelo transparente e descentralizado oferecido pelo *blockchain* é essencial para garantir a integridade e autenticidade dos dados em um ambiente onde a confiança é crucial.

A Métrica de Integridade de Referência (RIM) mantida no *blockchain* desempenha um papel crucial na validação e integridade dos conjuntos de dados, proporcionando uma solução descentralizada para preservar a privacidade e superar desafios relacionados à vida útil dos dados compartilhados. Essa descentralização das informações de associação, como endereço, proprietário e política de compartilhamento, é destacada como um componente fundamental dessa abordagem, conforme ressaltado por Minoli e Occhiogrosso (2018).

Outro cenário explorado refere-se à detecção de *firmware* comprometido e à auto-recuperação baseada em *blockchain* (Minoli & Occhiogrosso, 2018). Reconhecendo a inevitabilidade de comprometimentos de segurança em dispositivos IoT, essa proposta sublinha a importância de utilizar o *blockchain* para proteger a Métrica de Integridade de Referência associada ao *firmware*. Essa abordagem oferece uma estratégia eficaz de auto-recuperação, permitindo a substituição de *firmware* comprometido por versões conhecidas por sua segurança. O histórico do *firmware* registrado no blockchain facilita o rastreamento e a reversão para versões anteriores, contribuindo para a robustez da segurança em dispositivos IoT.

O interesse crescente em *blockchains* destaca sua relevância tanto na pesquisa quanto na prática, especialmente no contexto da segurança para dispositivos IoT (Minoli & Occhiogrosso, 2018). Além das aplicações originais em criptomoedas, os *blockchains* mostram potencial para casos de uso diversificados, incluindo contratos inteligentes, cibersegurança e gerenciamento de dados logísticos.

4.3.2 Machine learning

Uma temática recorrente que vem se destacando ao longo dos anos é o papel significativo do aprendizado de máquina (*Machine Learning*) na segurança dos dispositivos IoT. Conforme discutido por Farooq et al. (2022), o *machine learning* (ML) se destaca como um método intelectual que otimiza a interpretação de informações ou experiências por meio do aprendizado, sendo particularmente relevante na análise de dados massivos gerados pela IoT. Esse método, por sua vez, fundamenta-se em abordagens matemáticas e possibilita que

dispositivos inteligentes aprendam sem depender de programação explícita, tornando-se uma ferramenta essencial na previsão de tendências futuras para fluxos de dados de entrada.

O Aprendizado de Máquina apresenta soluções versáteis, sendo aplicável em diversas situações, desde a detecção de intrusões em sistemas de navegação em regiões hostis até a análise de ameaças em dispositivos móveis. Destaca-se sua importância na melhoria da inteligência das redes IoT, especialmente por meio da mineração de grandes volumes de dados gerados por essas redes. Além disso, os algoritmos de ML são utilizados para fortalecer a segurança em áreas como análise de *malware*, detecção de ataques, autenticação e gestão de anomalias, contribuindo significativamente para a robustez dos sistemas IoT (Farooq et al., 2022).

As técnicas de ML revelam-se particularmente eficazes na detecção precoce de ameaças à IoT, analisando comportamentos suspeitos dos dispositivos (Tahsien et al., 2020). A aplicação desses algoritmos não apenas identifica ataques, mas também viabiliza a implementação de políticas defensivas robustas. No contexto das técnicas supervisionadas de ML, como destacado por Tahsien et al. (2020), o aprendizado de máquina supervisionado desempenha um papel central. Essa abordagem, que inclui a classificação e regressão dos dados de entrada, oferece uma base sólida para a construção de modelos de segurança na IoT.

A transferência de rastros de aplicativos para servidores de segurança na nuvem ou dispositivos de borda também são evidenciadas nos principais estudos sobre o uso de ML na segurança de dispositivos IoT, destacando a necessidade de uma abordagem dinâmica. Esses resultados consolidam a importância do uso estratégico de técnicas de ML na segurança IoT, mas também apontam para a necessidade contínua de pesquisa e desenvolvimento para superar os desafios identificados (Xiao et al., 2018).

