CATÁLOGO DE VULNERABILIDADES DE SEGURANÇA EM SISTEMAS DE SOFTWARE IOT

Clinton Hudson Moreira Pessoa

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Engenharia de Sistemas e Computação, COPPE, da Universidade Federal do Rio de Janeiro, como parte dos requisitos necessários à obtenção do título de Mestre em Engenharia de Sistemas e Computação.

Orientador: Guilherme Horta Travassos

Rio de Janeiro
Junho de 2025

CATÁLOGO DEVULNERABILIDADES DE SEGURANÇA EM SISTEMAS DE SOFTWARE IOT

Clinton Hudson Moreira Pessoa

DISSERTAÇÃO SUBMETIDA AO CORPO DOCENTE DO INSTITUTO ALBERTO LUIZ COIMBRA DE PÓS-GRADUAÇÃO E PESQUISA DE ENGENHARIA DA UNIVERSIDADE FEDERAL DO RIO DE JANEIRO COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE MESTRE EM CIÊNCIAS EM ENGENHARIA DE SISTEMAS E COMPUTAÇÃO.

Orientador: Guilherme Horta Travassos

Aprovada por: Prof. Guilherme Horta Travassos
Prof. Cláudio Miceli de Farias
Prof. Lincoln Souza Rocha

RIO DE JANEIRO, RJ - BRASIL
JUNHO DE 2025

Pessoa, Clinton Hudson Moreira
Catálogo de Vulnerabilidades de Segurança em Sistemas de Software IoT/Clinton Hudson Moreira Pessoa. – Rio de Janeiro: UFRJ/COPPE, 2025.
XII, 182 p.: il.; 29,7 cm.
Orientador: Guilherme Horta Travassos
Dissertação (mestrado) – UFRJ/COPPE/Programa de Engenharia de Sistemas e Computação, 2025.
Referências Bibliográficas: p. 85 – 94.
1. Segurança. 2. Vulnerabilidade. 3. Internet das Coisas. 4. Engenharia de Software Baseada em Evidência. I. Travassos, Guilherme Horta. II. Universidade Federal do Rio de Janeiro, COPPE, Programa de Engenharia de Sistemas e Computação. III. Título.

Dedico este trabalho à minha família.

Agradecimentos

Nesse período em que fiz o mestrado, conheci e tive inúmeros contatos com excelentes pesquisadores e amigos que se tornaram especiais a mim.

Primeiramente, gostaria de agradecer ao meu orientador Guilherme Horta Travassos pela sua disponibilidade, por todas as conversas, oportunidades e paciência. Sou eternamente grato por tudo que fez.

Aos meus pais, José Jairo e Dorimar, e a meus irmãos Jéssica, Nataly, Cleize e Janelson por todo amor, carinho e apoio dado a mim, e por terem ficado ao meu lado quando tomei a decisão de sair de minha terra natal (Parintins-AM) para explorar outros horizontes!

Aos professores Claudio Miceli e Lincoln Rocha por aceitarem participar da minha banca e oferecerem valiosas contribuições.

Aos amigos que fiz desde a época da graduação e que estão comigo até hoje, Anna Thaís, Aline, Rodrigo e Sabrina. Gostaria de agradecer pela convivência e pela parceria de quase 9 anos.

Aos amigos que fiz ao ingressar no mestrado, Tales, Mariano e Vitor, parceiros nitidamente necessários para o início produtivo da pós. Aos amigos do laboratório, Larissa, André e Bruno. Obrigado pelo apoio, pela troca de experiência e pelas colaborações nas pesquisas que realizamos.

A toda equipe da secretaria do PESC e ao corpo docente da instituição pelo eficiente trabalho realizado. Ao próprio PESC pelo apoio financeiro dado a minha participação em eventos que possibilitaram a divulgação deste trabalho. Agradeço também à CAPES pelo apoio financeiro dado a mim, sem o qual este trabalho não poderia ter sido realizado.

Ter passado esse tempo como mestrando nessa instituição tão renomada foi uma experiência única. Aprendi muito, troquei ideias com pessoas incríveis e cresci bastante. Sou muito grato por tudo isso.

Resumo da Dissertação apresentada à COPPE/UFRJ como parte dos requisitos necessários para a obtenção do grau de Mestre em Ciências (M.Sc.)

CATÁLOGO DE VULNERABILIDADES DE SEGURANÇA EM SISTEMAS DE SOFTWARE IOT

Clinton Hudson Moreira Pessoa

Junho/2025

Orientador: Guilherme Horta Travassos

Programa: Engenharia de Sistemas e Computação

Apesar da popularidade dos sistemas de software IoT e da enorme variedade de dispositivos inteligentes, ainda existem desafios de segurança, considerando a escassez de descrições de práticas que possam apoiar a mitigação de riscos de segurança, o que aumenta as incertezas sobre as fragilidades que envolvem tais sistemas. Diante deste cenário, esta dissertação apresenta os resultados provenientes de dois estudos de literatura (*ad-hoc* e estruturado) com o objetivo de contribuir para a tomada de decisão quanto à mitigação de riscos associados a vulnerabilidades de segurança em sistemas de software IoT. Os resultados desses estudos foram organizados e consolidados em um Catálogo de Vulnerabilidades para Sistemas de Software IoT. O catálogo reúne um conjunto de informações que apoia a identificação e possíveis formas de mitigação das vulnerabilidades mapeadas. Ao todo foram identificadas 73 vulnerabilidades, classificadas em quatro categorias principais: Aplicação, Rede, Dispositivo e uma quarta categoria, até então pouco explorada em estudo similares, o *Peopleware*, que considera também o fator humano como elemento crítico na segurança desses sistemas.

Abstract of Dissertation presented to COPPE/UFRJ as a partial fulfillment of the requirements for the degree of Master of Science (M.Sc.)

SECURITY VULNERABILITIES CATALOGUE OF IOT SOFTWARE SYSTEMS

Clinton Hudson Moreira Pessoa

June/2025

Advisor: Guilherme Horta Travassos

Department: Computer Science and Systems Engineering

Despite the popularity of IoT software systems and the vast array of smart devices, security challenges persist, particularly due to the scarcity of documented practices that support the mitigation of security risks. This lack of guidance increases uncertainty regarding the vulnerabilities that affect such systems. In light of this scenario, this dissertation presents the findings of two literature studies (one ad-hoc and one structured) that support decision-making regarding mitigating security risks in IoT software systems. The results of these studies were organized and consolidated into a Vulnerability Catalog for IoT Software Systems. This catalog brings together information to support identifying and potential mitigation strategies for the mapped vulnerabilities. In total, 73 vulnerabilities were identified and classified into four main categories: Application, Network, Device, and a fourth category, *Peopleware*, which, unlike traditional studies, highlights the human factor as a critical element in the security of these systems.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

ABREVIAÇÕES

IoT - *Internet of Things* (Internet das Coisas)

OWASP - *Open Web Application Secutity Project*

NIST - *National Institute of Standards and Technology*

NVD - *National Vulnerability Database*

CVE - *Common Vulnerabilities and Exposures*

CWE – *Common Weakness Enumeration*

RFID - *Radio Frequency Identification*

ISO/IEC - *International Organization of Standardization / International Electrotechnical Commission*

QDAMiner - *Qualitative Data Analysis Software Package*

TCLE - Termo de Consentimento Livre e Esclarecido

1 Introdução

Neste capítulo são apresentadas a motivação e contexto para a realização deste trabalho, além dos objetivos e metodologia utilizada. E por fim, a organização dessa dissertação.

1.1 Contexto e Motivação

O paradigma da Internet das Coisas (IoT) tornou-se um elemento fundamental no planejamento e projeto de sistemas de software contemporâneos, permitindo a integração de dispositivos inteligentes em uma infraestrutura de rede abrangente que auxilia o desenvolvimento de sistemas de software modernos e melhora a capacidade perceptiva dos usuários humanos (SONG e GARCÍA-VALLS, 2022). No entanto, este potencial de crescimento contribui para que tais sistemas de software se tornem um dos principais alvos para os invasores explorarem no mundo cibernético, fornecendo-lhes os meios para acessar dispositivos conectados à rede (SIBONI *et al*., 2019; BOCHIE *et al.*, 2020).

A proteção dos ambientes IoT é uma tarefa desafiadora. Ao observamos o impacto dos aspectos de segurança nos dispositivos IoT, por serem usualmente construídos em tamanho pequeno e possuírem recursos inerentemente limitados (ou seja, bateria, processamento e armazenamento), a implementação de mecanismos de segurança convencionais torna-se desafiadora e, algumas vezes, inviável, pois requer um processo muito mais complexo e difícil (HARBI *et al.*, 2019).

Portanto, garantir a segurança e a privacidade têm sido uma preocupação nos sistemas de software nos últimos anos devido ao alto risco promovido pelos ambientes IoT em relação à falta inerente de segurança e de mecanismos para mitigá-la nos dispositivos IoT (ABDALLA e VAROL, 2020). O atributo segurança em sistemas de software IoT requer cuidados redobrados, uma vez que tais sistemas lidam com dados coletados e compartilhados por diferentes dispositivos, que normalmente capturam diversos tipos de informações (KHAN e SALAH, 2018). Além disso, é preciso estar atento à fragilidade e aos perigos que espreitam a rede, gerando inúmeras novas ameaças e evidenciando vulnerabilidades que os sistemas de software convencionais também enfrentam. No entanto, a compreensão das vulnerabilidades da IoT permite antecipar as

ameaças e conceber estratégias de mitigação para minimizar, por exemplo, os riscos de intrusão ou de roubo de dados (DAVIS *et al.*, 2020).

Neste sentido, é essencial reconhecer que, embora muitas das vulnerabilidades identificadas na IoT se assemelhem às encontradas nos sistemas de software tradicionais, as caraterísticas únicas dos ambientes IoT amplificam frequentemente esses riscos. A natureza interconectada dos dispositivos IoT, as diversas funcionalidades e as limitações de recursos introduzem complexidades que exigem considerações de segurança especializadas (AMMAYAPPAN *et al.*, 2020; GROMOV *et al.*, 2022). Por tanto, embora algumas vulnerabilidades possam transcender tanto os sistemas de software tradicionais como os da IoT, o contexto em que se manifestam nos ecossistemas da IoT exige estratégias adaptadas para as resolver eficazmente (GROMOV *et al.*, 2022).

O desenvolvimento de sistemas de software IoT por nossa equipe de engenharia de software revelou todas essas questões e desafios para garantir a segurança dos sistemas construídos. Entre muitos outros desafios envolvidos na engenharia de sistemas de software IoT (DA SILVA *et al.*, 2020), a falta de informações claras sobre vulnerabilidades de segurança relacionadas a esses sistemas de software modernos compromete a tomada de decisões em projetos de software industrial. Portanto, para preencher esta lacuna crítica de informação sobre sistemas de software IoT e responder às preocupações sobre as vulnerabilidades de segurança dentro das suas camadas de construção, esta pesquisa pretende identificar e categorizar as vulnerabilidades de segurança IoT conhecidas e evidenciadas tanto na literatura técnica quanto na acadêmica, fornecendo assim um conjunto baseado em evidências de informações, organizadas em um catálogo de vulnerabilidades, para apoiar os profissionais de software na decisão sobre a mitigação de riscos em seus projetos de software IoT, promovendo assim, a disseminação de boas práticas, a sistematização do conhecimento disperso na literatura e contribuindo para a construção de sistemas de software IoT mais seguros diante das ameaças crescentes.

Além disso, a abordagem adotada para a identificação desse conjunto de vulnerabilidades compreende uma visão ampla da segurança em sistemas de software IoT, considerando tanto os aspectos relacionados à infraestrutura, como rede,

comunicação e dispositivos, quanto elementos relacionados ao software, como aplicações, falhas no código, entre outros. Além disso, contempla também o fator humano, que se insere na complexidade desses ambientes, uma vez que as vulnerabilidades podem surgir em diferentes níveis.

1.2 Problema e Questão de Pesquisa

Com o crescimento exponencial e a proliferação de dispositivos IoT em diversos setores, aspectos como segurança em sistemas IoT passaram a ter uma visibilidade ainda maior, considerando as ameaças emergentes e os riscos associados à exploração de muitas das vulnerabilidades que permeiam esses sistemas (CARLOS e MATTOS, 2021; SEVERI, 2024).

Atualmente, ainda não foi possível identificar uma solução "padronizada" disponível que ofereça os requisitos de segurança necessários para o desenvolvimento de sistemas de software IoT, devido à flexibilidade com que esses sistemas se adaptam e diversificam (KORONA *et al.*, 2023). Portanto, compreender os principais pontos de vulnerabilidade nesses sistemas pode contribuir significativamente para mitigar muitos dos riscos mais comuns associados a eles.

Diante desse cenário, profissionais da indústria e pesquisadores têm buscado investigar ou adaptar estratégias para melhorar a segurança de sistemas de software IoT e garantir maior proteção para o produto final, por meio do uso de abordagens focadas nas vulnerabilidades de segurança ou ameaças inerentes a esses ambientes (LI, 2024). Exemplos dessas abordagens incluem o uso de listas de vulnerabilidades mapeadas e conduzidas por organizações, tais como OWASP, NIST ou CVE.

É importante identificar e mitigar as vulnerabilidades de segurança de forma ágil, utilizando abordagens estruturadas e reconhecidas, para garantir a segurança e atender às expectativas de construção de sistemas de software IoT para mitigação de riscos. Assim, a principal questão de pesquisa desta proposta de estudo é:

"*Quais vulnerabilidades de segurança afetam e podem ser identificadas em sistemas de software IoT?*"

Para responder esta questão de pesquisa, a proposta deste trabalho consiste no desenvolvimento de um catálogo de vulnerabilidades de segurança, que apoiará tanto profissionais da prática quanto pesquisadores da área a identificar, avaliar e mitigar riscos de segurança em sistemas de software IoT de maneira mais eficiente e estruturada.

1.3 Objetivo

Este trabalho visa identificar as vulnerabilidades de segurança em sistemas de software IoT, na busca de apresentar um conjunto de vulnerabilidades que estabeleça relação com as problemáticas de segurança inerentes a esse tipo de sistema, de forma a apoiar a identificação e prevenção à possíveis ameaças, auxiliando assim pesquisadores e profissionais da área.

Dessa forma, este trabalho vem como um esforço inicial de realizar uma investigação em torno das fraquezas de segurança que os sistemas de software IoT detém, tanto a nível organizacional quanto acadêmico. Para apoiar este estudo, é necessário que os seguintes objetivos específicos sejam contemplados:

- Conduzir uma pesquisa com foco nas vulnerabilidades de segurança identificadas e definidas por organizações que demandam e utilizam de sistemas de software e dispositivos IoT.
- Buscar identificar as vulnerabilidades de segurança em sistemas de software e dispositivos IoT segundo estudos vinculados à literatura técnica.
- Apresentar um conjunto de vulnerabilidades de segurança em sistema IoT com as principais problemáticas identificadas através da mesclagem dos resultados mapeados tantos pelas organizações quanto pela literatura técnica.
- Construir um catálogo de vulnerabilidades de segurança para sistemas IoT com informações sobre as vulnerabilidades e possíveis formas de mitigação.
- Avaliar experimentalmente o catálogo com profissionais da prática.

1.4 Metodologia

A proposta de método de desenvolvimento aplicada neste estudo é uma combinação de dois estudos de literatura, uma revisão da literatura *Ad-hoc* e uma revisão estruturada da literatura, apoiadas por diretrizes associadas aos estudos utilizados, seguido pela construção e validação de um Catálogo de Vulnerabilidades de Segurança em Sistemas de Software IoT.

Para a aplicação da revisão da literatura *Ad-hoc*, a adaptação da pesquisa foi baseada em Silva (2019), enquanto a revisão da estruturada da literatura teve embasamento nos estudos de Kuhrmann *et al.* (2017). Ambos os métodos foram planejados e executados com o objetivo de identificar e classificar vulnerabilidades de segurança em sistemas de software IoT. Após essa etapa, foi conduzida a organização de um corpo de conhecimento, materializado em um catálogo de vulnerabilidades baseado nas descobertas dos estudos. Por fim, foi realizado um estudo de viabilidade, com o propósito de avaliar a organização e utilidade do catálogo junto a profissionais da área. A Figura 1 mostra as etapas de investigação aplicados para este estudo.

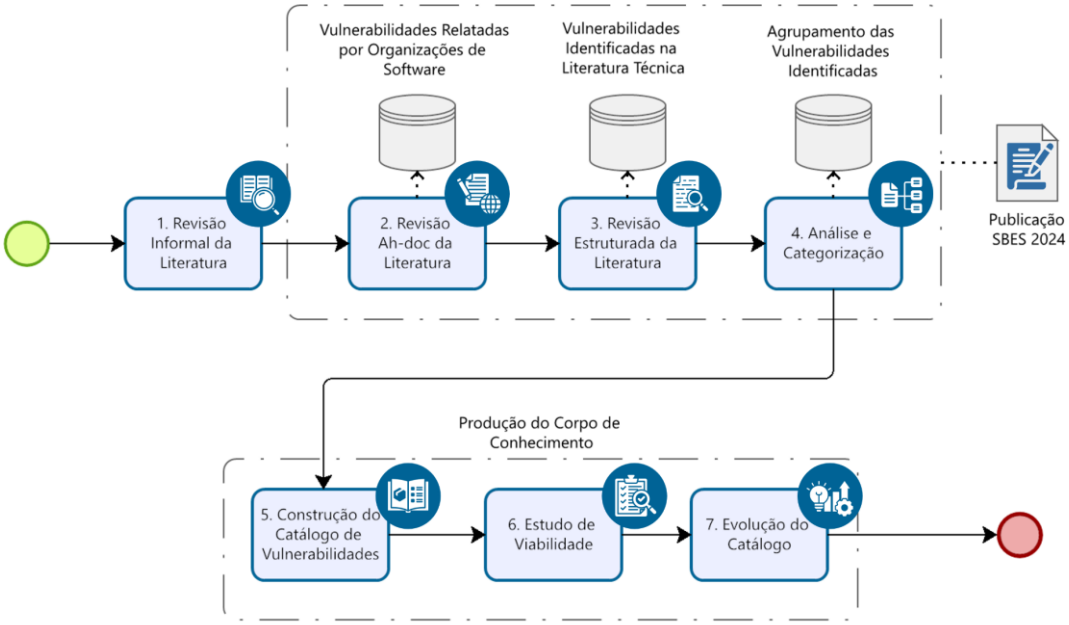


Figura 1: Metodologia de Pesquisa.