4.3.3 Autenticação

A autenticação, definida como o processo de identificar pessoas autorizadas a acessar sistemas digitais, desempenha um papel fundamental no cenário de segurança cibernética (Prathibha & Kaleem, 2018). A identificação de pessoas autorizadas é crucial para evitar acessos não autorizados a máquinas, serviços e aplicativos conectados à IoT, assegurando a legitimidade dos dados e a validade das conexões. A complexidade da autenticação na IoT é acentuada pela grande quantidade de objetos digitais na infraestrutura. A implantação de dispositivos IoT em áreas públicas sem proteção apresenta desafios adicionais, tornando-os suscetíveis a ataques físicos e dificultando a gestão eficaz. O reconhecimento e a autenticação de cada objeto digital tornam-se, portanto, uma tarefa complexa e crítica (Prathibha & Kaleem, 2018).

A autenticação de dois fatores e a autenticação multifatorial foram abordadas como métodos eficazes para fortalecer a segurança. A autenticação de dois fatores exige informações adicionais além da senha, enquanto a autenticação multifatorial, por meio de senhas dinâmicas de uso único, acrescenta uma camada adicional de segurança limitando a validade

das senhas temporárias (Prathibha & Kaleem, 2018) A autenticação baseada em fatores como identidade e contexto desempenha um papel de suma importância na segurança IoT. A autenticação de identidade, seja simétrica ou assimétrica, envolve características físicas (biometria) e comportamentais (identificação de voz, dinâmica de digitação) (Neha et al., 2019).

Os procedimentos de autenticação incluem autenticação unidirecional, bidirecional e tridirecional, cada um atendendo a diferentes requisitos de segurança. A arquitetura de autenticação pode ser distribuída ou centralizada, empregando esquemas planos ou hierárquicos conforme necessário. Além disso, a autenticação baseada em *token* oferece protocolos distintos, como baseada em *token* (com baixo tráfego de mensagens) e não baseada em *token* (com alto tráfego de mensagens) (Neha et al., 2018).

A autenticação de dispositivos na Internet das Coisas é uma preocupação crucial, particularmente no contexto da Internet das Coisas para Saúde (IoHT), uma aplicação que está crescendo exponencialmente e proporciona maior conforto às vidas humanas (Mamdouh et al., 2021). O desafio da autenticação de dispositivos IoHT se concentra na camada de percepção, onde mecanismos de autenticação pouco confiáveis podem aumentar a suscetibilidade desses dispositivos a ameaças e ataques maliciosos.

4.3.4 Criptografia

A segurança em dispositivos IoT apresenta desafios significativos, como interoperabilidade, segurança de privacidade, expectativa de vida, suporte tecnológico, entre outros (Thabit et al., 2023). A criptografia surge como uma ferramenta crucial para enfrentar esses desafios, garantindo a privacidade, integridade, autenticação e autorização da transferência de dados através de dispositivos IoT (Thabit et al., 2023). No entanto, a aplicação convencional de técnicas de criptografia baseadas em computadores pessoal (PC) revela-se inadequada para dispositivos IoT devido a suas limitações de recursos. A necessidade de abordagens mais eficientes, como a criptografia leve, torna-se evidente diante desses desafios.

A criptografia leve para dispositivos IoT com recursos limitados oferece características essenciais, considerando fatores como desempenho, custo físico e segurança (Thabit et al., 2023). Avaliar o custo de implementação, demanda de memória, consumo de energia e outros fatores é crucial ao adicionar criptografia a dispositivos com recursos restritos. A análise dessas características proporciona escolha de abordagens mais eficazes que atendam às demandas específicas de dispositivos IoT.

A classificação da criptografia leve com base em sua estrutura destaca a distinção entre cifras de chave simétrica e assimétrica (Thabit et al., 2023). A criptografia de chave simétrica, embora relativamente rápida e segura, requer a pré-compartilhamento da chave entre as partes comunicantes. Por outro lado, a criptografia assimétrica utiliza pares de chaves privadas e públicas, proporcionando confidencialidade e integridade, mas introduzindo complexidade e exigindo gerenciamento cuidadoso das chaves. Essas escolhas estruturais são

cruciais para adaptar a criptografia aos requisitos específicos dos dispositivos IoT.

Uma das técnicas que está sendo amplamente discutida em criptografia e a metodologia de Criptografia de Curva Elíptica melhorada (ECC) e detecção de *malware* (Criptografia de chave pública com base na estrutura algébrica de curvas elípticas). que visa introduzir um mecanismo de segurança aprimorado que emprega criptografia. Essa abordagem é destinada ao desenvolvimento de dispositivos IoT conectados a servidores na nuvem para receber *firmware* de substituição de forma segura, incorporando a geração dinâmica de chaves.