[1] Revisão Informal da Literatura: Este método é uma abordagem informal que consiste em compreender os principais conceitos de uma linha de pesquisa e

identificar uma lacuna que ainda não coberta por pesquisas científicas. Normalmente, ações seguidas não são documentadas ou sistematizadas. Os termos investigados na literatura abordaram sobre as questões de segurança em sistema de software IoT, com destaque as vulnerabilidades encontradas nesses ambientes.

[2] Revisão da Literatura *Ad-hoc*: Esta etapa consistiu na realização de um estudo de literatura *Ad-hoc* voltado em compreender e identificar vulnerabilidades de segurança em sistemas de software IoT, utilizando de informações disponibilizadas em sites por organizações especializadas no tema, permitindo obter uma estrutura base acerca das vulnerabilidades de segurança que permeiam esses sistemas.

[3] Revisão Estruturada da Literatura: Esta etapa consistiu na realização de um estudo de literatura voltado para identificar vulnerabilidades de segurança em sistemas de software IoT utilizando de informações da própria literatura técnica. Permitiu ainda a aplicação de estratégias que apoiaram a classificação das vulnerabilidades em grupos específicos.

[4] Análise e Categorização das Vulnerabilidades de Segurança: Nesta etapa são apresentados os métodos e critérios utilizados para analisar e categorizar as vulnerabilidades de segurança em sistemas de software IoT identificadas neste trabalho. Foram organizadas em categorias específicas que refletem a estrutura base dos sistemas de software IoT, com o objetivo de facilitar sua compreensão e apoiar na elaboração de estratégias de mitigação eficazes a depender do contexto.

[5] Construção do Catálogo de Vulnerabilidades de Segurança: Com base nos resultados do estudo, esta etapa descreve o processo de identificação e organização das vulnerabilidades de segurança encontradas em sistemas de software IoT em um catálogo, fornecendo um artefato como base de conhecimento para desenvolvedores e pesquisadores acerca da mitigação dos riscos associadas às vulnerabilidades.

[6] Estudo de Viabilidade: Avaliar o uso do catálogo construído e descrever os resultados obtidos em sua utilização como fonte base de informações sobre vulnerabilidades de segurança em sistemas de software IoT.

[7] Evolução do Catálogo de Vulnerabilidades de Segurança: Descreve as melhorias adquiridas por meio das sugestões dos participantes do estudo de viabilidade e como foram aplicadas à versão final do artefato.

1.5 Contribuições e Publicações

Diferentes contribuições podem ser observadas com a leitura dessa dissertação. De forma objetiva, as principais contribuições podem ser apresentadas como:

- Um conjunto de vulnerabilidades de segurança descritas na literatura técnica e evidenciadas por organizações que fazem uso da tecnologia IoT.
- Indicação dos problemas de segurança mais comuns que permeiam o domínio de sistemas de software IoT, baseados na comparação entre os resultados identificados nos estudos de revisão da literatura (*Ad-hoc* e Estruturado).
- Acesso a um conjunto geral de vulnerabilidades de segurança, por meio de um catálogo, que permitirá aos profissionais e estudantes da área desenvolver sistemas de software IoT aplicando estratégias de segurança direcionada a solucionar problemas previamente evidenciados.
- Desenvolvimento de um pacote experimental com o objetivo de avaliar a organização, usabilidade e aplicabilidade do catálogo, possibilitando a coleta de feedbacks de profissionais da área. Através de questionários e a combinação das respostas tanto das análises quantitativas quanto das qualitativas, foi possível validar a consistência das informações apresentadas no catálogo, além de identificar oportunidades de aprimoramento em sua estrutura e apresentação.

Ao longo da realização desse trabalho, tivemos uma publicação diretamente relacionada ao conteúdo do catálogo de vulnerabilidades de segurança:

- **PESSOA, Clinton Hudson Moreira**; TRAVASSOS, Guilherme Horta. **Categorizing IoT Software Systems Security Vulnerabilities Through Literature Studies**. *In*: SIMPÓSIO BRASILEIRO DE ENGENHARIA DE SOFTWARE (SBES), 2024, Curitiba/PR. Porto Alegre: Sociedade Brasileira de Computação, 2024. p. 169-180. DOI: https://doi.org/10.5753/sbes.2024.3346

Adicionalmente, a participação em disciplinas e atividades de projetos de pesquisa permitiu que experiências adicionais fossem discutidas, das quais se destacam:

- NASCIMENTO, Luciana; GALENO, Larissa; **PESSOA, Clinton Hudson**; SILVA, Patricia Furtado; TRAVASSOS, Guilherme Horta. **Uso de *Technology Probe* na Engenharia de Sistemas de Software para Saúde**. In: CONGRESSO IBERO-AMERICANO EM ENGENHARIA DE SOFTWARE (CIBSE), 2024, Curitiba/PR. Porto Alegre: Sociedade Brasileira de Computação, 2024. p. 211-225. DOI: https://doi.org/10.5753/cibse.2024.28449
- Paes, Vítor de Castro; **Pessoa, Clinton Hudson Moreira**; Pagliusi, Rodrigo Pereira; Barbosa, Carlos Eduardo; Argôlo, Matheus; Lima, Yuri Oliveira; Salazar, Herbert; Lyra, Alan and Jano Moreira de Souza. **Analyzing the Challenges for Future Smart and Sustainable Cities**. 2023. Sustainability 15, no. 10: 7996. https://doi.org/10.3390/su15107996
- Paes, Vitor C.; **Pessoa, Clinton H.**; Costa, Viviane C.; Oliveira, Luiz F. and Souza, Jano M. **IoE Knowledge Flow Model in Smart Cities**. 2022 IEEE International Conference on Systems, Man, and Cybernetics (SMC), Prague, Czech Republic, 2022, pp. 982-987, doi: 10.1109/SMC53654.2022.9945275
- PARREIRAS, Marcus; **PESSOA, Clinton H. M**.; PAIVA, Tales M.; LIMA, Yasmin Barbosa; XEXÉO, Geraldo. **Batalha das Lendas: Uma proposta de jogo de tabuleiro para valorização cultural do folclore brasileiro**. In: TRILHA DE ARTES & DESIGN – ARTIGOS CURTOS - SIMPÓSIO BRASILEIRO DE JOGOS E ENTRETENIMENTO DIGITAL (SBGAMES). 2022, Natal/RN. Porto Alegre: Sociedade Brasileira de Computação, 2022. p. 263-267. DOI: https://doi.org/10.5753/sbgames_estendido.2022.226068

1.6 Organização do Texto

Esta dissertação está organizada em outros cinco capítulos, além deste primeiro que descreveu a introdução, motivação e o contexto no qual essa dissertação está inserida. A organização desse trabalho segue a estrutura abaixo:

Capítulo 2 – Fundamentação Teórica*:* são apresentados conceitos sobre o Internet das Coisas, Segurança e Vulnerabilidades de Segurança em Sistemas de Software IoT. Além disso, são apresentados os trabalhos relacionados a esta pesquisa.

Capítulo 3 – Categorizando Vulnerabilidades de Segurança de Sistemas de Software de IoT: Apresenta os estudos aplicados na identificação das vulnerabilidades de segurança em sistemas de software IoT, que permitiram evoluir o conjunto de dados, conteúdo principal do catálogo, objeto final deste trabalho.

Capítulo 4 – Catálogo de Vulnerabilidades de Segurança em Sistemas de Software IoT: Descreve a construção do catálogo de vulnerabilidades de segurança, com a identificação e organização das informações de descrição e mitigações para cada uma das vulnerabilidades evidenciadas nos estudos de revisão de literatura realizados.

Capítulo 5 – Estudo de Viabilidade do Catálogo de Vulnerabilidades de Segurança IoT: Apresenta os resultados obtidos dos participantes do estudo de viabilidade do uso do catálogo, incluindo as suas observações e refinamentos necessários.

Capítulo 6 – Conclusão: Apresenta as conclusões e contribuições desse trabalho, suas limitações, além de sugerir perspectivas futuras da pesquisa.

2 Fundamentação Teórica

Neste capítulo, fornecemos uma visão geral dos principais conceitos relacionados para o melhor entendimento da pesquisa, e os trabalhos relacionados.

2.1 Internet das Coisas

O termo Internet das Coisas (ou "*Internet of Things* - IoT") teve sua denominação atribuída por Kevin Ashton (1999), cofundador do *Auto-ID Center do Massachusetts Institute of Technology* (MIT). Em 2009, Ashton afirmou que a ideia original da IoT previa a conexão de todos os objetos físicos à Internet, atribuindo assim a capacidade de capturar informações por meio de identificação por radiofrequência (RFID) e tecnologias de sensoriamento, que permitiriam observar, identificar e compreender o mundo independentemente da atividade humana direta e suas limitações de tempo, atenção e precisão (LACERDA e LIMA-MARQUES, 2015).

O conceito de IoT ganhou destaque com a evolução da miniaturização de componentes eletrônicos, o avanço de tecnologias de comunicação como 5G e Wi-Fi de baixa potência e a expansão do processamento em nuvem e em borda (*edge computing*) (EJAZ *et al.*, 2016). Esses fatores permitiram a criação de dispositivos acessíveis, altamente conectados e capazes de operar em redes distribuídas, fomentando sua adoção em larga escala (VILLAMIL *et al.*, 2020).

Neste sentido, o paradigma da Internet das Coisas compreende tecnologias inteligentes que influenciam nossas vidas, fornecendo dispositivos inteligentes projetados para compartilhar informações, dados e recursos para atender às necessidades das pessoas (ATZORI *et al.*, 2010). Ele permite a composição de sistemas de software a partir de objetos exclusivamente endereçáveis (as coisas), como leitores de impressão digital, sistemas de detecção de gases, dispositivos de monitoramento de temperatura, sistemas de detecção de movimento e câmeras de vigilância residencial, entre muitos outros, que são equipados com dispositivos de identificação, detecção ou comportamentos de atuação e capacidades de processamento. Portanto, essas coisas podem se comunicar e cooperar para atingir um objetivo (MOTTA[1] *et al.*, 2019). Elas se comunicam entre si para diversos fins. Em uma casa inteligente, por exemplo, podem auxiliar na otimização do consumo

de energia, na redução de custos nas contas e na garantia da segurança dos ocupantes (ALDAHMANI *et al.*, 2023).

A arquitetura básica da Internet das Coisas é geralmente estruturada em camadas, que organizam os processos desde a coleta de dados até sua utilização em aplicações inteligentes. A modelagem clássica da IoT contempla três camadas principais: a camada de percepção, a camada de rede e a camada de aplicação (ATZORI *et al.*, 2010). A camada de percepção é responsável por identificar, coletar e capturar dados do ambiente físico por meio de sensores, atuadores, dispositivos RFID, câmeras e outros elementos. Já a camada de rede tem a função de transmitir esses dados, conectando os dispositivos aos centros de processamento, seja na nuvem, na borda ou em servidores locais, utilizando diversas tecnologias de comunicação, como Wi-Fi, 4G/5G, Zigbee, LoRaWAN e Bluetooth (GUBBI *et al.*, 2013). Por fim, a camada de aplicação oferece os serviços e funcionalidades que atendem às necessidades dos usuários, como automação residencial, monitoramento remoto, sistemas inteligentes de transporte, saúde conectada, entre outros (XU *et al.*, 2014). Além desse modelo clássico, algumas abordagens incluem camadas adicionais, como a camada de processamento ou camada de serviços, que intermedeiam a análise, o armazenamento e a tomada de decisão, especialmente no contexto de computação em nuvem, névoa (*fog computing*) e borda (*edge computing*) (KHAN et al., 2019). A compreensão dessa arquitetura é fundamental, pois cada uma dessas camadas apresenta requisitos específicos de segurança e privacidade, os quais impactam diretamente na proteção dos sistemas de software IoT.

A IoT oferece uma ampla gama de aplicações que impactam setores essenciais da sociedade. No campo da saúde, dispositivos vestíveis monitoram sinais vitais e fornecem dados em tempo real para médicos e pacientes, permitindo diagnósticos mais precisos e cuidados personalizados. Em cidades inteligentes, sensores ajudam a gerenciar o tráfego, a reduzir o consumo de energia e a melhorar a segurança pública. Na indústria, a IoT impulsiona a automação e a análise preditiva, permitindo a identificação antecipada de falhas em máquinas e a otimização de processos produtivos. No setor agrícola, sensores de umidade e temperatura ajudam na gestão eficiente de recursos, promovendo a sustentabilidade (ONGUN *et al.*, 2018; VILLAMIL *et al.*, 2020).

Figura 2: Internet das Coisas.

Fonte: Revista Segurança Eletrônica (RIGATIERI, 2018).

No entanto, com este sucesso crescente, muitos problemas críticos de segurança em sistemas de software IoT surgiram como uma ameaça. Uma vez que se prevê que cerca de 24 bilhões de dispositivos deverão estar em linha no domínio público até 2025, várias vulnerabilidades de segurança podem ser susceptíveis a ataques, que conduzem a problemas graves se estes sistemas de software não estiverem devidamente protegidos ou configurados. Adicionalmente, vários dispositivos interligados coletam informações pessoais, tais como nome, data de nascimento, morada, dados do cartão de crédito etc. (ARORA *et al.*, 2019; PAES *et al.*, 2022), tornando a privacidade uma grande preocupação.

Por isso, a implantação da comunicação automática entre objetos em nossas vidas representa um perigo para o nosso futuro, pois de fato, sem serem vistas pelos usuários, as etiquetas RFID incorporadas em nossos dispositivos pessoais, roupas e mantimentos podem, sem saber, ser acionadas para responder com sua identificação e outras informações. Isso potencialmente permite um mecanismo de vigilância oculto que permearia grandes partes de nossas vidas (BELLI, 2020; ATZORI *et al.*, 2010). A interconexão massiva de dispositivos cria uma vasta superfície de ataque, expondo sistemas de software IoT a riscos que podem comprometer não apenas informações sensíveis, mas também a operação de infraestruturas críticas (LIU *et al.*, 2019; BROWN e KETEL, 2020).

2.2 Segurança em sistemas de software IoT

A segurança é um dos pilares principais e um dos maiores desafios para os sistemas de software da IoT. À medida que o número de dispositivos conectados aumenta, a probabilidade de explorar vulnerabilidades de segurança também cresce. As organizações se esforçam para mitigar violações de segurança implantando ferramentas eficazes para proteger seus sistemas contra-ataques digitais, visando prevenir, detectar e relatar ataques usando tecnologias de ponta e melhores práticas (ZANON *et al.*, 2022; TORRE *et al.*, 2023).

Figura 3: Segurança em Sistemas de Software.

Fonte: Hacker Cibercriminoso (FREEP!K, 2024).

A segurança em sistemas de software IoT é especialmente desafiadora devido às suas características singulares. Muitos dispositivos IoT são projetados para cumprir funções específicas com recursos limitados, o que muitas vezes exclui a implementação de soluções robustas de segurança (PRAKASH *et al.*, 2024). Em dispositivos de baixo custo, por exemplo, devido a fluxos de dados incompletos e hardware extremamente limitado, as chances de roubo de dados aumentam, afetando diretamente a segurança e o bem-estar das pessoas que os utilizam (YADAV *et al.*, 2018). Adicionalmente, a interconexão de dispositivos de diferentes fabricantes, com padrões e capacidades heterogêneas, aumenta a complexidade em se criar um ecossistema efetivamente protegido (WATSON *et al.*, 2017; SONI *et al.*, 2023).

Muitas infraestruturas críticas, incluindo redes elétricas inteligentes, transporte inteligente, infraestrutura crítica, transporte aéreo, resposta a emergências e cuidados com

a saúde, dependem de sistemas ciberfísicos. No entanto, as vulnerabilidades de segurança nesses sistemas são altamente graves (KOZIOLEK, 2011; SHEIKH e SINGH, 2022). Por exemplo, um ataque de segurança cibernética tem como objetivo obter acesso não autorizado a um dispositivo, aplicação ou rede de computadores com a intenção de causar danos (ALDAHMANI *et al.*, 2023; TORRE *et al.*, 2023). É devido a esses tipos de violações de segurança que existem vários desafios de implementação a serem considerados nos sistemas de software da IoT, incluindo, principalmente, características associadas à prevenção de divulgação, engano e interrupções para garantir elementos relacionados aos pilares fundamentais da segurança: confidencialidade, integridade e disponibilidade de dados (BARISIC e CUNHA, 2017).

A garantia de segurança em sistemas de software IoT não é apenas uma questão técnica, mas também estratégica, dado o impacto potencial de vulnerabilidades nesses sistemas. Além de proteger informações e infraestruturas, a segurança em IoT é essencial para manter a confiança dos usuários, promover a adoção de novas tecnologias e evitar consequências catastróficas em setores críticos, como saúde, transporte e energia (ONGUN *et al.*, 2018; LI, 2024).

2.3 Vulnerabilidades de segurança em sistemas de software IoT

Uma vulnerabilidade de segurança pode ser definida como a fraqueza de um ativo ou mecanismo de segurança que uma ou mais ameaças podem explorar. Pode resultar de uma falha de projeto ou defeito de implementação, permitindo que um invasor cause danos às partes interessadas desse ativo, conforme descrito pela ISO/IEC 27000 (2018). As partes interessadas incluem o proprietário, usuários, atores e coisas que dependem do sistema de software. O termo “vulnerabilidade” é frequentemente usado de forma muito genérica quando mesclado com os termos “ameaça” ou “ataque” (OWASP, 2016). Ao contrário do conceito aplicado ao termo “vulnerabilidade”, “ameaça” é definida como a causa potencial de um incidente indesejado que provavelmente resultará em danos a um sistema de software ou organização. Por outro lado, um “ataque” é a tentativa de destruir, expor, alterar, roubar ou obter acesso não autorizado a um ativo (ISO/IEC, 2018).

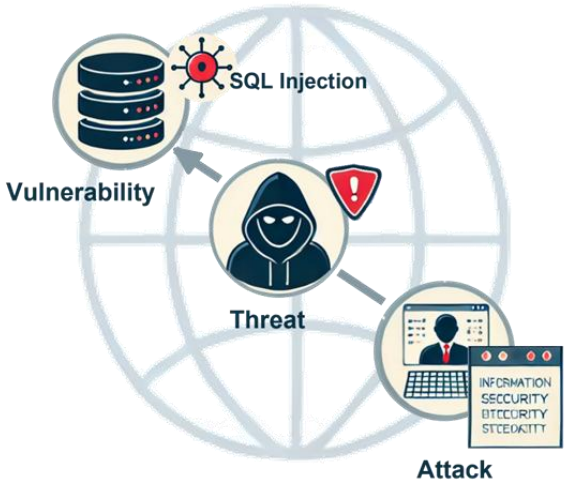


Figura 4: Vulnerabilidade x Ameaça x Ataque.

Fonte: o autor (2024).

Dada a crescente descoberta e exploração de vulnerabilidades, tem havido um aumento significativo na investigação sobre detecção e mitigação de vulnerabilidades de segurança em ambientes IoT, resultando em muitos artigos acadêmicos e artigos de pesquisa abordando os desafios de segurança da IoT (ABDALLA e VAROL, 2020; DAVIS *et al.*, 2020; KARIRI, 2022; ALFADEL *et al.*, 2023). Isto se deve à importância da avaliação de riscos de segurança e ao desenvolvimento de novas estratégias de segurança aplicadas a vulnerabilidades em sistemas de software IoT (BAHO *et al.*, 2023). Além disso, estudar como as vulnerabilidades de segurança se propagam, são descobertas e corrigidas ajuda a fortalecer a saúde do ecossistema do sistema de software IoT, uma vez que o atraso entre a descoberta da vulnerabilidade ou o lançamento da sua correção pode expor os ativos a ameaças e aumentar a probabilidade de exploração (ALFADEL *et al.*, 2023).

Com base nestes estudos, podemos considerar diferentes tipos de vulnerabilidades de segurança que podem surgir, como:

- *Phishing*, ocorre quando indivíduos mal-intencionados manipulam mensagens de e-mail para induzir os destinatários a abri-las, muitas vezes com a intenção de induzi-los a revelar informações confidenciais (SAHMI *et al.*, 2019; DAVIS *et al.*, 2020; ZHAO *et al.*, 2020).

- Falta de autenticação forte, muitos dispositivos IoT ainda utilizam métodos de autenticação inadequados, como senhas padrão ou fracas, que podem ser facilmente explorados por atacantes. Em alguns casos, nem mesmo existe um sistema de autenticação, permitindo acesso irrestrito a dispositivos sensíveis (ROOHI *et al.*, 2019; TOMUR *et al.*, 2021; KARIE *et al.*, 2021).
- Injeção em Banco de Dados (SQL, código e afins), ocorre quando código malicioso é inserido em servidores utilizando linguagens de programação como SQL, com o objetivo de fazer com que o servidor divulgue dados confidenciais ou execute ações não intencionais (XU *et al.*, 2017; SOOKHAK *et al.*, 2019; ZHAO *et al.*, 2020).
- Comunicações Inseguras, a troca de informações entre dispositivos IoT frequentemente ocorre sem o uso de protocolos de segurança robustos. Dados são transmitidos em texto claro, tornando-os suscetíveis a interceptações em ataques (PANCHAL *et al.*, 2018; SHAH e SENGUPTA, 2020; KARIE *et al.*, 2021).

Estas são apenas algumas das vulnerabilidades de segurança que podem surgir em sistemas de software IoT. Portanto, é crucial compreender e abordar estas e outras vulnerabilidades para garantir a segurança e integridade dos sistemas de software IoT.

As vulnerabilidades de segurança em ambientes IoT representam uma ameaça significativa tanto para usuários individuais quanto para organizações e governos (MENEGHELLO *et al.*, 2019). É crucial que a segurança seja tratada como uma prioridade, incorporando práticas que promovam a proteção dos sistemas e a conscientização entre desenvolvedores e usuários.

A identificação, categorização e disseminação de informações sobre vulnerabilidades são práticas fundamentais para a segurança de sistemas de software. Iniciativas como o *Common Vulnerabilities and Exposures* (CVE), mantido pela *MITRE Corporation*, e *o National Vulnerability Database* (NVD), mantido pelo *National Institute of Standards and Technology* (NIST), desempenham importantes papéis nesse contexto. O CVE provê um identificador único para vulnerabilidades conhecidas, enquanto o NVD complementa esses registros com informações adicionais, como

métricas de severidade (via CVSS), impactos, referências e soluções. Esses repositórios auxiliam nos processos de gerenciamento de vulnerabilidades, mitigação de riscos e desenvolvimento de sistemas mais seguros (NIST, 2025; MITRE, 2025).

2.4 Trabalhos Relacionados

Esta seção apresenta estudos que visam identificar vulnerabilidades de segurança nos sistemas de software IoT. Cada estudo contribui de forma importante para o tema, produzindo resultados com ideias semelhantes às do nosso trabalho, ao abordar diversos cenários e apresentar as suas conclusões de forma clara e objetiva.

Davis *et al.* (2020) discutem os problemas da adoção de tecnologias IoT e a consequente necessidade de segurança, tornando muitos destes dispositivos vulneráveis a ataques. No seu estudo, os autores analisam a vulnerabilidade e a postura de segurança dos dispositivos IoT utilizados em casas inteligentes. O estudo começa com uma revisão da literatura sobre estudos conhecidos de vulnerabilidade de segurança dos dispositivos IoT, considerando quatro categorias de ataques: 1) físico, 2) de rede, 3) de software e 4) de encriptação. A seguir, são realizados estudos experimentais que comparam as posturas de segurança entre fornecedores de dispositivos conhecidos e menos conhecidos. Os autores concluem que os ataques físicos, de rede, de software e/ou de encriptação são viáveis para vários dispositivos IoT. Além disso, com base nos seus estudos de vulnerabilidade de segurança, os autores concluem que a postura de segurança dos dispositivos mais conhecidos é mais forte do que a dos menos conhecidos.

No trabalho de Chhetri e Motti (2021), os autores centram-se nas disposições de segurança e privacidade aplicáveis aos dispositivos domésticos inteligentes. Eles adotam uma abordagem sistemática para identificar, analisar e categorizar as vulnerabilidades de segurança destes ambientes. O estudo produziu 153 vulnerabilidades de segurança, organizadas em categorias com base no local de ocorrência ou no componente da arquitetura da casa inteligente, por exemplo, dispositivo, protocolo, gateway, rede e arquitetura de software. Os autores esperam que os resultados possam beneficiar outros investigadores com uma análise abrangente e uma categorização sistemática das vulnerabilidades das casas inteligentes.

Pedreira *et al.* (2021) analisaram as vulnerabilidades, os ataques e as defesas de segurança na Indústria 4.0. A sua revisão apresenta artigos sobre estes três tópicos

principais (vulnerabilidades de segurança, defesas e ataques) ou a sua intersecção. As vulnerabilidades identificadas foram classificadas em quatro categorias: aplicações Web, dispositivos, redes e autenticação. Para cada categoria, são apresentados alguns dos tipos de vulnerabilidade associados. Os resultados deste estudo mostram também que o número de artigos centrados nas vulnerabilidades de segurança é relativamente baixo em comparação com os que se centram nos ataques e nas defesas. Em suma, o estudo fornece informações sobre o estado atual da investigação sobre vulnerabilidades de segurança na Indústria 4.0 e destaca a necessidade de mais investigação.

Nos trabalhos mencionados nesta seção, tal como no nosso estudo, é crucial examinar e identificar um conjunto adequado de vulnerabilidades de segurança que afetam os sistemas de software IoT, utilizando estudos da literatura. No entanto, nos destacamos pela adoção de abordagens específicas para categorizar as vulnerabilidades de segurança, o que nos permitiu a identificação e introdução de uma nova categoria até então não mencionada em outros trabalhos, a do "*Peopleware*". Ao contrário de outros trabalhos, nos concentramos na identificação de pontos fracos estritamente definidos como vulnerabilidades de segurança, distintos de ameaças ou ataques, em conformidade com as normas ISO/IEC 27000. Entendemos que esta abordagem proporciona uma visão mais transparente e direcionada sobre os desafios a enfrentar e a mitigar nos sistemas de software IoT.

2.5 Considerações Finais

Este capítulo apresentou a revisão bibliográfica executada em busca dos conceitos dos tópicos principais relacionados a esta dissertação e os trabalhos relacionados.

O primeiro tópico dos conceitos buscou contextualizar sobre a transformação tecnológica englobada no uso da abordagem de Internet das Coisas, revolucionando desde o cotidiano das pessoas até operações em setores mais críticos como saúde, transporte e indústria.

Com o segundo tópico buscamos apresentar o impacto que aspectos como segurança possuem nos cenários IoT, dada a crescente integração desses sistemas com infraestruturas críticas e com o cotidiano das pessoas, sendo necessário desenvolver soluções e práticas cada vez mais eficazes.

Já no terceiro, abordamos o conceito central deste estudo, apontando a problemática envolvendo as vulnerabilidades de segurança para com os sistemas de software IoT. Além de incluir de forma bem simplificadas algumas das possíveis vulnerabilidades que podem ser encontradas nesses ambientes.

Ao conectar os conceitos de IoT, segurança em sistemas de software IoT e suas vulnerabilidades, revelamos a necessidade de abordagens cada vez mais integradas e colaborativas para enfrentar os desafios que surgem no desenvolvimento destes sistemas. Portanto, ao entender esses conceitos de maneira integrada, criamos a base para desenvolver soluções tecnológicas que maximizem os benefícios da IoT enquanto auxiliam na redução de possíveis ameaças a sua segurança. Visto isso, no próximo capítulo, continuaremos nossa investigação, explorando mais a fundo as vulnerabilidades de segurança em sistemas de software IoT.

3 Categorizando Vulnerabilidades de Segurança de Sistemas de Software de IoT

Este capítulo descreve o estudo exploratório apresentado no artigo Pessoa e Travassos (2024), que foi conduzido para identificar as vulnerabilidades de segurança em sistemas de software IoT. Os resultados obtidos nesse estudo serviram como motivação para a elaboração do catálogo de vulnerabilidades deste trabalho, que serão apresentadas nos capítulos subsequentes.

3.1 Introdução

Há uma demanda crescente por estudos sobre estruturas que avaliam e quantificam as vulnerabilidades de segurança nos sistemas de software IoT. Essa demanda se deve ao alto impacto das avaliações de risco de segurança e ao desenvolvimento de estratégias de segurança no paradigma IoT (BAHO e ABAWAJY, 2023). No entanto, embora existam trabalhos de pesquisa que melhoram nossa compreensão das vulnerabilidades de segurança em IoT, ainda há algumas lacunas em relação àquelas que precisam ser melhor definidas devido à heterogeneidade dos cenários que abrangem os dispositivos da IoT. Além disso, isso levanta questões sobre as principais necessidades de segurança que mantêm os sistemas de software da IoT sob constante vigilância.

Com base nessa necessidade, nosso objetivo é investigar essas vulnerabilidades de segurança realizando dois estudos da literatura, uma revisão *Ad-hoc* e uma revisão estruturada, buscando assim abranger um conjunto mais amplo de informações.

(i) A revisão *Ad-hoc* baseou-se na coleta de dados diretamente em fontes práticas, como sites de organizações de segurança e bases de dados de vulnerabilidades de segurança disponibilizados por fabricantes de dispositivos IoT ou comunidades de desenvolvimento. Essa metodologia permitiu ter uma visão inicial e atualizada acerca do cenário de vulnerabilidades de segurança para com os sistemas de software IoT.

(ii) Com a revisão estruturada exploramos a literatura técnica e científica de maneira sistemática, seguindo protocolos rigorosos para a identificação, seleção e análise de trabalhos relevantes. Essa abordagem permitiu categorizar vulnerabilidades de segurança de forma fundamentada. Além de contribuir para a identificação de categorias específicas de vulnerabilidades de segurança em sistemas de software IoT (Rede, Aplicação, Dispositivo e *Peopleware*) visando sua melhor organização e compreensão.

A combinação dessas duas estratégias permitiu ainda evidenciar as vulnerabilidades de segurança em sistemas de software IoT mais impactantes e que requerem maior atenção e tratamento nos projetos de software, baseadas na comparação e combinação das vulnerabilidades identificadas.

3.2 Revisão da Literatura: *Ad-hoc*

Uma revisão *Ad-hoc* da literatura é simplesmente uma discussão de alguma literatura, tal como acontece na maioria dos artigos de investigação como parte de uma seção de antecedentes. As revisões *Ad-hoc* podem desenvolver uma teoria ou integrar uma nova teoria na literatura existente. São frequentemente apropriadas, para apoiar o desenvolvimento de teorias, identificar tópicos de investigação promissores ou mesmo preparar um exame global (RALPH e BALTES, 2022).

A revisão *Ad-hoc* pode ser realizada sem um rigor descritivo forte, já que podem ser utilizadas como amostragem intencional, com investigações à documentos ou estudos que são propositalmente uteis, relevantes ou que apoiem os argumentos da pesquisa (SILVA, 2019; RALPH e BALTES, 2022).

A revisão aplicada neste estudo foca na captura de informações de organizações de software disponíveis na web acerca das vulnerabilidades de segurança de sistemas de software IoT. No entanto, para especificar as etapas utilizadas na identificação das vulnerabilidades de segurança, seguimos os seguintes passos:

(i) selecionar um mecanismo de busca amplamente utilizado para pesquisas diretas e informais, no nosso caso o *Google*;

(ii) utilizar as expressões de busca "*Vulnerabilities in IoT systems*" e "*Security Vulnerabilities in IoT Software Systems*";

(iii) selecionar sites industriais que forneçam informações correspondentes à pesquisa, limitando-se à primeira página de resultados para identificar os mais relevantes.

A pesquisa resultou em sete sites que mencionavam explicitamente as vulnerabilidades de segurança, apresentados na Tabela 1. Limitamos nossa análise inicial a essas fontes de informação, considerando o fator de referência entre as páginas, resultando em vulnerabilidades de segurança previamente indicadas nos documentos referenciados.

Tabela 1: Fontes de Informação na Web identificadas na revisão *Ad-hoc*

Fonte	Descrição
OWASP	A OWASP é uma comunidade aberta dedicada a permitir que as organizações concebam, desenvolvam, adquiram, operem e mantenham aplicativos confiáveis. As ferramentas, os documentos, os fóruns e os capítulos da OWASP são gratuitos e abertos a qualquer pessoa interessada em melhorar a segurança dos aplicativos.
NIST National Vulnerability Database (NVD)	O NVD é um banco de dados de vulnerabilidades mantido pelo Instituto Nacional de Padrões e Tecnologia dos Estados Unidos (NIST). Ele inclui informações sobre vulnerabilidades de segurança em dispositivos de IoT.
FORTINET	A Fortinet continua a ser uma força motriz na evolução da segurança cibernética e na convergência de rede e segurança. Sua missão é proteger pessoas, dispositivos e dados em todos os lugares.
ZDNET	A ZDNet é um site de notícias de tecnologia empresarial com notícias, conselhos e percepções globais sobre tecnologia.
INFOSEC	O Infosec é um site que fornece as informações e atualizações mais recentes sobre tópicos de segurança cibernética, as últimas tendências em educação de segurança, ameaças cibernéticas e desenvolvimento de carreira.
LINKEDIN	O LinkedIn é um site de rede profissional criado para ajudar as pessoas a fazer conexões de negócios, compartilhar suas experiências e currículos e encontrar empregos.
RESILLION	A Resillion oferece soluções de transformação digital, segurança cibernética e garantia de qualidade, permitindo que seus clientes adotem e aproveitem o poder do futuro digital.

Com base no processo de investigação nesta etapa do estudo, foram identificadas 27 vulnerabilidades de segurança IoT nessas fontes da Web, que foram agregadas para evitar duplicação, mesmo que mencionadas em fontes diferentes ou usando nomes diferentes. A Tabela 2 apresenta as vulnerabilidades de segurança identificadas durante a execução da revisão *Ad-hoc*.