A proposta abrange três fases distintas, envolvendo detecção contextual de anomalias, previsão de diferentes tipos de *malwares* e transmissão segura de dados utilizando um algoritmo de Criptografia de Curva Elíptica Melhorada (Devi & Arunachalam, 2023).

Na primeira fase, a detecção contextual de anomalias é realizada para categorizar nós normais e nós de ataque na rede IoT. Parâmetros como alcance de transmissão, consumo de energia e outros são considerados para estimar o valor de confiança, identificando nós atacados com base nesse limiar. A segunda fase aborda a previsão de diferentes tipos de *malwares*, utilizando pacotes relacionados aos nós de ataque identificados anteriormente. E a terceira fase concentra-se na transmissão segura de dados, criptografando arquivos de dispositivos IoT usando um algoritmo de Criptografia de Curva Elíptica Melhorada. Essa medida visa restringir o acesso de *malwares*, garantindo a segurança dos dados durante a transferência para servidores na nuvem (Devi & Arunachalam, 2023).

4.3.5 Inteligência Artificial (IA)

Com um forte vínculo ao aprendizado de máquinas, observamos a aplicação de técnicas de segurança para dispositivos IoT fundamentadas em inteligência artificial. Segundo Zaman et al. (2021), a abordagem pautada em Inteligência Artificial (IA) concentra-se nos dados, demandando, assim, um extenso conjunto de dados reais provenientes do ambiente do mundo real, essenciais como blocos de construção para os modelos baseados em IA. Para atingir um desempenho otimizado, esse vasto volume de dados é particionado em dois conjuntos distintos: o conjunto de treinamento e o conjunto de teste. O modelo é treinado com um conjunto de treinamento equilibrado e imparcial, enquanto o conjunto de teste é empregado para avaliar o desempenho do modelo.

A autora ressalta a importância de um modelo de ameaça baseado em IA capaz de analisar grandes volumes de dados recebidos em tempo real, identificar ameaças e iniciar uma resposta rápida para prevenir ataques cibernéticos antes que o invasor danifique ou roube dados do sistema. A análise de *big data* em tempo real pode examinar os registros de eventos de uma organização e detectar ameaças, auxiliando na prevenção de ataques. Nesse sentido, há uma oportunidade para o desenvolvimento de uma plataforma de análise de dados em larga escala, que seja capaz de identificar ataques contextualmente conscientes sem atrasos significativos.

O mercado em ascensão da Inteligência Artificial, aliado ao *blockchain* para IoT, reflete

a crescente importância dessas tecnologias na resolução de desafios fundamentais. A convergência dessas tecnologias é projetada para catalisar a inovação em diversas áreas, como evidenciado pelo crescimento projetado para o mercado de IA até 2030 (Singh et al., 2020). A abordagem descentralizada de IA, combinada com *Blockchain*, destaca-se como uma solução para compartilhamento seguro de informações, tomada de decisões autônoma e mitigação de pontos únicos de falha, promovendo assim a eficiência na análise de *big data* para aplicações de IoT.

A aplicação de abordagens fundamentadas em regras e algoritmos de aprendizado de máquina, que são ramos da Inteligência Artificial, pode ser utilizada como uma medida preventiva, juntamente com os protocolos de segurança de rede já existentes. Essas abordagens mostram-se promissoras no contexto da segurança da Internet das Coisas, com o intuito de mitigar as ameaças presentes nesse ambiente (Zaman et al. 2021).

4.3.6 Controle de Acesso

O controle de acesso em dispositivos IoT é uma questão crítica para garantir a segurança e a integridade da rede, considerando a potencial entrada de nós maliciosos que podem comprometer as operações e manipular informações sensíveis (Khalid et al., 2023). Nesse contexto, é vital que os dispositivos IoT ingressem em uma rede com algoritmos de autenticação e políticas de segurança, visando prevenir atividades maliciosas (Khalid et al., 2023). A necessidade de resistência a manipulações e adulterações nos dispositivos IoT é evidenciada, destacando a importância de políticas de controle de acesso eficientes para manter a segurança do ambiente (Khalid et al., 2023).

Essa complexidade do ecossistema da IoT, caracterizado por baixo consumo de energia, latência limitada, redes distribuídas e uma ampla variedade de dispositivos, demanda diferentes sistemas de controle de acesso (Khalid et al., 2023). Nesse contexto, a proposição de uma abordagem de centralização na rede IoT, integrando uma estrutura de gerenciamento baseada na Rede Definida por Software (SDN), objetiva o registro das operações de rede e a concessão de acesso exclusivamente a usuários previamente verificados por intermédio do controle de acesso.