Tabela 2: Vulnerabilidades de segurança da revisão *Ad-hoc*

ID	Vulnerabilidades
AD1	Transferência e Armazenamento Inseguro de Dados
AD2	Senhas fracas
AD3	Mecanismos de Atualização Inseguros
AD4	Segurança Física Insuficiente
AD5	Proteção Insuficiente da Privacidade
AD6	Falta de Gerenciamento de Dispositivos
AD7	Serviços de Rede Inseguros
AD8	Interfaces de Ecossistema Inseguras
AD9	Manipulação da Execução de Código
AD10	Falta de Criptografia
AD11	Vulnerabilidades de Aplicações
AD12	Controle de Acesso Incorreto
AD13	Ignorância de Intrusão
AD14	Falta de um Ambiente de Execução Confiável
AD15	Software Desatualizado
AD16	Superfície de Ataque Excessivamente Grande
AD17	Interação com o Usuário
AD18	Postura de Segurança do Fornecedor
AD19	Configurações Padrão Inseguras
AD20	Componentes Inseguros ou Desatualizados
AD21	Pilhas TCP/IP
AD22	Bloqueio de Conta
AD23	Componentes de Terceiros Inseguros
AD24	Obtenção de Acesso ao Console
AD25	Falta de Autenticação de Dois Fatores
AD26	Atualizar Local Gravável
AD27	Enumeração de Nomes de Usuário

É importante observar que, entre as vulnerabilidades de segurança destacadas nos sites identificados, dois itens que foram inicialmente considerados vulnerabilidades de segurança tiveram de ser excluídos dos resultados: Negação de serviço (DoS - *Denial of Service*), que envolve a inundação e o comprometimento de serviços com pacotes

falsificados, resultando em graves interrupções dos serviços fornecidos; e *Botnet*, um conjunto de dispositivos conectados à Internet projetados para comprometer redes, roubar dados ou enviar spam. Essa decisão foi tomada com base em como definimos o termo "vulnerabilidade" neste estudo, em que ambos os itens se enquadram na definição de ameaças ao invés de vulnerabilidades.

3.3 Revisão Estruturada da Literatura

A adoção de uma revisão estruturada da literatura exigiu o uso de um protocolo de pesquisa mais bem definido e claro. Portanto, ela se inspira nos princípios das Revisões Sistemáticas da Literatura (BIOLCHINI *et al.*, 2005). Embora não inclua algumas etapas de uma literatura sistemática completa, uma Revisão Estruturada utiliza um protocolo sistemático e replicável (MOHER *et al.*, 2015). O protocolo de pesquisa consiste em três etapas principais: a) Planejamento: Nessa etapa, estabelecemos o problema prático a ser abordado pela revisão, fornecemos a pergunta básica de pesquisa e definimos o protocolo de pesquisa; b) Procedimento de extração: Nessa fase, extraímos informações dos estudos selecionados com base nos critérios definidos no protocolo do estudo; e c) Relatório: Nessa fase, sintetizamos e apresentamos os dados identificados nos resultados do estudo.

3.3.1 Planejamento da Revisão Estruturada

Seguindo essa abordagem estruturada, nosso objetivo é garantir o rigor e a reprodutibilidade na identificação e análise de vulnerabilidades de segurança nos sistemas de software da IoT. No entanto, precisamos de uma solução unificada que atenda às demandas de segurança no desenvolvimento desses sistemas. Portanto, compreender os principais pontos de vulnerabilidades nesses sistemas pode ajudar a mitigar uma parte significativa dos riscos principais e comuns associados a esses sistemas de software. Portanto, este trabalho tem como objetivo identificar vulnerabilidades de segurança em sistemas de software e dispositivos de IoT.

A pergunta geral de pesquisa formulada, "Quais vulnerabilidades de segurança afetam e podem ser identificadas nos sistemas de software de IoT?", é de grande importância para abordar o problema de segurança nesses sistemas. Ao procurar responder a essa pergunta de pesquisa, espera-se obter *insights* valiosos sobre as vulnerabilidades de segurança específicas que comprometem estes sistemas.

Depois de definir a pergunta da pesquisa, a próxima etapa é estabelecer a estratégia de busca. Usamos a máquina de busca Scopus para realizar a Revisão Estruturada e pesquisar fontes de informação relevantes. A Scopus foi selecionada com base em sua proeminência e relevância como mecanismo de busca, que integra uma ampla gama de literatura técnica de várias bibliotecas digitais em sua coleção (MOTTA[2] *et al.*, 2019). Combinada com o procedimento de *snowballing*, incluindo artigos citados ou artigos que mencionam os estudos identificados na revisão estruturada, essa abordagem pode reforçar a base de conhecimento por meio de um conjunto representativo de fontes primárias sobre o tópico de interesse e apoiar descobertas (MOURÃO *et al.*, 2020).

A próxima etapa da fase de planejamento é definir os critérios de inclusão e exclusão. Conforme mostrado na Tabela 3, esses critérios serão usados na fase de extração da Revisão Estruturada para determinar quais estudos contribuem para abordar o problema prático.

Tabela 3: Critérios de inclusão e exclusão

Critério	**Descrição**
Critério de Inclusão	Deve atender à pergunta de pesquisa definida
	Revisado por pares
	O texto completo deve estar disponível
Critério de Exclusão	Estudos duplicados
	Não escrito em inglês

Usamos todas as informações anteriores para criar uma cadeia de pesquisa correspondente aos critérios definidos para a Revisão Estruturada. Em seguida, a pesquisa foi restrita ao uso de palavras-chave específicas para encontrar publicações relevantes. A expressão da pesquisa foi determinada de acordo com o princípio PICOC (PETTICREW e ROBERTS, 2006), usando os parâmetros “População”, “Intervenção”, “Resultado” e “Contexto”, do inglês “*Population*”, “*Intervention*”, “*Outcome*” e “*Context*”.

A Tabela 4 mostra a sequência de pesquisa usada no banco de dados Scopus para encontrar estudos relacionados. As buscas realizadas nas revisões *Ad-hoc* e estruturadas tiveram sua última atualização ao final de 2024.

Tabela 4: Expressão de pesquisa usada na máquina de busca Scopus

Para investigação por expressão de pesquisa	
População	*"ambient intelligence" OR "assisted living" OR "multiagent systems" OR "systems of systems" OR "Cyber-Physical Systems" OR "Industry 4" OR "fourth industrial revolution" OR "web of things" OR "contemporary software systems" OR "smart manufacturing" OR "digitalization" OR "digitization" OR "digital transformation" OR "smart cit*" OR "smart building" OR "smart health" OR "smart environment" OR "smart grid"*
Intervenção	*"security" OR "vulnerability" OR "weakness" OR "Invasion" OR "threat" OR "attack" OR "anomaly" OR "malware" OR "confidentiality" OR "auditability" OR "risk"*
Comparação	*Not available*
Resultado	*"taxonomy" OR "categories" OR "classification" OR "Catalog"*
Contexto	*"internet of things" OR "Internet of Everything" OR "IoT"*
String de pesquisa final usada na Scopus	
TITLE-ABS-KEY (("ambient intelligence" OR "assisted living" OR "multiagent systems" OR "systems of systems" OR "Cyber-Physical Systems" OR "Industry 4" OR "fourth industrial revolution" OR "web of things" OR "contemporary software systems" OR "smart manufacturing" OR "digitalization" OR "digitization" OR "digital transformation" OR "smart cit" OR "smart building" OR "smart health" OR "smart environment" OR "smart grid" OR "autonomous system") AND ("security" OR "vulnerability" OR "weakness" OR "Invasion" OR "threat" OR "attack" OR "anomaly" OR "malware" OR "confidentiality" OR "auditability" OR "risk" OR "menace") AND ("taxonomy" OR "categories" OR "classification" OR "Catalog") AND ("internet of things" OR "Internet of Everything" OR "IoT")) AND PUBYEAR > 2010 AND PUBYEAR < 2025 AND (LIMIT-TO (SUBJAREA , "ENGI") OR LIMIT-TO (SUBJAREA , "COMP")) AND (LIMIT-TO (LANGUAGE , "English")) AND (LIMIT-TO (DOCTYPE , "cp") OR LIMIT-TO (DOCTYPE , "ar"))*	

3.3.2 Procedimento de Extração de Dados na Revisão Estruturada

Nessa etapa, escolhemos e extraímos dados de estudos selecionados. A extração começou com a definição de uma estratégia de filtro para avaliar os artigos com base nos critérios estabelecidos. Avaliamos títulos e resumos, excluindo estudos que não se alinhavam com a questão da pesquisa. Os estudos que passaram por esse filtro foram lidos na íntegra e, se abordaram a questão da pesquisa sem atender aos critérios de exclusão, foram incluídos na lista final.

Depois de definir a estratégia de filtro, usamos a Scopus para recuperar 812 documentos. Após a análise do título, resumo e palavras-chave, 85 artigos foram selecionados. A leitura do texto completo reduziu ainda mais esse número para 44. Esses artigos iniciaram um processo de *snowballing* resultando em 45 artigos pelo método *Forward* e 90 pelo *Backward*. Para minimizar o viés, ambos os pesquisadores conduziram o processo de filtragem, compararam os resultados e chegaram a um consenso. Por fim, 179 artigos foram selecionados, conforme ilustrado na Figura 5.

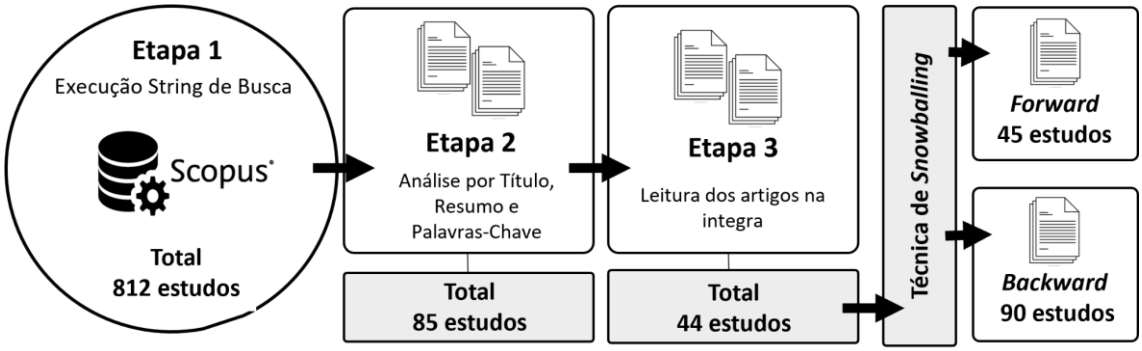


Figura 5: Estratégia de filtragem dos estudos.

Na última etapa do procedimento de extração, os dados foram extraídos usando um protocolo de coleta de dados. O procedimento envolveu o uso de um formulário padronizado para cada documento selecionado. A Tabela 5 apresenta o formulário usado para extrair informações relevantes dos documentos para análise posterior.

Tabela 5: Campos de coleta de dados

Publicação	
Título	Indica o título do artigo
Autor(es)	Lista o nome do autor
Fonte	Indica a revista, os anais da conferência ou o livro em que o artigo foi publicado
Ano	Indica o ano em que o artigo foi publicado
Resumo	Cópia do resumo para facilitar a análise posterior
Dados derivados do objetivo	
Vulnerabilidades	Quais são as vulnerabilidades de segurança dos sistemas de software de IoT que o estudo destaca?

Após a extração dos dados, os resultados foram analisados com base nas respostas identificadas em cada formulário de extração de dados, conforme apresentado na Tabela 5. A análise e a discussão subsequentes são detalhadas na seção a seguir. Os dados de extração podem ser encontrados no Apêndice A.

3.3.3 Resultados da Revisão Estruturada

Esta seção apresenta os resultados do processo de revisão estruturado. As análises são conduzidas para abordar a questão principal do estudo, identificando vulnerabilidades de segurança em sistemas de software de IoT.

O planejamento sistemático dessa etapa de revisão permitiu uma extração mais rigorosa das vulnerabilidades identificadas nos estudos selecionados. O estágio de extração avaliou as especificações de vulnerabilidade nos estudos por meio de "codificações", capturando os principais trechos. Isso permitiu uma análise detalhada de cada vulnerabilidade e uma comparação entre os estudos.

A estratégia de codificação empregada neste estudo foi baseada no método de "*Grounded Theory*", ou Teoria Fundamentada, que envolve a coleta e a análise sistemática de dados para desenvolver uma teoria (NOBLE e MITCHELL, 2016). Neste estudo, a abordagem sistematiza os dados e gera categorias relacionadas. Esse processo ajudou a identificar e agrupar vulnerabilidades que, apesar de formas e contextos variados, abordam o mesmo problema de segurança. Esse agrupamento também ajudou a definir e categorizar as vulnerabilidades nos cenários de sistemas de software da IoT: Dispositivo, Rede, Aplicação e *Peopleware*.

As vulnerabilidades de segurança classificadas na categoria “Dispositivo” podem ser exploradas por meio de acesso físico ao hardware. A categoria “Rede” engloba os pontos fracos relacionados à comunicação ou ao tráfego dentro de uma rede IoT. Na categoria “Aplicação”, as vulnerabilidades de segurança estão associadas a pontos fracos do sistema de software. Por fim, a categoria “*Peopleware”* classifica os pontos fracos de segurança da IoT diretamente relacionados ao fator humano. A Tabela 6 lista as 69 vulnerabilidades de segurança identificadas e catalogadas e suas respectivas categorias.

Tabela 6: Vulnerabilidades de segurança da revisão estruturada

ID	Vulnerabilidade	Categoria
VUL1	Quebra de Autenticação	Aplicação
VUL2	Estouro de *Buffer*	Aplicação
VUL3	Inconsistência de Dados	Aplicação
VUL4	Gerenciamento de Acesso Inseguro	Aplicação
VUL5	Configuração de Interface Insegura	Aplicação
VUL6	Gestão Insegura de Dados	Aplicação
VUL7	Software Inseguro	Aplicação
VUL8	Falta de Monitoramento Ativo de Dispositivo	Aplicação
VUL9	Código de Baixa Qualidade	Aplicação
VUL10	Não Repúdio	Aplicação
VUL11	Injeção em Banco Dados	Aplicação
VUL12	Fraca/Falta de Criptografia na Aplicação	Aplicação
VUL13	Código Malicioso no Aplicativo	Aplicação
VUL14	Sistemas de Baixo Custo	Dispositivo
VUL15	Canal de Voz	Dispositivo
VUL16	Configuração Padrão	Dispositivo
VUL17	Falsificação de Dispositivo	Dispositivo
VUL18	Vazamento de Emanações Eletromagnéticas	Dispositivo
VUL19	Restrições de Energia	Dispositivo
VUL20	Interação Heterogênea	Dispositivo
VUL21	Transferência e Armazenamento Inseguro de Dados	Dispositivo
VUL22	Firmware Inseguro	Dispositivo
VUL23	Inicialização Insegura	Dispositivo
VUL24	Senha Insegura	Dispositivo

VUL25	Testes Insuficientes	Dispositivo
VUL26	Falta de Proteção de Canal Lateral	Dispositivo
VUL27	Falta de Autenticação Forte	Dispositivo
VUL28	Baixo Poder Computacional	Dispositivo
VUL29	Baixo Alcance de Transmissão de Dados	Dispositivo
VUL30	Injeção de Código Malicioso	Dispositivo
VUL31	Obtenção de Acesso ao Console	Dispositivo
VUL32	Dano Físico	Dispositivo
VUL33	Violação Física	Dispositivo
VUL34	Privação do Sono	Dispositivo
VUL35	Clonagem de Etiquetas	Dispositivo
VUL36	Acesso Físico Não Protegido	Dispositivo
VUL37	Controle de Acesso Fraco	Dispositivo
VUL38	Fraco/Falta de Criptografia nos Dispositivos	Dispositivo
VUL39	Interface Física Insegura	Dispositivo
VUL40	Interferência de Canal	Rede
VUL41	Sobrecarga de Comunicação	Rede
VUL42	Vazamento ou Violação de Dados	Rede
VUL43	Escuta Clandestina	Rede
VUL44	Nó Falso/Malicioso	Rede
VUL45	Comunicação Heterogênea	Rede
VUL46	Servidor Inseguro	Rede
VUL47	Mecanismos de Atualização Inseguros	Rede
VUL48	Falta de Mecanismos de Autenticação Adequados	Rede
VUL49	Falta de Senha Forte	Rede
VUL50	Falta de Protocolos de Comunicação Seguros	Rede
VUL51	Configurar a Rede Repetidamente	Rede
VUL52	Falsificação de Sinal	Rede
VUL53	Acesso Não Autorizado	Rede
VUL54	Rede Insegura	Rede
VUL55	Portas Não Utilizadas Habilitadas	Rede
VUL56	Fraca/Falta de Criptografia na Comunicação	Rede
VUL57	Propriedades Físicas do Sistema de Energia	Rede

VUL58	Desautenticação de Wi-Fi	Rede
VUL59	Controle de Tráfego Inseguro	Rede
VUL60	Arquitetura Centralizada	Rede
VUL61	Acesso a Links Maliciosos	*Peopleware*
VUL62	Identificação do Fornecedor do Produto	*Peopleware*
VUL63	Conhecimento do Sistema	*Peopleware*
VUL64	Falta de Suporte Técnico	*Peopleware*
VUL65	Circunstâncias Pessoais e Sociais	*Peopleware*
VUL66	*Phishing*	*Peopleware*
VUL67	Engenharia Social	*Peopleware*
VUL68	Aquisição de Dispositivo Não Confiável	*Peopleware*
VUL69	Postura de Segurança do Fornecedor	*Peopleware*

A ferramenta QDA Miner (FORTUNA *et al.*, 2014) foi fundamental para apoiar a categorização dos trechos dos artigos. Ela facilitou a análise de vulnerabilidade, a organização de categorias e a extração de informações, auxiliando na síntese geral das descobertas, conforme mostrado na Figura 6.