Dessa forma, os desafios e requisitos críticos de segurança em redes IoT incluem a necessidade de estabelecer uma relação confiável entre dispositivos, impedir acesso não autorizado a recursos, garantir a integridade e confidencialidade das informações, e reduzir a carga computacional relacionada ao controle de acesso (Khalid et al., 2023). Nesse cenário, a integração de SDN e blockchain emerge como uma solução complementar. Estratégias como a administração de acesso, limites de vinculação de nós, segurança contra-ataques maliciosos e o significado de políticas aceitas são abordadas por meio dessa integração, proporcionando um ambiente mais seguro e confiável para a IoT (Khalid et al., 2023).

Além disso, pesquisas em métodos e técnicas de segurança para dispositivos IoT têm desempenhado um papel fundamental na evolução das soluções de controle de acesso. A

classificação das abordagens em soluções centralizadas e distribuídas destaca a importância de escolher a arquitetura mais adequada às necessidades específicas de diferentes ambientes (TRABELSI et al., 2023). Embora as soluções centralizadas sejam eficazes para ambientes domésticos inteligentes com um número limitado de dispositivos, sua escalabilidade pode ser desafiadora em sistemas maiores, como cidades inteligentes. Nesse contexto, as soluções distribuídas mostram-se mais eficientes, lidando bem com o aumento de dispositivos, sendo escaláveis e tolerantes a falhas.

O cenário de cooperação entre organizações na IoT destaca a importância do controle de acesso interorganizacional. Quando dispositivos de uma organização buscam acessar recursos pertencentes a outras organizações, a necessidade de controle de acesso entre elas é crucial (TRABELSI et al., 2023). Dessa forma, a integração de técnicas físicas, como bloqueio físico, proteção contra roubo e ocultação de portas de acesso, em conjunto com as soluções de controle de acesso, mostrou-se crucial no reforço da segurança desses dispositivos em ambientes diversos.

4.3.7 Monitoramentos de Segurança e Detecção de Intrusão

Segundo Choi et al. (2018), o monitoramento de segurança desempenha um papel fundamental no acompanhamento contínuo do *status* de fortalecimento do sistema dos dispositivos IoT. Essa funcionalidade de monitoramento está diretamente ligada à análise dos registros gerados a partir da ativação da função de registro nos dispositivos IoT, com o intuito de identificar precocemente sinais anômalos e minimizar vulnerabilidades e ameaças à segurança. Por exemplo, por meio de uma análise contínua dos registros internos, o monitoramento de segurança é capaz de detectar indícios anômalos, como solicitações persistentes de acesso *Secure Shell* (SSH) provenientes de *Internet Protocol* (IPs) externos não autorizados, e assim, acionar uma variedade de planos de resposta, como notificar o gerente do dispositivo IoT ou bloquear o IP correspondente.

No âmbito da detecção de intrusão, uma investigação conduzida por Kamble et al. (2018) destaca que as técnicas associadas desempenham um papel crucial na mitigação de diversas ameaças à segurança em dispositivos da IoT. Essas técnicas são capazes de identificar atividades suspeitas no sistema por meio de um monitoramento contínuo e do registro detalhado das ações do invasor, o que possibilita o rastreamento posterior. Atualmente, existem abordagens únicas para a detecção de intrusão, incluindo a utilização de métodos de mineração de informações e a detecção de anomalias. Essas estratégias visam fornecer respostas efetivas no contexto da segurança dos dispositivos IoT.

Um desafio relacionado à segurança na camada de percepção dos dispositivos IoT envolve a detecção de nós de sensores anormais. Essa situação pode ocorrer quando um nó é alvo de ataques físicos, como danos ou desativação, ou quando é comprometido por ataques cibernéticos. Esses nós são comumente denominados como nós defeituosos. Para assegurar a qualidade do serviço, é imprescindível identificar esses nós defeituosos e adotar medidas

para evitar uma degradação adicional do serviço (Yang et al., 2017).

4.3.8 Regulamentação para Proteção de Dados e Privacidade

Conforme Schiller et al. (2022), o mercado oferece várias soluções para combater ameaças relacionadas à Internet das Coisas. No entanto, é importante destacar que o mercado não é o único agente envolvido na abordagem das preocupações de segurança nesse contexto. Nos últimos anos, têm surgido novas regulamentações que impactam o domínio da IoT e abordam as preocupações de segurança de uma perspectiva diferente. O amplo uso da tecnologia IoT e seu impacto na vida cotidiana têm gerado uma crescente necessidade de regulamentações específicas, considerando que bilhões de sensores implantados rastreiam cada movimento e percebem cada mudança, resultando em uma quantidade massiva de informações que revelam detalhes como "quem somos, onde estamos, o que fazemos e como fazemos".

Os dispositivos IoT coletam enormes volumes de dados, tornando essencial a análise de como a IoT pode ser suficientemente segura e a necessidade de regulamentar o manuseio e processamento desses dados. Uma legislação recente com implicações significativas é o Regulamento Geral de Proteção de Dados (GDPR, na sigla em inglês)[1]. O principal objetivo do GDPR é proteger e regulamentar a privacidade dos dados dos cidadãos da União Europeia (UE). Portanto, os dados altamente sensíveis coletados por dispositivos IoT também devem estar sujeitos às disposições do GDPR (Schiller et al., 2022).

Seguindo os mesmos princípios da GDPR, foi instituída no Brasil a Lei Geral de Proteção de Dados (LGPD)[2], estabelecida no segundo semestre de 2018, representa uma regulamentação crucial para empresas públicas e privadas em relação ao tratamento de dados pessoais e sigilosos dos usuários (Nobre et al., 2019). Com prazo de adequação até fevereiro de 2020, a LGPD busca equilibrar o tratamento desses dados pelos dispositivos IoT, especialmente desafiador em setores como automação residencial, onde a coleta, análise e cruzamento de informações pessoais são frequentes. Garantir a privacidade do usuário nesse contexto se torna uma tarefa complexa, demandando métodos específicos para coleta de autorização, padrões seguros de transmissão, modelos de armazenamento seguro e procedimentos para exclusão de dados após o término do relacionamento entre usuário e empresa (Nobre et al., 2019).

A LGPD estabelece diretrizes importantes para a responsabilidade das empresas no uso e armazenamento de dados dos usuários. A responsabilidade exigida pela LGPD pode ser alcançada por meio da aplicação de mecanismos e técnicas de Segurança da Informação (SI), visto que a abordagem de muitos aspectos da lei está diretamente relacionada a controles e modelos de privacidade de dados inerentes a essa área (Nobre et al., 2019). A interseção entre LGPD, SI e IoT destaca-se como um ponto crítico na busca por conformidade e proteção dos dados pessoais.

[1]GDPR site: <https://gdpr-info.eu/>
[2]LGPD site: <https://www.lgpdbrasil.com.br/>

No contexto da segurança da informação, LGPD e IoT, destaca-se o desafio de implementar mecanismos e tecnologias capazes de garantir a privacidade dos dados dos usuários em dispositivos IoT que, por natureza, possuem limitações físicas significativa. Dispositivos presentes em residências, veículos e atividades diárias já coletam informações sensíveis sobre o comportamento e perfil dos usuários, exigindo um esforço adicional para atender aos objetivos da LGPD. A aplicação dos requisitos de segurança em dispositivos restritos, considerando suas limitações de processamento, vida útil da bateria, memória e armazenamento, demanda a utilização de normas de Segurança da Informação para atingir os padrões estabelecidos pela LGPD (Nobre et al., 2019).

Capítulo 5

Considerações Finais

Este trabalho de conclusão de curso (TCC) teve como objetivo a investigação e análise da segurança na Internet das Coisas, fundamentando-se em estudos e pesquisas recentes. Para a seleção dos estudos a serem analisados neste TCC, foi adotado um processo meticuloso e sistemático. A metodologia de pesquisa foi apresentada por meio de uma RSL, na qual os detalhes das buscas e os resultados obtidos foram discutidos, incluindo a apresentação de alguns dados numéricos.

Ao abordar diferentes aspectos relacionados a esta área, foram obtidas percepções valiosas acerca dos desafios enfrentados, dos protocolos de segurança empregados, das vulnerabilidades e ataques potenciais, bem como dos modelos de segurança, tecnologias e abordagens utilizadas para fortalecer a segurança na IoT. Ficou evidente que a segurança na IoT é uma preocupação crescente devido à diversidade de dispositivos conectados e ao ambiente heterogêneo em que operam. Os desafios identificados incluem a falta de padronização de segurança, a presença de dispositivos com recursos limitados e a necessidade de proteger os dados sensíveis dos usuários.