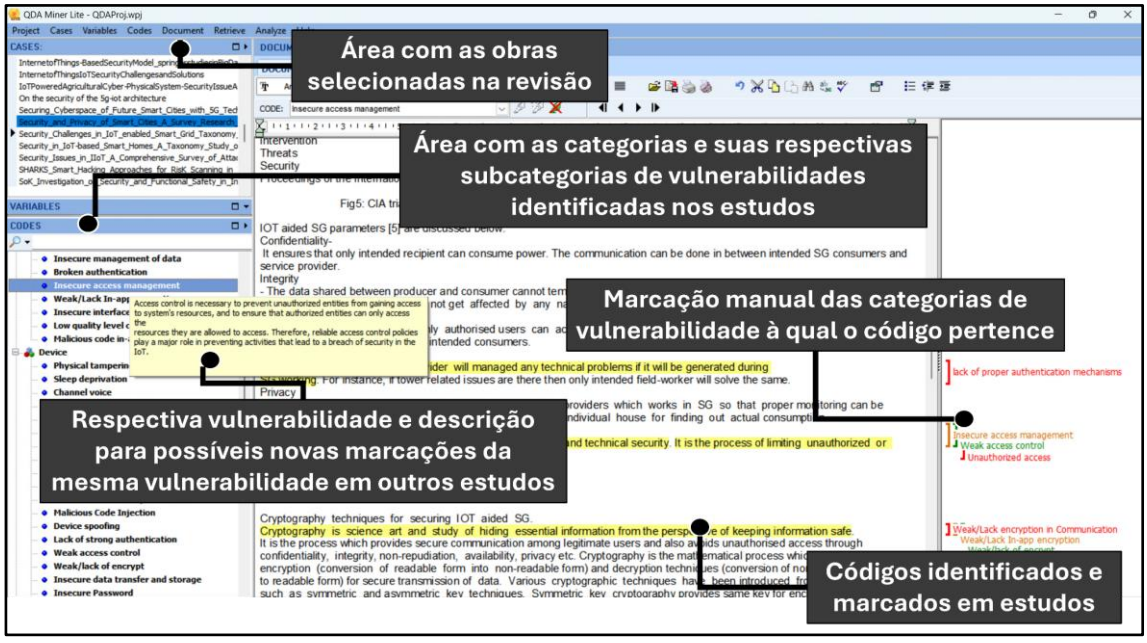


Figura 6: Classificação de vulnerabilidades de segurança usando a ferramenta QDA Miner Lite.

Foram realizadas codificações abertas, onde os trechos de texto que apresentavam informações relevantes sobre vulnerabilidades foram destacados e codificados. As marcações eram feitas diretamente sobre os fragmentos dos textos, atribuindo alguns rótulos (*codings*) que descreviam, de forma simples e objetiva, o significado de cada trecho. Alguns exemplos de códigos aplicados incluem: "falha de autenticação", "falta de criptografia", "problema na atualização de firmware", entre outros.

A interface do QDA Miner Lite permitiu selecionar trechos específicos do texto e associá-los a códigos previamente criados e criar códigos conforme a necessidade. A cada nova ocorrência de uma característica ou padrão de vulnerabilidade, a ferramenta permitia: "Marcar o texto", selecionando diretamente a sentença, parágrafo ou expressão relevante; "Atribuir o código", escolhendo de uma lista existente ou criando um novo código; e "Gerenciar os códigos": agrupando, renomeando ou excluindo, conforme a evolução da análise. Esse processo foi iterativo, com refinamento nos códigos à medida que novos padrões surgiam dos dados. Posteriormente, os códigos foram organizados em categorias, de acordo com suas relações semânticas e conceituais. O pacote contendo os artefatos desenvolvidos, incluindo os dados de codificação no QDA Miner, pode ser encontrado por meio do link[1].

É importante observar que algumas vulnerabilidades de segurança podem parecer repetidas. Entretanto, o que precisa ser observado é que, em cada categoria, as dimensões de risco associadas a determinadas vulnerabilidades podem variar dependendo do contexto. Portanto, é necessário abordá-las com base nas necessidades específicas ou na priorização do sistema de software IoT. Por exemplo, considere a vulnerabilidade [VUL6] "Gerenciamento Inseguro de Dados", que está relacionada as vulnerabilidades associadas à falta de privacidade ou segurança em dados compartilhados ou armazenados na categoria Aplicação. Problemas semelhantes também podem ser encontrados nos contextos de Dispositivos e Redes. Para esclarecer os contextos em que o mesmo problema pode surgir, listamos [VUL21] para a categoria Dispositivo e [VUL42] para a categoria Rede, refletindo os contextos específicos destacados nos estudos extraídos.

[1] https://github.com/BillHuds/Files-StudyVulnerabilitiy

Portanto, embora certas vulnerabilidades possam ter semelhanças, sua categorização e diferenciação com base em fatores contextuais permitem uma compreensão mais abrangente e uma abordagem direcionada para tratá-las no paradigma IoT. Além disso, cada vulnerabilidade tem sua descrição, o que permite um relato do problema que cada uma representa. A explicação de cada vulnerabilidade de segurança pode ser encontrada no Apêndice B.

3.4 Discussão

Certas vulnerabilidades de segurança foram mais proeminentes nos dados extraídos, exigindo atenção devido à sua presença recorrente e à ameaça à integridade do sistema de software IoT. Com base nessa necessidade, a Tabela 7 contém os pontos de vulnerabilidade de segurança que se sobrepõem entre os dados relatados nas revisões *Ad-hoc* e estruturadas. Esse mapeamento busca destacar as vulnerabilidades mais comuns e que exigem mais atenção.

Tabela 7: Vulnerabilidades de segurança destacadas nos estudos da literatura

Revisão Ad Hoc	Revisão Estruturada	Vulnerabilidades	Categoria
AD13	VUL53	Acesso Não Autorizado	Rede
AD26	VUL48	Falta de Mecanismos de Autenticação Adequados	Rede
AD1, AD5	VUL21	Transferência e Armazenamento Inseguro de Dados	Dispositivo
AD26	VUL27	Falta de Autenticação Forte	Dispositivo
AD15	VUL33	Violação Física	Dispositivo
AD13	VUL37	Controle de Acesso Fraco	Dispositivo
AD1, AD5	VUL42	Vazamento ou Violação de Dados	Rede
AD11	VUL56	Fraca/Falta de Criptografia na Comunicação	Rede
AD14	VUL44	Nó Falso/Malicioso	Rede
AD12, AD13	VUL4	Gerenciamento de Acesso Inseguro	Aplicação
AD11	VUL38	Fraco/Falta de Criptografia nos Dispositivos	Dispositivo

AD3, AD20, AD27	VUL22	Firmware Inseguro	Dispositivo
AD22	VUL50	Falta de Protocolos de Comunicação Seguros	Rede
AD3, AD12, AD16, AD21	VUL7	Software Inseguro	Aplicação
AD14	VUL17	Falsificação de Dispositivo	Dispositivo
AD10, AD25	VUL31	Obtenção de Acesso ao Console	Dispositivo
AD12, AD26	VUL1	Quebra de Autenticação	Aplicação
AD1, AD5, AD12	VUL6	Gestão Insegura de Dados	Aplicação
AD20	VUL16	Configuração Padrão	Dispositivo
AD4	VUL32	Dano Físico	Dispositivo
AD2	VUL24	Senha Insegura	Dispositivo
AD7	VUL54	Rede Insegura	Rede
AD2	VUL49	Falta de Senha Forte	Rede
AD8, AD12	VUL5	Configuração de Interface Insegura	Aplicação
AD11, AD12	VUL12	Fraca/Falta de Criptografia na Aplicação	Aplicação
AD6, AD12	VUL8	Falta de Monitoramento Ativo de Dispositivo	Aplicação
AD8	VUL39	Interface Física Insegura	Dispositivo
AD3	VUL47	Mecanismos de Atualização Inseguros	Rede
AD18	VUL64	Falta de Suporte Técnico	*Peopleware*
AD19	VUL69	Postura de Segurança do Fornecedor	*Peopleware*

As vulnerabilidades de segurança foram agrupadas com base em suas descrições relevantes, razão pela qual há uma relação entre várias vulnerabilidades nos estudos, conforme apresentado na Tabela 7. Esse agrupamento se deve ao fato de a revisão estruturada ter categorias específicas para as vulnerabilidades, diferentes daquelas destacadas na revisão *Ad-hoc*.

A ordem usada na Tabela 7 baseia-se na frequência de citações nas fontes primárias selecionadas, conforme determinado pelos dados da revisão estruturada. Com

base nisso, destacamos, para fins de observação, os pontos de vulnerabilidade de segurança que tiveram a maior incidência nos trabalhos selecionados e são proeminentes em ambos os estudos de literatura: Acesso não autorizado, falta de mecanismos de autenticação adequados e transferência e armazenamento inseguro de dados.

O acesso não autorizado desempenha um papel fundamental na prevenção de atividades que levam a uma violação de segurança nos sistemas de software IoT, pois o controle de acesso é necessário para impedir que entidades não autorizadas obtenham acesso aos recursos do sistema e garantir que as entidades autorizadas só possam acessar os recursos que têm permissão para acessar (ALQASSEM e SVETINOVIC, 2014). A falta de mecanismos de autenticação adequados também é vista com grande importância nos sistemas inteligentes, pois sem uma autenticação forte, fica fácil para os invasores se disfarçarem de usuários legítimos e usarem credenciais ou qualquer outra informação que lhes conceda acesso aos recursos do ambiente IoT (KARIE *et al.*, 2021). A transferência e o armazenamento inseguro de dados em dispositivos também é uma das características que marcam uma preocupação significativa em IoT. O grande número de dispositivos que podem coletar e transferir dados confidenciais para bancos de dados ou armazenamento em nuvem apresenta riscos substanciais se algum dado for exposto (SOOKHAK *et al*., 2019). É importante destacar que ambas as vulnerabilidades estão diretamente associadas ao contexto de rede/comunicação dos serviços de IoT, enfatizando a influência e o impacto significativos da IoT na melhoria da infraestrutura de rede global devido às novas demandas que ela impõe (PAES *et al.*, 2022).

Também enfatizamos que os itens de vulnerabilidade destacados têm um impacto e uma relevância significativos quando observamos que esses resultados se assemelham aos achados nos trabalhos de DAVIS *et al.* (2020) e CHHETRI e MOTTI (2021), que, apesar de terem uma restrição contextual focada em dispositivos domésticos inteligentes, perfazem uma infinidade de desafios e vulnerabilidades para promover um maior alinhamento em relação aos desafios que afetam os cenários de IoT.

Embora essas vulnerabilidades tenham tido uma incidência maior, é essencial observar que todas as outras vulnerabilidades listadas na Tabela 7 são igualmente importantes de serem abordadas para obter sistemas de software de IoT mais seguros. Por fim, com relação ao aspecto quantitativo dos estudos que citam e reforçam os argumentos

destacados no estudo, fornecemos um relatório técnico que detalha a metodologia e os resultados do estudo de revisão estruturada, que pode ser consultado no APÊNDICE A.

Ao adotar uma definição específica de “Vulnerabilidade” para a categorização de itens, podemos observar que identificamos um conjunto relativamente menor do que CHHETRI e MOTTI (2021). Entretanto, é importante destacar que essa diferenciação é válida para ambos os estudos. Essa abordagem mais específica nos produz dados mais precisos ao restringir a inclusão de itens diretamente associados a ameaças ou ataques nos resultados.

Um item importante são as categorias alinhadas a cada vulnerabilidade identificada na análise estruturada. A estrutura obtida assemelha-se àquelas definidas nos trabalhos de DAVIS *et al.* (2020), CHHETRI e MOTTI (2021) e PEDREIRA *et al.* (2021), exceto pela categoria *Peopleware*, que ainda não havia sido descrita em estudos anteriores que abordavam vulnerabilidades de segurança em sistemas de software de IoT. Ela indica um importante componente de observação que pode afetar diretamente os riscos associados às vulnerabilidades de segurança relacionadas a agentes humanos.

Vale a pena observar que, apesar do impacto significativo do agente humano nos sistemas de software IoT, poucos estudos o mencionam como um ponto de vulnerabilidade no sistema. Além disso, aqueles que o fazem geralmente não enfatizam essa questão nem vinculam diretamente o ponto fraco ao fator humano. Como exemplo, destacamos duas vulnerabilidades de segurança categorizadas como “*Peopleware*” na Tabela 6: [VUL66] *Phishing*, usado para induzir as pessoas a inserir suas informações pessoais, fazer *download* de software malicioso capaz de espalhar malware ou manipular dados de sensores para fornecer informações falsas que podem afetar a tomada de decisões; e [VUL67] Engenharia Social, que envolve a manipulação de usuários para extrair informações privadas, dados confidenciais ou informações que podem ser usadas para obter acesso a redes em ambientes inteligentes. Com base nessas duas vulnerabilidades, podemos entender o perigo em potencial dos pontos fracos do sistema. Portanto, um controle mais rigoroso da função humana nos sistemas torna-se fundamental para minimizar ameaças significativas e ataques subsequentes.

Ao analisar os dados comparativos apresentados na Tabela 7, destacaram-se duas vulnerabilidades relacionadas ao *Peopleware*: especificamente [VUL64] Falta de Suporte

Técnico e [VUL69] Postura de Segurança do Fornecedor. Esses pontos são identificados como principais vulnerabilidades nessa categoria, principalmente associadas à negligência por parte de alguns fornecedores de dispositivos IoT. Em determinadas situações, esses fornecedores devem conceder diretrizes de segurança adequadas aos usuários. Embora não seja possível inferir o impacto específico com base em nossos dados, sabe-se que essa negligência traz consequências. Portanto, abordar essas questões com a mesma importância atribuída a outras vulnerabilidades é essencial.

Outro ponto relevante é a especificidade das vulnerabilidades de segurança em IoT, já que muitas podem ser compartilhadas com sistemas de software tradicionais. Ao analisar as vulnerabilidades destacadas na Tabela 6, observamos que a principal diferença está nas vulnerabilidades específicas de dispositivos IoT e em algumas vulnerabilidades únicas nas demais categorias, como evidenciado na Tabela 8.

Tabela 8: Vulnerabilidades específicas de IoT

ID	Vulnerabilidades	Categoria
VUL15	Canal de Voz	Dispositivo
VUL17	Falsificação de Dispositivo	Dispositivo
VUL18	Vazamento de Emanações Eletromagnéticas	Dispositivo
VUL19	Restrições de Energia	Dispositivo
VUL22	Firmware Inseguro	Dispositivo
VUL26	Falta de Proteção de Canal Lateral	Dispositivo
VUL28	Baixo Poder Computacional	Dispositivo
VUL29	Baixo Alcance de Transmissão de Dados	Dispositivo
VUL31	Obtenção de Acesso ao Console	Dispositivo
VUL32	Dano Físico	Dispositivo
VUL33	Violação Física	Dispositivo
VUL34	Privação do Sono	Dispositivo
VUL35	Clonagem de Etiquetas	Dispositivo
VUL36	Acesso Físico Não Protegido	Dispositivo
VUL8	Falta de Monitoramento Ativo de Dispositivo	Aplicação
VUL40	Interferência de Canal	Rede

VUL68	Aquisição de Dispositivo Não Confiável	*Peopleware*

A categoria Dispositivo é exclusiva dos sistemas de software IoT, pois engloba sensores, atuadores e dispositivos diretamente envolvidos na captura e transmissão de dados remotos, o que não é característico de sistemas tradicionais. Além disso, conforme mencionado anteriormente, embora as vulnerabilidades de segurança em IoT frequentemente compartilhem características com aquelas em sistemas de software tradicionais, as estratégias de mitigação podem diferir, exigindo, por vezes, uma abordagem mais cuidadosa.

Também é importante enfatizar que o fato de algumas vulnerabilidades serem comuns em cenários tradicionais não deve reduzir a importância das vulnerabilidades específicas de IoT. Os sistemas IoT estão sujeitos às mesmas fragilidades de um sistema de software convencional, e é essencial tratá-las de maneira adequada.

3.4.1 Soluções e Recomendações

Diversas soluções potenciais podem ajudar a mitigar as fragilidades inerentes às vulnerabilidades de segurança em sistemas de software IoT. Quando adotadas, essas soluções podem reduzir os riscos de ameaças a esses sistemas. A Tabela 7 destaca algumas soluções e melhores práticas para as três vulnerabilidades de segurança.

Acesso Não Autorizado (KAMORU *et al.*, 2014; TAKADA, 2017; ALI *et al.*, 2021**):**

- **Autenticação Forte:** Implemente um sistema de autenticação robusto para dispositivos IoT. Isso pode incluir o uso de senhas fortes, autenticação de dois fatores (2FA) e certificados digitais para verificar as identidades dos dispositivos.
- **Segmentação de Rede:** Isole a rede IoT do restante da infraestrutura de TI. Utilize VLANs (Redes Locais Virtuais) ou redes separadas para garantir que os dispositivos IoT não possam ser acessados facilmente a partir de outros pontos da rede.