Uma descoberta notável que emergiu durante a pesquisa reside na significativa quantidade de artigos dedicados à exploração do *Blockchain* como uma medida de segurança robusta e promissora para dispositivos da IoT. Essa abordagem, quando integrada com técnicas de *machine learning* e inteligência artificial, revelou-se de notável importância nos avanços tecnológicos desses dispositivos, os quais estão cada vez mais inseridos em nosso cotidiano.

Além disso, várias tecnologias e abordagens têm sido exploradas para fortalecer a segurança na IoT. O aprendizado de máquina, por exemplo, tem sido utilizado para melhorar a detecção de *malware*, controle de acesso e detecção de intrusões. O monitoramento contínuo de segurança desempenha um papel fundamental na identificação de atividades anômalas e na resposta rápida a possíveis ameaças. A aplicação de inteligência artificial, especialmente a análise de *big data* em tempo real, possibilita a detecção de ameaças contextualmente conscientes.

Do mesmo modo, a proteção dos dados e da privacidade dos usuários mostrou-se como uma preocupação central na segurança da IoT. Regulamentações como o Regulamento Geral

de Proteção de Dados na União Europeia e a Lei Geral de Proteção de Dados no Brasil estabelecem diretrizes importantes para o tratamento adequado dos dados pessoais coletados pelos dispositivos IoT.

A presente RSL proporcionou uma visão abrangente sobre a segurança na IoT. Os estudos examinados evidenciaram os desafios enfrentados nesse contexto, bem como os protocolos de segurança, vulnerabilidades e ataques identificados, modelos de segurança implementados, além das tecnologias e abordagens adotadas. Deve-se ressaltar que não se identificou uma técnica singularmente superior, mas sim a necessidade de uma combinação de várias técnicas, as quais se mostram essenciais para estabelecer uma barreira adicional contra potenciais problemas de segurança.

Referências Bibliográficas

[Aiyshwariya Devi e Arunachalam 2023] Aiyshwariya Devi, R.; ARUNACHALAM, A. Enhancement of iot device security using an improved elliptic curve cryptography algorithm and malware detection utilizing deep lstm. *High-Confidence Computing*, v. 3, n. 2, p. 100117, 2023. ISSN 2667-2952. Disponível em: <https://www.sciencedirect.com/science/article/pii/S2667295223000156>.

[Asghari, Rahmani e Javadi 2019] ASGHARI, P.; RAHMANI, A. M.; JAVADI, H. H. S. Internet of things applications: A systematic review. *Computer Networks*, v. 148, p. 241–261, 2019. ISSN 1389-1286. Disponível em: <https://www.sciencedirect.com/science/article/pii/S1389128618305127>.

[Banerjee, Lee e Choo 2018] BANERJEE, M.; LEE, J.; CHOO, K.-K. R. A blockchain future for internet of things security: a position paper. *Digital Communications and Networks*, v. 4, n. 3, p. 149–160, 2018. ISSN 2352-8648. Disponível em: <https://www.sciencedirect.com/science/article/pii/S2352864817302900>.

[Bello e Zeadally 2019] BELLO, O.; ZEADALLY, S. Toward efficient smartification of the internet of things (iot) services. *Future Generation Computer Systems*, v. 92, p. 663–673, 2019. ISSN 0167-739X. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0167739X17317326>.

[Choi, Yang e Kwak 2018] CHOI, S.-K.; YANG, C.-H.; KWAK, J. System hardening and security monitoring for iot devices to mitigate iot security vulnerabilities and threats. *KSII Transactions on Internet and Information Systems*, v. 12, p. 906–918, 02 2018.

[Das, Zeadally e He 2018] DAS, A. K.; ZEADALLY, S.; HE, D. Taxonomy and analysis of security protocols for internet of things. *Future generation computer systems*, Elsevier B.V, v. 89, p. 110–125, 2018. ISSN 0167-739X.

[El-hajj *et al.* 2019] EL-HAJJ, M. *et al.* A survey of internet of things (iot) authentication schemes. *Sensors*, v. 19, n. 5, 2019. ISSN 1424-8220. Disponível em: <https://www.mdpi.com/1424-8220/19/5/1141>.

[Farooq *et al.* 2022] FAROOQ, U. *et al.* Machine learning and the internet of things security: Solutions and open challenges. *Journal of Parallel and Distributed Computing*, v. 162, p. 89–104, 2022. ISSN 0743-7315. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0743731522000235>.