- **Auditoria e Monitoramento:** Estabeleça um sistema contínuo de auditoria e monitoramento para rastrear atividades em dispositivos IoT e identificar comportamentos anômalos.
- **Gerenciamento de Identidade:** Adote soluções de gerenciamento de identidade para controlar e gerenciar as identidades e os privilégios de usuários e dispositivos IoT.

Falta de Mecanismos de Autenticação Adequados (AL ABDULWAHID *et al.*, 2015; PATIL *et al.*, 2018; ALI *et al*., 2021**):**

- **Autenticação de Dispositivos:** Implemente autenticação robusta utilizando senhas complexas ou chaves criptográficas de autenticação. Além disso, utilize certificados digitais para verificar as identidades dos dispositivos e garantir sua autenticidade.
- **Controle Físico:** Mantenha os dispositivos IoT fisicamente seguros para evitar acessos não autorizados. Adote medidas de proteção física, como fechaduras e alarmes.
- **Conformidade com Padrões e Regulamentações:** Esteja atento às regulamentações e padrões de segurança relevantes, como o GDPR (Regulamento Geral de Proteção de Dados) na União Europeia, e siga as diretrizes aplicáveis.

Transferência e Armazenamento de Dados Inseguros (WANG *et al.*, 2018; ROOHI *et al.*, 2019; ALI *et al*., 2021**):**

- **Criptografia de Dados:** Implemente criptografia robusta para proteger dados em trânsito e em repouso. Utilize protocolos seguros como HTTPS para transmissão de dados e criptografia de disco para dados armazenados.
- **Proteção de Chaves:** Mantenha as chaves de criptografia seguras e fora do alcance de atacantes. Use dispositivos como Módulos de Segurança de Hardware (*Hardware Security Modules* - HSMs) para proteger as chaves.
- **Autenticação Mútua:** Configure a autenticação mútua entre dispositivos IoT e servidores para garantir que ambas as partes se autentiquem antes de trocar dados.

- **Redes Privadas Virtuais (VPNs):** Utilize VPNs para criar túneis seguros para a transmissão de dados entre dispositivos IoT e servidores, especialmente em redes não confiáveis, como a Internet pública.
- **Contratos com Fornecedores:** Certifique-se de que os fornecedores de dispositivos IoT implementem medidas adequadas de segurança para transferência e armazenamento de dados.
- **Atualizações Seguras de Firmware:** Mantenha o firmware dos dispositivos IoT atualizado para corrigir vulnerabilidades conhecidas que possam impactar o armazenamento e a transmissão de dados.

Essas recomendações representam apenas um subconjunto de algumas estratégias para proteger sistemas de software IoT. Ressaltamos que a identificar e compartilhar definitiva de estratégias de mitigação para as outras vulnerabilidades estão melhor explanadas no próximo capítulo.

3.5 Ameaças à Validade

Algumas implicações e limitações em relação aos resultados deste estudo devem ser destacadas. Primeiramente, reconhecemos que não temos controle sobre a integridade das listas de vulnerabilidades de segurança. Pode haver viés do pesquisador, onde certas expectativas ou predisposições influenciam a coleta, análise ou interpretação dos dados. Por essa razão, algumas vulnerabilidades ou estudos podem ter sido ignorados durante o processo de seleção e extração.

Utilizamos um processo menos rigoroso para a revisão *Ad-hoc* ao selecionar vulnerabilidades de segurança. Muitas foram identificadas em documentos disponíveis em sites industriais selecionados, o que não garante a consistência dos dados coletados e do processo de percepção dessas vulnerabilidades de segurança. Apesar de sua natureza flexível e menos estruturada, reconhecemos que o uso da revisão *Ad-hoc* impactou positivamente a identificação de vulnerabilidades organizacionais. Ela permitiu uma resposta rápida a mudanças e novas informações, algo crucial em ambientes organizacionais dinâmicos. A ausência de uma estrutura rígida possibilitou adaptação imediata a novas tendências e padrões emergentes, facilitando uma detecção mais

intuitiva e direta de vulnerabilidades, que posteriormente serviram como base para a identificação de outras vulnerabilidades.

Destacamos ainda que, para o processo de "*snowballing*", o viés de dados pré-definidos pode levar a suposições de correlação de dados com base nas vulnerabilidades identificadas em estudos anteriores (revisões *Ad-hoc* e estruturadas), o que limita o surgimento de "novas informações" com base em vocabulários diferentes, pois, para este trabalho, as vulnerabilidades foram delimitadas com base em suas definições.

Também temos um viés temporal devido à data de catalogação e análise dos resultados, onde novas fontes ou observações podem surgir com base em fatores não relacionados à data de intervenção de nosso estudo. No entanto, esse é um desafio que os estudos na literatura sempre enfrentam.

3.6 Conclusão

Dada a significativa expansão que os sistemas de software IoT tiveram nos últimos anos, seu potencial de engajamento em diversos setores é evidente. Isso exige uma atenção especial sobre como os dispositivos IoT gerenciam e manipulam dados, especialmente considerando a grande variedade de dados sensíveis. Portanto, a segurança em sistemas de software IoT torna-se crucial para operacionalizar corretamente essa tecnologia. Entre os principais vetores associados à segurança, as vulnerabilidades de software se destacam como um campo de estudo com um impacto significativo na mitigação dos danos causados por ameaças ou ataques que podem interferir diretamente no desempenho das tecnologias IoT.

Este capítulo apresentou um conjunto de vulnerabilidades de segurança identificadas no contexto de sistemas de software IoT, com base em dois estudos de literatura: revisão ad hoc e estruturada. Inicialmente, nossa observação focou no levantamento de vulnerabilidades de segurança com base em revisões *Ad-hoc* de sites de sete organizações, onde catalogamos 27 vulnerabilidades. Após obter uma estrutura base de vulnerabilidades de segurança, prosseguimos para a revisão estruturada da literatura, onde identificamos um total de 69 vulnerabilidades de segurança, classificadas em quatro categorias relacionadas a cenários específicos de sistemas de software IoT: Dispositivo, Aplicação, Rede e uma nova categoria adicional, *Peopleware*, que abrange as

vulnerabilidades de segurança relacionadas a fatores humanos. O conjunto final de vulnerabilidades de segurança demonstra a unidade entre aquelas identificadas dentro das organizações (usando a revisão *Ad-hoc*) e as encontradas na revisão estruturada da literatura, apresentando, assim, as 30 principais vulnerabilidades de segurança em sistemas de software IoT que exigem maior atenção e tratamento.

Dentre elas, destacamos três vulnerabilidades com maior relevância: Acesso Não Autorizado, Falta de Mecanismos de Autenticação Adequados e Transferência e Armazenamento de Dados Inseguros, para as quais também descrevemos um pequeno conjunto de recomendações com possíveis estratégias e soluções para mitigar tais ameaças.

Os resultados obtidos nestes estudos de literatura podem contribuir com a mitigação dos riscos associados à falta de segurança em projetos de sistemas de software IoT, fornecendo diretrizes iniciais para aprimorar a segurança desses sistemas. Como desdobramento desta pesquisa, pretende-se ainda aprofundar a investigação sobre vulnerabilidades de segurança, construindo um catálogo de vulnerabilidades que reúna informações necessárias para a construção de sistemas IoT mais seguros. Esse catálogo poderá não apenas apoiar os profissionais da área, mas também inspirar novas pesquisas e aprimoramentos nas práticas de segurança.

4 Catálogo de Vulnerabilidades de Segurança em Sistemas de Software IoT

Este capítulo apresenta e discute os principais resultados diante da condução dos estudos de revisão, que resultaram no Catálogo de Vulnerabilidades de Segurança em Sistemas de Software IoT, com um conjunto mais detalhado de informações acerca de cada vulnerabilidade de segurança identificada, com as suas descrições e possíveis formas de mitigação.

4.1 Introdução

O crescente uso de dispositivos IoT em diversos domínios, como residências inteligentes, saúde, automação industrial e cidades conectadas, tem transformado significativamente a forma como interagimos com as soluções tecnológicas (AHLUWALIA *et al.*, 2024). No entanto, essa expansão também trouxe à tona uma série de desafios relacionados à segurança, destacando vulnerabilidades que podem ser exploradas por agentes maliciosos. A complexidade e a diversidade dos sistemas de software IoT, associadas à falta de padronização e à limitação de recursos desses dispositivos, tornam-nos alvos atrativos para ataques cibernéticos (SIBONI *et al.*, 2019; BOCHIE *et al.*, 2020).

O "Catálogo de Vulnerabilidades de Segurança em Sistemas de Software IoT", que a partir deste ponto será referido como “Catálogo de Vulnerabilidades IoT” para maior concisão, tem como objetivo identificar, classificar e analisar as principais vulnerabilidades de segurança presentes em nestes sistemas, com o intuito de auxiliar profissionais e pesquisadores na compreensão e mitigação destas ameaças. Este capítulo busca preencher uma lacuna crítica no campo da segurança, fornecendo uma visão abrangente sobre as vulnerabilidades associadas a esses dispositivos e as potenciais formas de mitigá-las.

A criação de um catálogo estruturado permite não apenas a organização do conhecimento capturado, mas também a de promover a disseminação de boas práticas e a apoiar a adoção de medidas preventivas. Com base em revisões da literatura (*Ad-hoc* e

Estruturada), este trabalho oferece *insights* valiosos para a construção de sistemas IoT mais seguros.

Embora bases como o NVD e o CVE forneçam um amplo catálogo de vulnerabilidades, a identificação específica de vulnerabilidades relacionadas ao ecossistema de IoT ainda é um desafio. Muitos dos registros não oferecem um detalhamento contextualizado sobre o ambiente ou as particularidades de sistemas de software IoT. Neste sentido, este trabalho busca contribuir na direção de um catálogo que possa apoiar profissionais e pesquisadores na identificação e mitigação de vulnerabilidades de segurança específicas desse contexto.

4.2 Processo de Construção do Catálogo de Vulnerabilidades IoT

O processo de construção do catálogo de vulnerabilidades IoT foi dividido em três fases principais, envolvendo o levantamento e reconhecimento das vulnerabilidades de segurança em sistemas de software IoT evidenciadas na literatura, a organização e implementação do catálogo dado o conjunto de vulnerabilidades de segurança identificadas e a sua avaliação. A Figura 7 ilustra o processo de construção do catálogo, sendo possível observar além das fases definidas para a construção do catálogo, o conjunto de atividades que permitiram alcançar o resultado final do catálogo.

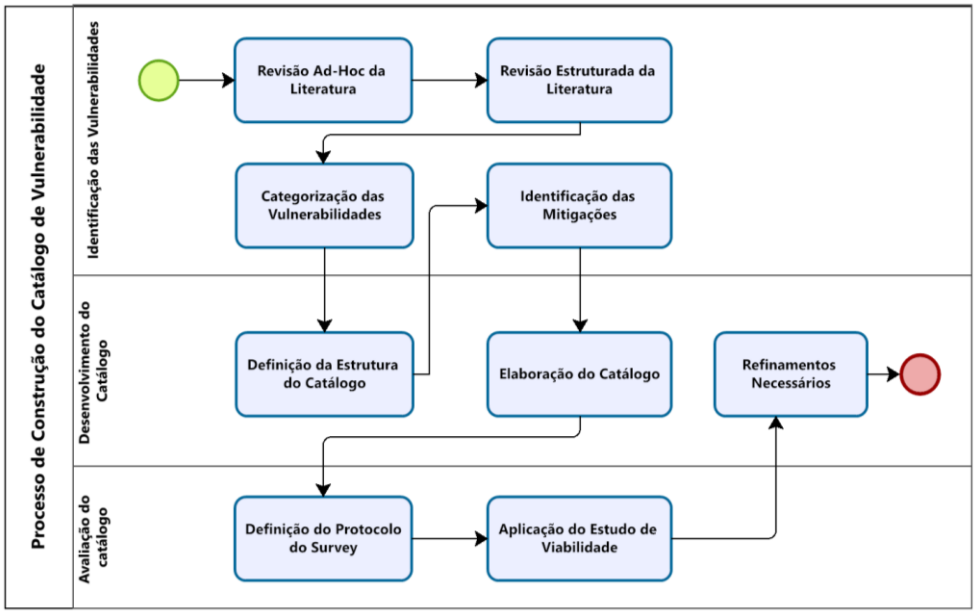


Figura 7: Processo de construção do catálogo.

A primeira fase teve como objetivo identificar as vulnerabilidades de segurança em sistemas de software IoT. A segunda fase focou no desenvolvimento do catálogo, por meio da definição de sua estrutura, implementação e refinamento do artefato gerado. A terceira fase focou em avaliar a viabilidade da utilização do catálogo por profissionais e pesquisadores da área. A seguir são apresentadas de forma mais detalhada cada uma das fases e atividades do processo de construção do catálogo, com exceção da fase 3 que será descrita no capítulo seguinte.

4.2.1 Levantamento das Vulnerabilidades de Segurança em Sistemas de Software IoT

Como descrito no capítulo 3, foram utilizados alguns métodos para o levantamento das vulnerabilidades de segurança em sistemas de software IoT, incluindo revisões *Ad-hoc* e estruturada da literatura. Esses métodos permitiram identificar as vulnerabilidades recorrentes, classificá-las e explorar as estratégias de mitigação usualmente realizadas. O foco foi a coleta e organização de informações que contribuam para a compreensão aprofundada dos desafios enfrentados na segurança de sistemas de software no paradigma IoT e a elaboração de um corpo de conhecimento sobre vulnerabilidades de segurança.

Conforme detalhado no capítulo 3, a revisão *Ad-hoc* realizada neste estudo focou na identificação de vulnerabilidades de segurança em sistemas de software IoT, utilizando uma abordagem mais flexível e baseada em amostragem intencional. O processo incluiu a utilização do Google como mecanismo de busca e a pesquisa por expressões como "vulnerabilidades em sistemas IoT" e "Vulnerabilidades de segurança em sistemas de software IoT". A análise se concentrou nos sites mais relevantes encontrados nas primeiras páginas de resultados, resultando em sete fontes que mencionavam explicitamente essas vulnerabilidades. Dessa análise, foram identificadas 27 vulnerabilidades de segurança.

A Revisão Estruturada da Literatura foi conduzida com base em um protocolo sistemático e replicável, inspirado nas Revisões Sistemáticas da Literatura, com o objetivo de identificar vulnerabilidades de segurança em sistemas de software IoT. O processo incluiu três etapas principais: Planejamento, onde foram definidos o problema e

a pergunta de pesquisa; Procedimento de extração, onde dados foram extraídos de estudos selecionados; e Relatório, que sintetiza os dados encontrados.

Foram identificadas cerca de 69 vulnerabilidades de segurança em sistemas de software IoT. As vulnerabilidades identificadas foram organizadas por categoria (Dispositivo, Rede, Aplicação e *Peopleware*) e analisadas por meio de codificação, usando da abordagem *Grounded Theory* (Teoria Fundamentada) para agrupar vulnerabilidades relacionadas. As vulnerabilidades catalogadas foram analisadas em seus contextos específicos, permitindo uma compreensão aprofundada dos riscos associados a cada tipo de vulnerabilidade.

4.2.2 Desenvolvimento de um Catálogo de Vulnerabilidades IoT

Nesta fase serão abordadas a estruturação do catálogo de vulnerabilidades IoT, descrevendo a classificação e as categorias de vulnerabilidades identificadas, bem como as fontes utilizadas para sua compilação. Além disso, a seção explora como as informações foram organizadas para facilitar a consulta e a aplicação prática pelos diferentes interessados, como pesquisadores e profissionais da prática.

4.2.2.1 Definição da Estrutura do Catálogo

O catálogo foi estruturado para oferecer uma visão clara e abrangente das vulnerabilidades de segurança inerentes ao paradigma IoT, classificando-as em categorias que refletem aspectos técnicos e contextuais. As principais categorias incluem:

- **Vulnerabilidades de Rede**: Falhas em protocolos, autenticação ou encriptação.
- **Vulnerabilidades de Dispositivo**: Exposição física, firmware desatualizado ou configuração inadequada.
- **Vulnerabilidades de Aplicação**: Bugs no código, falta de validação de entrada ou bibliotecas inseguras.
- **Vulnerabilidades de *Peopleware***: Exposição de dados sensíveis ou coleta excessiva de informações.

Cada vulnerabilidade é atribuída a uma ou mais categorias para permitir uma análise multidimensional. Além disso, para cada vulnerabilidade catalogada, os seguintes campos são documentados:

- **Título**: Nome da vulnerabilidade catalogada, baseada nas nomenclaturas identificadas durante os estudos de revisão.
- **Descrição**: Um resumo detalhado da vulnerabilidade, incluindo o contexto de sua ocorrência.
- **Categoria**: Descrição dos danos que a vulnerabilidade pode causar (ex.: interrupção de serviços, violação de dados).
- **Mitigações**: Recomendações para prevenção ou correção.
- **Fonte:** Referência da base ou artigo de onde a vulnerabilidade foi extraída.