[Gubbi *et al.* 2013] GUBBI, J. *et al.* Internet of things (iot): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, v. 29, n. 7, p. 1645–1660, 2013. ISSN 0167-739X. Including Special sections: Cyber-enabled Distributed Computing for Ubiquitous Cloud and Network Services Cloud Computing and Scientific Applications — Big

Data, Scalable Analytics, and Beyond. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0167739X13000241>.

[Hart *et al.* 2020] HART, S. *et al.* Riskio: A serious game for cyber security awareness and education. *Computers Security*, v. 95, p. 101827, 2020. ISSN 0167-4048. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0167404820301012>.

[Kamble e Bhutad 2018] KAMBLE, A.; BHUTAD, S. Survey on internet of things (iot) security issues solutions. In: *2018 2nd International Conference on Inventive Systems and Control (ICISC)*. [S.l.: s.n.], 2018. p. 307–312.

[Kashyap *et al.* 2021] KASHYAP, N. *et al.* Enhanced data security and authentication techniques for iot devices on cloud. In: *2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*. [S.l.: s.n.], 2021. p. 1–6.

[Khalid *et al.* 2023] KHALID, M. *et al.* Towards sdn-based smart contract solution for iot access control. *Computer Communications*, v. 198, p. 1–31, 2023. ISSN 0140-3664. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0140366422004303>.

[Khan e Salah 2018] KHAN, M. A.; SALAH, K. Iot security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*, v. 82, p. 395–411, 2018. ISSN 0167-739X. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0167739X17315765>.

[Kimani, Oduol e Langat 2019] KIMANI, K.; ODUOL, V.; LANGAT, K. Cyber security challenges for iot-based smart grid networks. *International Journal of Critical Infrastructure Protection*, v. 25, p. 36–49, 2019. ISSN 1874-5482. Disponível em: <https://www.sciencedirect.com/science/article/pii/S1874548217301622>.

[Leszczyna 2021] LESZCZYNA, R. Review of cybersecurity assessment methods: Applicability perspective. *Computers Security*, v. 108, p. 102376, 2021. ISSN 0167-4048. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0167404821002005>.

[Li e Liu 2021] LI, Y.; LIU, Q. A comprehensive review study of cyber-attacks and cyber security; emerging trends and recent developments. *Energy Reports*, v. 7, p. 8176–8186, 2021. ISSN 2352-4847. Disponível em: <https://www.sciencedirect.com/science/article/pii/S2352484721007289>.

[Liao, Loures e Deschamps 2018] LIAO, Y.; LOURES, E. de F. R.; DESCHAMPS, F. Industrial internet of things: A systematic literature review and insights. *IEEE Internet of Things Journal*, v. 5, n. 6, p. 4515–4525, 2018.

[Mamdouh *et al.* 2021] MAMDOUH, M. *et al.* Authentication and identity management of ioht devices: Achievements, challenges, and future directions. *Computers Security*, v. 111, p. 102491, 2021. ISSN 0167-4048. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0167404821003151>.

[Minoli e Occhiogrosso 2018] MINOLI, D.; OCCHIOGROSSO, B. Blockchain mechanisms for iot security. *Internet of Things*, v. 1-2, p. 1–13, 2018. ISSN 2542-6605. Disponível em: <https://www.sciencedirect.com/science/article/pii/S2542660518300167>.

[Mohamad Noor e Hassan 2019] Mohamad Noor, M. binti; HASSAN, W. H. Current research on internet of things (iot) security: A survey. *Computer Networks*, v. 148, p. 283–294, 2019. ISSN 1389-1286. Disponível em: <https://www.sciencedirect.com/science/article/pii/S1389128618307035>.

[Mullet, Sondi e Ramat 2021] MULLET, V.; SONDI, P.; RAMAT, E. A review of cybersecurity guidelines for manufacturing factories in industry 4.0. *IEEE Access*, v. 9, p. 23235–23263, 2021.

[Nobre *et al.* 2019] NOBRE, J. *et al.* Segurança da informação para internet das coisas (iot): uma abordagem sobre a lei geral de proteção de dados (lgpd). *Revista Eletrônica de Iniciação Científica em Computação*, v. 17, n. 4, 2019. ISSN 1519-8219.

[Prathibha e Fatima 2018] PRATHIBHA, L.; FATIMA, K. Exploring security and authentication issues in internet of things. In: *2018 Second International Conference on Intelligent Computing and Control Systems (ICICCS)*. [S.l.: s.n.], 2018. p. 673–678.

[Roman, Zhou e Lopez 2013] ROMAN, R.; ZHOU, J.; LOPEZ, J. On the features and challenges of security and privacy in distributed internet of things. *Computer Networks*, v. 57, n. 10, p. 2266–2279, 2013. ISSN 1389-1286. Towards a Science of Cyber Security Security and Identity Architecture for the Future Internet. Disponível em: <https://www.sciencedirect.com/science/article/pii/S1389128613000054>.

[Romkey 2017] ROMKEY, J. Toast of the iot: The 1990 interop internet toaster. *IEEE Consumer Electronics Magazine*, v. 6, n. 1, p. 116–119, 2017.

[Schiller *et al.* 2022] SCHILLER, E. *et al.* Landscape of iot security. *Computer Science Review*, v. 44, p. 100467, 2022. ISSN 1574-0137. Disponível em: <https://www.sciencedirect.com/science/article/pii/S1574013722000120>.

[Sicari *et al.* 2015] SICARI, S. *et al.* Security, privacy and trust in internet of things: The road ahead. *Computer Networks*, v. 76, p. 146–164, 2015. ISSN 1389-1286. Disponível em: <https://www.sciencedirect.com/science/article/pii/S1389128614003971>.

[Singh, Rathore e Park 2020] SINGH, S. K.; RATHORE, S.; PARK, J. H. Blockiotintelligence: A blockchain-enabled intelligent iot architecture with artificial intelligence. *Future Generation Computer Systems*, v. 110, p. 721–743, 2020. ISSN 0167-739X. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0167739X19316474>.

[Suresh *et al.* 2014] SURESH, P. *et al.* A state of the art review on the internet of things (iot) history, technology and fields of deployment. p. 1–8, 2014.

[Tahsien, Karimipour e Spachos 2020] TAHSIEN, S. M.; KARIMIPOUR, H.; SPACHOS, P. Machine learning based solutions for security of internet of things (iot): A survey. *Journal of Network and Computer Applications*, v. 161, p. 102630, 2020. ISSN 1084-8045. Disponível em: <https://www.sciencedirect.com/science/article/pii/S1084804520301041>.

[Thabit *et al.* 2023] THABIT, F. *et al.* Cryptography algorithms for enhancing iot security. *Internet of Things*, v. 22, p. 100759, 2023. ISSN 2542-6605. Disponível em: <https://www.sciencedirect.com/science/article/pii/S2542660523000823>.

[Trabelsi, Fersi e Jmaiel 2023] TRABELSI, R.; FERSI, G.; JMAIEL, M. Access control in internet of things: A survey. *Computers Security*, v. 135, p. 103472, 2023. ISSN 0167-4048. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0167404823003826>.

[Xiao *et al.* 2018] XIAO, L. *et al.* Iot security techniques based on machine learning: How do iot devices use ai to enhance security? *IEEE Signal Processing Magazine*, v. 35, n. 5, p. 41–49, 2018.

[Yang *et al.* 2017] YANG, Y. *et al.* A survey on security and privacy issues in internet-of-things. *IEEE Internet of Things Journal*, v. 4, n. 5, p. 1250–1258, 2017.

[Zaman *et al.* 2021] ZAMAN, S. *et al.* Security threats and artificial intelligence based countermeasures for internet of things networks: A comprehensive survey. *IEEE Access*, v. 9, p. 94668–94690, 2021.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DA PARAÍBA
Campus Campina Grande
R. Tranqüilino Coelho Lemos, 671, Dinamérica, CEP 58432-300, Campina Grande (PB)
CNPJ: 10.783.898/0003-37 - Telefone: (83) 2102.6200

Documento Digitalizado Restrito

Entrega Final do TCC

Assunto:	Entrega Final do TCC
Assinado por:	Alex Araujo
Tipo do Documento:	Dissertação
Situação:	Finalizado
Nível de Acesso:	Restrito
Hipótese Legal:	Direito Autoral (Art. 24, III, da Lei no 9.610/1998)
Tipo do Conferência:	Cópia Simples

Documento assinado eletronicamente por:

- **Alex Rodrigues Araujo**, **ALUNO (202011210009) DE TECNOLOGIA EM TELEMÁTICA - CAMPINA GRANDE**, em 26/01/2024 14:13:39.

Este documento foi armazenado no SUAP em 26/01/2024. Para comprovar sua integridade, faça a leitura do QRCode ao lado ou acesse https://suap.ifpb.edu.br/verificar-documento-externo/ e forneça os dados abaixo:

Código Verificador: 1063440
Código de Autenticação: 09507ef644