A seguir, são apresentados alguns exemplos de vulnerabilidades de segurança documentadas:

Tabela 9: Canal de Voz (Dispositivo)

Título	Canal de Voz
Descrição	Associados à segurança e à privacidade quando os dispositivos IoT incorporam capacidades de voz, como assistentes pessoais ativados por voz, sistemas de controle de casa inteligente ou dispositivos de comunicação por voz. Em casas inteligentes, essas informações podem agora ser facilmente captadas ao explorar dispositivos IoT mal protegidos com sistemas de microfone integrados, como serviços de assistente pessoal (por exemplo, Google Home, Amazon Echo), brinquedos infantis e outros eletrodomésticos controlados por voz. Esses sistemas são vulneráveis a ataques como voz intrusa e mascaramento de voz.
Categoria	Dispositivo
Mitigações	**Criptografia de Ponta a Ponta:** Utilizar criptografia de ponta a ponta para proteger as comunicações de voz entre os dispositivos IoT e os servidores de processamento de voz, garantindo a confidencialidade e a integridade dos dados de voz. **Autenticação de Voz:** Implementar mecanismos robustos de autenticação de voz para verificar a identidade dos usuários e detectar tentativas de spoofing de voz ou falsificação de comandos de voz. **Monitoramento de Tráfego:** Monitorar o tráfego de voz na rede para detectar atividades suspeitas, como tentativas de interceptação de

	comunicações de voz ou manipulação de comandos de voz. **Atualizações de Segurança:** Manter os dispositivos IoT e os aplicativos associados atualizados com as últimas correções de segurança e patches de software para mitigar vulnerabilidades conhecidas que possam ser exploradas nos canais de voz. **Controle de Acesso:** Implementar políticas de controle de acesso para restringir o acesso aos dispositivos IoT e aos sistemas de comunicação de voz, garantindo que apenas usuários autorizados possam interagir com esses dispositivos.
Fontes	- Heartfield, R., Loukas, G., Budimir, S., Bezemskij, A., Fontaine, J.R.J., Filippoupolitis, A., Roesch, E. (2018). A taxonomy of cyber-physical threats and impact in the smart home (Open Access). Computers and Security, 78, pp. 398-428. doi: 10.1016/j.cose.2018.07.011. - Sengupta, J., Ruj, S. and Das Bit, S. (2020). A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT. Journal of Network and Computer Applications, 149, art. no. 102481. doi: 10.1016/j.jnca.2019.102481.

Tabela 10: Interferência de Canal (Rede)

Título	Interferência de Canal
Descrição	Suscetibilidade dos dispositivos IoT a interferências eletromagnéticas ou de sinais em seus canais de comunicação. Essas interferências podem ocorrer de várias formas e podem comprometer a integridade e a confiabilidade das comunicações entre os dispositivos IoT. Ataques de *Jamming* são ataques de disponibilidade contra o meio sem fio ou os sensores voltados para o exterior, onde um dispositivo de interferência pode ser usado para bloquear os sensores do dispositivo de receber sinais.
Categoria	Rede
Mitigações	**Seleção de Canais Livres:** Utilizar ferramentas de análise de espectro para identificar canais de comunicação menos congestionados e menos suscetíveis à interferência, minimizando assim os efeitos da interferência de canal. **Implementação de Técnicas de Mitigação:** Utilizar técnicas de mitigação de interferência, como a seleção dinâmica de canais, controle de potência de transmissão adaptativa e protocolos de correção de erros robustos, para lidar com interferências de forma proativa. **Diversidade de Antenas:** Implementar antenas de diversidade e técnicas de MIMO (*Multiple-Input Multiple-Output*) para melhorar a resiliência da comunicação sem fio e mitigar os efeitos da interferência de canal. **Isolamento e Blindagem:** Isolar fisicamente dispositivos sensíveis à

	interferência eletromagnética ou empregar técnicas de blindagem para reduzir a exposição à interferência externa. **Monitoramento e Diagnóstico:** Implementar sistemas de monitoramento contínuo para detectar e diagnosticar interferências de canal, permitindo uma resposta rápida e eficaz a problemas de desempenho na rede IoT.
Fontes	- Davis B. D., Mason J. C. and Anwar M. (2020). "Vulnerability Studies and Security Postures of IoT Devices: A Smart Home Case Study," in IEEE Internet of Things Journal, vol. 7, no. 10, pp. 10102-10110, doi: 10.1109/JIOT.2020.2983983. - Akhunzada A., Islam S. U. and Zeadally S. (2020), "Securing Cyberspace of Future Smart Cities with 5G Technologies," in IEEE Network, vol. 34, no. 4, pp. 336-342, doi: 10.1109/MNET.001.1900559. - Sengupta, J., Ruj, S. and Das Bit, S. (2020). A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT. Journal of Network and Computer Applications, 149, art. no. 102481. doi: 10.1016/j.jnca.2019.102481.

Tabela 11: Falta de Monitoramento Ativo de Dispositivos (Aplicação)

Título	Falta de Monitoramento Ativo de Dispositivos
Descrição	Ausência de um sistema robusto para monitorar continuamente o status, o comportamento e as atividades dos dispositivos IoT na rede. Monitorar dispositivos IoT pode ser desafiador. Isso ocorre porque a maioria das ferramentas e práticas de monitoramento existentes, especialmente aquelas com foco em nuvem, tradicionalmente foram projetadas para monitorar dados métricos de séries temporais sem foco nos dispositivos IoT modernos ou seus processos. A falta de ferramentas de monitoramento ativo de dispositivos IoT dificulta alcançar uma visibilidade completa da rede em ambientes inteligentes baseados em IoT
Categoria	Aplicação
Mitigações	**Implementação de Sistemas de Monitoramento:** Instalar sistemas de monitoramento contínuo para capturar e analisar dados de atividade, desempenho e segurança dos dispositivos. **Uso de Análise de Comportamento e Detecção de Anomalias:** Aplicar técnicas de aprendizado de máquina e análise de comportamento para identificar padrões incomuns ou suspeitos que possam indicar problemas de segurança. **Gerenciamento e Análise de Logs:** Registrar todas as atividades dos dispositivos e realizar análises periódicas para detectar e investigar atividades suspeitas. **Alertas e Notificações em Tempo Real:** Configurar alertas para

	notificar os administradores de sistemas sobre incidentes ou anomalias em tempo real, permitindo uma resposta rápida a problemas. **Revisão e Atualização de Políticas de Segurança:** Regularmente revisar e atualizar as políticas de segurança e procedimentos operacionais para garantir que estejam alinhados com as melhores práticas e requisitos regulatórios.
Fontes	- Karie N. M. et al. (2021). "A Review of Security Standards and Frameworks for IoT-Based Smart Environments," in IEEE Access, vol. 9, pp. 121975-121995, doi: 10.1109/ACCESS.2021.3109886.

Tabela 12: Aquisição de Dispositivo Não Confiável (*Peopleware*)

Título	Aquisição de Dispositivo Não Confiável
Descrição	Usuários ou organizações adquirem e integram dispositivos IoT em suas redes sem garantir a confiabilidade ou segurança desses dispositivos
Categoria	*Peopleware*
Mitigações	**Avaliação de Segurança Rigorosa:** Implementar processos para avaliar a segurança dos dispositivos antes da compra, incluindo a verificação de certificações de segurança e práticas do fabricante. **Desenvolver Políticas de Aquisição:** Estabelecer políticas e diretrizes claras para a aquisição de dispositivos IoT, que incluam critérios de segurança e confiabilidade. **Treinamento e Conscientização:** Oferecer treinamento e conscientização para os responsáveis pela aquisição sobre os riscos de segurança associados a dispositivos IoT e como avaliá-los adequadamente. **Verificação de Reputação do Fornecedor:** Investigar a reputação e histórico do fornecedor, assegurando que eles tenham um histórico de fornecer produtos seguros e confiáveis. **Testes e Validações:** Realizar testes e validações dos dispositivos adquiridos em ambientes controlados antes de integrá-los ao sistema de produção, para identificar e mitigar problemas de segurança.
Fontes	- Karie N. M. et al. (2021). "A Review of Security Standards and Frameworks for IoT-Based Smart Environments," in IEEE Access, vol. 9, pp. 121975-121995, doi: 10.1109/ACCESS.2021.3109886.

4.2.2.2 Identificando Mitigações para as Vulnerabilidades

Durante o desenvolvimento do catálogo de vulnerabilidades IoT, a inclusão de mitigações para cada vulnerabilidade identificada não foi inicialmente planejada como parte do escopo do trabalho. No entanto, ao longo do estudo, tornou-se evidente que a

disponibilização de orientações práticas para lidar com essas vulnerabilidades seria essencial para aumentar a utilidade do catálogo, tanto para pesquisadores quanto para profissionais de segurança da informação.

A decisão de incluir mitigações foi motivada dado os seguintes fatores:

- As revisões iniciais identificaram as vulnerabilidades, mas nem todas ofereciam soluções diretas, limitando o impacto prático do catálogo.
- Em interações preliminares com o catálogo, foi apontada a importância de associar vulnerabilidades a estratégias de mitigação para facilitar sua adoção em cenários reais.
- A associação de cada vulnerabilidade a medidas preventivas, ou mesmo corretivas, reforça a visão de segurança proativa, essencial para a construção de qualquer sistema.

4.2.2.3 Elaboração do Catálogo

A visualização do catálogo é apresentada por meio de uma interface simples e organizada em categorias de vulnerabilidades (Dispositivo, Rede, Aplicação e *Peopleware*). Cada item do catálogo foi enriquecido com atributos padronizados, como nome, descrição, estratégias de mitigação e referências. Essas referências incluem tanto as fontes das vulnerabilidades quanto os estudos que indicam possíveis mitigações, permitindo que os usuários localizem rapidamente informações relevantes.

Para o armazenamento e publicação do catálogo, foi escolhido o GitHub[2], uma plataforma amplamente utilizada para colaboração e gerenciamento de código. A escolha baseou-se em alguns fatores, como:

- O GitHub permite o acesso público ao catálogo, promovendo a disseminação das informações.
- As ferramentas de controle de versão do GitHub garantem que as alterações no catálogo sejam rastreadas e documentadas.

[2] https://github.com

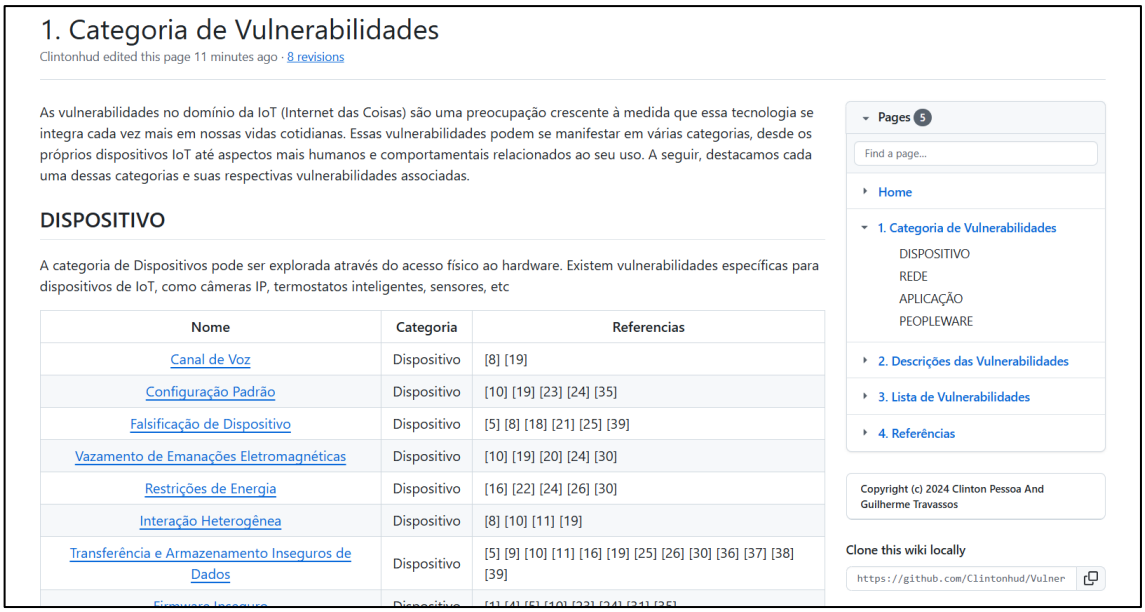
- A compatibilidade com ferramentas de integração de código e automações facilitaria a expansão do catálogo para a construção de artefatos mais automatizados.

O repositório foi estruturado para facilitar a navegação e o uso do catálogo, incluindo um arquivo README com instruções para o redirecionamento para a Wiki do catálogo, contendo seções organizadas para acesso rápido.

Figura 8: Arquivo README.

Figura 9: Página Inicial da WIKI do Catálogo.

A organização do catálogo no GitHub foi complementada com tabelas e links interativos para melhorar a usabilidade. Exemplos de entradas foram destacados para ajudar novos usuários a navegar pelo conteúdo.



1. Categoria de Vulnerabilidades

Clintonhud edited this page 11 minutes ago · 8 revisions

As vulnerabilidades no domínio da IoT (Internet das Coisas) são uma preocupação crescente à medida que essa tecnologia se integra cada vez mais em nossas vidas cotidianas. Essas vulnerabilidades podem se manifestar em várias categorias, desde os próprios dispositivos IoT até aspectos mais humanos e comportamentais relacionados ao seu uso. A seguir, destacamos cada uma dessas categorias e suas respectivas vulnerabilidades associadas.

DISPOSITIVO

A categoria de Dispositivos pode ser explorada através do acesso físico ao hardware. Existem vulnerabilidades específicas para dispositivos de IoT, como câmeras IP, termostatos inteligentes, sensores, etc

Nome	Categoria	Referencias
Canal de Voz	Dispositivo	[8] [19]
Configuração Padrão	Dispositivo	[10] [19] [23] [24] [35]
Falsificação de Dispositivo	Dispositivo	[5] [8] [18] [21] [25] [39]
Vazamento de Emanações Eletromagnéticas	Dispositivo	[10] [19] [20] [24] [30]
Restrições de Energia	Dispositivo	[16] [22] [24] [26] [30]
Interação Heterogênea	Dispositivo	[8] [10] [11] [19]
Transferência e Armazenamento Inseguros de Dados	Dispositivo	[5] [9] [10] [11] [16] [19] [25] [26] [30] [36] [37] [38] [39]

Pages 5

Find a page...

Home

1. Categoria de Vulnerabilidades

DISPOSITIVO

REDE

APLICAÇÃO

PEOPLEWARE

2. Descrições das Vulnerabilidades

3. Lista de Vulnerabilidades

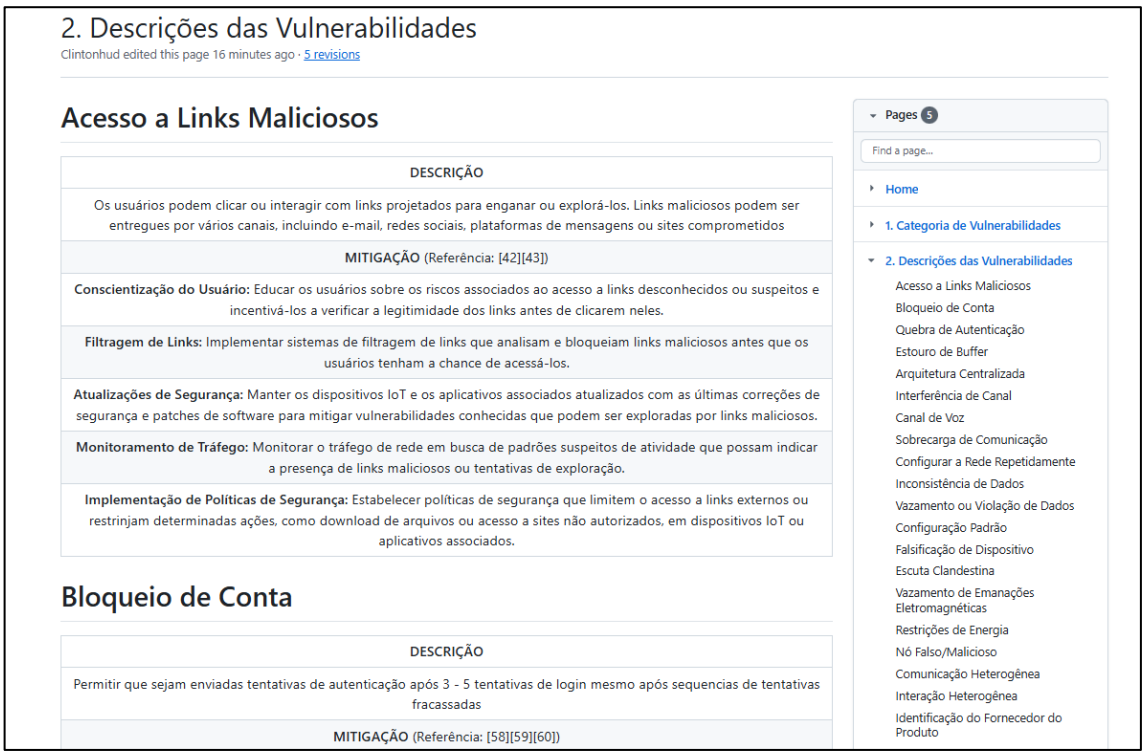
4. Referências

Copyright (c) 2024 Clinton Pessoa And Guilherme Travassos

Clone this wiki locally

https://github.com/Clintonhud/Vulner

Figura 10: Catálogo Estruturado no GitHub Exibindo a Organização por Categorias.



2. Descrições das Vulnerabilidades

Clintonhud edited this page 16 minutes ago · 5 revisions

Acesso a Links Maliciosos

DESCRIÇÃO
Os usuários podem clicar ou interagir com links projetados para enganar ou explorá-los. Links maliciosos podem ser entregues por vários canais, incluindo e-mail, redes sociais, plataformas de mensagens ou sites comprometidos
MITIGAÇÃO (Referência: [42][43])
Conscientização do Usuário: Educar os usuários sobre os riscos associados ao acesso a links desconhecidos ou suspeitos e incentivá-los a verificar a legitimidade dos links antes de clicarem neles.
Filtragem de Links: Implementar sistemas de filtragem de links que analisam e bloqueiam links maliciosos antes que os usuários tenham a chance de acessá-los.
Atualizações de Segurança: Manter os dispositivos IoT e os aplicativos associados atualizados com as últimas correções de segurança e patches de software para mitigar vulnerabilidades conhecidas que podem ser exploradas por links maliciosos.
Monitoramento de Tráfego: Monitorar o tráfego de rede em busca de padrões suspeitos de atividade que possam indicar a presença de links maliciosos ou tentativas de exploração.
Implementação de Políticas de Segurança: Estabelecer políticas de segurança que limitem o acesso a links externos ou restrinjam determinadas ações, como download de arquivos ou acesso a sites não autorizados, em dispositivos IoT ou aplicativos associados.

Bloqueio de Conta

DESCRIÇÃO
Permitir que sejam enviadas tentativas de autenticação após 3 - 5 tentativas de login mesmo após sequencias de tentativas fracassadas
MITIGAÇÃO (Referência: [58][59][60])

Pages 5

Find a page...

Home

1. Categoria de Vulnerabilidades

2. Descrições das Vulnerabilidades

Acesso a Links Maliciosos

Bloqueio de Conta

Quebra de Autenticação

Estouro de Buffer

Arquitetura Centralizada

Interferência de Canal

Canal de Voz

Sobrecarga de Comunicação

Configurar a Rede Repetidamente

Inconsistência de Dados

Vazamento ou Violação de Dados

Configuração Padrão

Falsificação de Dispositivo

Escuta Clandestina

Vazamento de Emanações Eletromagnéticas

Restrições de Energia

Nó Falso/Malicioso

Comunicação Heterogênea

Interação Heterogênea

Identificação do Fornecedor do Produto

Figura 11: Visualização de uma Entrada Específica no Catálogo.

Vale ressaltar que a elaboração do catálogo com base em uma Wiki de repositório público, como o GitHub, apresenta diversas vantagens, além da escalabilidade, que facilita a adição de novas vulnerabilidades e mitigações, destaca-se a portabilidade, permitindo que os usuários clonem ou façam o download do catálogo para uso offline ou integração com outras ferramentas.

4.3 Limitações

A construção do catálogo foi baseada em estudos de literatura e dados técnicos disponíveis em fontes públicas. No entanto, algumas restrições podem ter impactado o escopo das vulnerabilidades incluídas, como:

- As informações provenientes das bases utilizadas para o estudo podem estar incompletas ou desatualizadas, especialmente por se tratar de vulnerabilidades de segurança em dispositivos IoT.
- Algumas falhas específicas, especialmente em dispositivos de fabricantes que não divulgam abertamente seus relatórios de segurança, podem não ter sido incluídas.

Quanto as limitações na identificação das mitigações, embora o catálogo forneça mitigações detalhadas para as vulnerabilidades identificadas, este componente foi integrado posteriormente ao escopo de construção. Isso resultou em limitações na cobertura das mitigações, já que nem todas as vulnerabilidades possuem soluções documentadas, amplamente testadas ou validadas no contexto de IoT. Para superar essas lacunas, nos baseamos em estratégias de mitigação derivadas de instruções fornecidas por ferramentas de inteligência artificial. Além disso, é importante destacar que as mitigações propostas não foram aplicadas em cenários reais durante este estudo.

Estas limitações não comprometem o valor do catálogo, mas apontam áreas de melhoria e expansão para trabalhos futuros. A integração de métodos empíricos para validar mitigações por exemplo, é um passo importante para fortalecer o impacto e a usabilidade do catálogo.

4.4 Considerações Finais

O desenvolvimento do catálogo de vulnerabilidades IoT, conforme apresentado neste capítulo, dispõe de recursos que pretendem auxiliar a área de segurança em sistemas de software IoT. Partindo dos resultados obtidos durante os estudos de revisão, o catálogo consolidou um conjunto estruturado de informações sobre as principais vulnerabilidades de segurança, suas descrições e possíveis formas de mitigação.

O catálogo foi construído com base em um processo sistemático de coleta e organização de dados, integrando fontes acadêmicas e técnicas. A estruturação das informações em um formato padronizado, complementada pela escolha de um repositório público como o GitHub, assegurou a acessibilidade, a transparência e até mesmo a escalabilidade do artefato proposto.

Além de buscar contribuir para a compreensão teórica das vulnerabilidades em sistemas IoT, o catálogo também tem a intenção de seguir como uma ferramenta prática para profissionais e pesquisadores que buscam implementar medidas de segurança em dispositivos conectados.

A criação do catálogo mostra um esforço para enfrentar os desafios crescentes de segurança em um mundo cada vez mais conectado. Ao organizar informações de maneira clara e acessível, buscamos contribuir para a redução de riscos com a utilização de práticas mais seguras no desenvolvimento de sistemas IoT. Apesar das limitações inerentes a um trabalho dessa natureza, buscamos reforçar a importância da segurança como um aspecto essencial no desenvolvimento tecnológico.

É importante lembrar que estamos propondo um catálogo, organizado por categorias que podem ser armazenadas usando a base de dados de um repositório geral para recuperação futura de uma base de conhecimento necessário. Prevemos que este catálogo será usado por pesquisadores e profissionais. Não estamos propondo integrar o catálogo com outros artefatos de software no momento. Portanto, não exploramos outras possibilidades de organização, como, por exemplo, padrões ou frameworks.

Além disso, o catálogo proposto não visa substituir bases consolidadas como o NVD ou CVE, mas sim complementá-las, oferecendo uma visão especializada sobre vulnerabilidades no contexto de sistemas de software IoT. A combinação das informações

contidas no catálogo organizado nesta pesquisa com as informações contidas nesses repositórios pode fortalecer as práticas de gestão de riscos e segurança no desenvolvimento de sistemas de software IoT.

5 Estudo de Viabilidade do Catálogo de Vulnerabilidades IoT

Este capítulo apresenta a avaliação do catálogo de vulnerabilidades IoT, realizado por meio de um survey aplicado a profissionais e pesquisadores da área. A estrutura e a organização da avaliação serão detalhadas ao longo deste capítulo.

5.1 Introdução

Este capítulo tem por objetivo apresentar um estudo da avaliação da viabilidade do Catálogo de Vulnerabilidades IoT por meio de um *survey*, com o objetivo de obter retorno de profissionais da área de segurança. O uso desta estratégia de observação foi escolhido devido à sua capacidade de alcançar um amplo público, permitindo a coleta de dados de diversos perfis de participantes, como pesquisadores, desenvolvedores e profissionais de segurança (EASTERBROOK *et al.*, 2008). Além disso, o *survey* oferece uma valiosa combinação de respostas quantitativas, que possibilitam uma análise objetiva do catálogo, e qualitativas, que permitem uma melhor compreensão das necessidades dos usuários e de suas sugestões de melhoria (WOHLIN *et al.*, 2012).

A aplicação do *survey* focou em avaliar a clareza das informações apresentadas no catálogo, como as descrições das vulnerabilidades e as mitigações propostas, bem como a facilidade de uso da interface e a estrutura do repositório GitHub. O estudo também buscou entender a percepção dos participantes quanto a utilidade prática do catálogo em cenários reais de segurança IoT e identificar possíveis faltas em seu conteúdo ou mesmo na navegação que pudessem ser evoluídas. Os resultados obtidos fornecem percepções valiosas sobre o impacto e eficácia do catálogo.

5.2 Objetivo do Estudo

O principal objetivo deste estudo foi avaliar a viabilidade do Catálogo de Vulnerabilidades IoT como um artefato de apoio prático e informativo para os profissionais e pesquisadores da área de segurança. Por meio de um *survey*, buscamos obter um entendimento sobre a utilidade do catálogo de vulnerabilidades IoT, sua clareza

e sua capacidade de atender às demandas do público-alvo. Mais especificamente, o *survey* teve como objetivos:

- **Validar a Estrutura e Organização do Catálogo:** Verificar se a categorização das vulnerabilidades, a organização das informações e o formato adotado são intuitivos e atendem às expectativas dos usuários. Avaliando a facilidade de uso do repositório GitHub, considerando a navegação e a acessibilidade.
- **Avaliar a Clareza e a Completude das Informações:** Obter retorno sobre a qualidade das descrições das vulnerabilidades e das mitigações sugeridas, identificando possíveis ambiguidades ou mesmo falta de informação.
- **Coletar Sugestões para Melhorias Futuras:** Captar as percepções e recomendações dos participantes para aprimorar o catálogo, tanto em termos de conteúdo quanto de estrutura e apresentação.

Ao alinhar esses objetivos, o estudo buscou não apenas avaliar o artefato desenvolvido, mas também identificar oportunidades para tornar o catálogo uma ferramenta mais robusta e relevante para a comunidade de segurança em sistemas de software IoT.

5.3 Planejamento

Para delinear a realização do estudo de viabilidade do catálogo de vulnerabilidades IoT, foi definido um protocolo a ser seguido pelos pesquisadores. Durante a fase de planejamento do estudo, foram executadas as seguintes atividades: (i) definição do estudo; (ii) seleção e caracterização dos participantes; (iii) definição do formato de execução.

5.3.1 Definição do Estudo

Para avaliar a viabilidade do Catálogo de Vulnerabilidades IoT, foi elaborado e conduzido um estudo experimental baseado na aplicação de um *survey*. Esta etapa foi planejada para coletar os dados qualitativos e quantitativos de participantes do estudo. O estudo seguiu com a definição dos objetivos e dos instrumentos de coleta de dados,

buscando assegurar resultados relevantes e representativos. O estudo foi estruturado da seguinte forma:

5.3.2 Objeto de Estudo

Como objeto de estudo temos o Catálogo de Vulnerabilidades IoT, disponível em: https://github.com/Clintonhud/Vulnerabilidades/wiki.

5.3.3 Objetivo

Nossa proposta está em avaliar a sua eficácia e utilidade do ponto de vista de profissionais que atuam ou já atuaram junto a sistemas de software IoT no contexto das fragilidades de segurança existentes na concepção destes sistemas.

5.3.3.1 Foco da Qualidade

A qualidade das informações coletadas e disponibilizadas para profissionais que atuam no contexto de sistemas IoT devem considerar a **Abrangência e Precisão**, avaliando a cobertura da ampla gama de vulnerabilidades relevantes para sistemas de software IoT; a **Clareza e Completude**, se as descrições são claras e abrangentes o suficiente para ajudar o profissional da prática a entender os riscos; e a **Organização e Navegabilidade**, verificando se o catálogo é bem organizado, permitindo que os usuários encontrem rapidamente as informações necessárias

5.3.3.2 Contexto

O estudo se propõe a ser executado de forma *online*, já que não será necessário um monitoramento contínuo sobre as respostas fornecidas pelos participantes. Os participantes do estudo serão obtidos por conveniência dentre profissionais ou pesquisadores que atuam ou tem interesse na área de segurança de sistemas de software IoT.

5.3.3.3 Questões e Métricas

Para uma avaliação detalhada do catálogo, foram definidas um conjunto de questões e métricas que permitissem medir alguns aspectos, como clareza das informações e usabilidade do repositório. As questões foram formuladas de forma a capturar tanto percepções subjetivas dos participantes quanto dados quantitativos,

possibilitando uma análise mais estruturada dos resultados. Além disso, foram estabelecidas métricas para quantificar a aceitação e a utilidade do catálogo, garantindo uma base sólida para interpretação dos achados do estudo.

Tabela 13: Estratégia para avaliação de viabilidade do catálogo

Viabilidade	Questões	Métricas
Relevância do Catálogo	O catálogo de vulnerabilidades aborda de maneira abrangente os tipos de fraquezas de segurança mais comuns encontradas em sistemas de software IoT?	Taxa de concordância (%) dos profissionais com a abrangência do catálogo em relação às vulnerabilidades de segurança comumente observadas em sistemas de software IoT.
Usabilidade do Catálogo	Os participantes consideram o catálogo de vulnerabilidades fácil de entender e navegar?	Taxa de aceitação (%) da organização geral do catálogo.
	O catálogo de vulnerabilidades fornece informações práticas e acionáveis para mitigar as vulnerabilidades de segurança identificadas?	Classificação média (em uma escala de 1 a 5, por exemplo) da utilidade das informações fornecidas no catálogo para ações de mitigação.
Efetividade na Identificação de Vulnerabilidades	Os participantes conseguem identificar as vulnerabilidades em seus sistemas de software IoT com base nas informações fornecidas pelo catálogo?	Número de vulnerabilidades identificadas com base no catálogo, em comparação com a referência de vulnerabilidades conhecidas pelos participantes.
Satisfação e Utilidade Geral	Os participantes estão satisfeitos com a qualidade e utilidade geral do catálogo de vulnerabilidades?	Classificação média (em uma escala de 1 a 5) da satisfação geral com o catálogo.
	O catálogo de vulnerabilidades atende às expectativas dos participantes em termos de suas necessidades de segurança em sistemas de software IoT?	Taxa de concordância (%) com o atendimento das expectativas do catálogo em relação às necessidades de segurança específicas em sistemas de software IoT.

5.3.4 Seleção e Caracterização dos Participantes

A seleção dos participantes se deu por sua experiência profissional em soluções envolvendo sistemas de software IoT, incluindo especialistas em segurança de sistemas

embarcados, analistas de segurança de rede, pesquisadores em cibersegurança focados em IoT, entre outros. A divulgação do estudo e a obtenção de participantes foram realizadas por meio de múltiplos canais, como redes acadêmicas, plataformas como LinkedIn e grupos de redes sociais, listas de e-mails e divulgação em eventos técnicos e científicos, visando alcançar profissionais e pesquisadores com experiência em segurança de sistemas IoT. No entanto, apesar dos esforços para ampliar o alcance, o número de respondentes foi inferior ao esperado.

Para isso, a Tabela 14 descreve a caracterização dos participantes. Devido a questões de confidencialidade e anonimato, os participantes não foram identificados em suas respostas.

Tabela 14: Características dos participantes

ID	Função Atual	Experiência com IoT	Conhecimento em Segurança	Quantidade de Projetos	Domínio de Aplicações
P1	Engenheiro em Computação	1-2 anos	Conhecimento básico	3 projetos	Saúde
P2	Engenheiro em Computação	1-2 anos	Conhecimento intermediário	2 projetos	Agronegócio, Industria
P3	Analista de Requisitos	6-10 anos	Conhecimento básico	3 projetos	Saúde, Automação Residencial
P4	Analista de Sistemas Computacionais	1-2 anos	Conhecimento intermediário	2 projetos	Educação, Automação Residencial
P5	Gerente de Tecnologia da Informação	3-5 anos	Conhecimento avançado	5 projetos ou mais	Saúde, Agronegócio, Automação Residencial, Industria
P6	Especialista em Segurança de Redes	Mais de 10 anos	Experiente / Especialista	5 projetos ou mais	Automação Residencial, Industria, Energia
P7	Analista de Requisitos	Menos de 1 ano	Conhecimento básico	2 projetos	Agronegócio, Industria

P8	Engenheiro de Requisitos	6-10 anos	Conhecimento avançado	5 projetos ou mais	Saúde, Educação, Automação Residencial, Cidades Inteligentes

5.3.5 Execução

A estruturação do estudo incluiu o detalhamento dos critérios de avaliação, o formato das questões, e os procedimentos para análise dos dados, a fim de garantir uma avaliação abrangente e confiável do catálogo. O *survey* foi aplicado online, por meio de um formulário (*google forms*), com o objetivo de facilitar a participação de profissionais de diferentes localidades.

Para garantir a Ética da Pesquisa, incluímos junto ao formulário o TCLE (Termo de Consentimento Livre e Esclarecido), nos certificando de obter o consentimento informado dos participantes e garantindo ter explicado como as informações serão tratadas para garantir confidencialidade e anonimato das informações repassadas.

Para a resolução das questões indicadas anteriormente, foram conduzidos os seguintes questionamentos:

Perfil do Respondente (Cargo atual, experiência na área de segurança IoT, setores de atuação, etc.)

Tabela 15: Questões sobre o perfil do respondente do formulário de avaliação

Questão 1	Que papel você desempenha atualmente em sua organização?
Questão 2	Você já participou ou participa de projetos voltados para a área de desenvolvimento de sistemas de software IoT?
Questão 3	Há quanto tempo você atua/atuou no desenvolvimento de sistemas de software IoT?
Questão 4	O quanto você conhece sobre segurança em sistemas de software IoT?
Questão 5	Em quantos projetos de desenvolvimento de sistemas de software IoT você participou?
Questão 6	Quais os domínios das aplicações dos projetos de sistemas de software IoT que você participou?

Conhecimento de Trabalhos Semelhantes (Conhecimento prévio de catálogos de vulnerabilidades semelhantes)

Tabela 16: Questão sobre conhecimento de trabalhos semelhantes ao catálogo

Questão 7	Você está familiarizado com algum documento (catálogo) de vulnerabilidades de segurança para sistemas de software?

Usabilidade e Compreensão (Avaliação da clareza e utilidade das informações contidas no catálogo.)

Tabela 17: Questões sobre a usabilidade e compreensão do catálogo

Questão 8	Eu consigo compreender as definições apresentadas para as Categorias de Vulnerabilidades de Segurança em Sistemas de Software IoT.
Questão 9	As vulnerabilidades de segurança em sistemas de software IoT estão consistentes com a categoria associada?
Questão 10	As informações (Descrição e Mitigação) são consistentes com as vulnerabilidades de segurança em sistemas de software IoT.

Relevância e Efetividade do Catálogo (Avaliação da pertinência das vulnerabilidades listadas no catálogo para sistemas de software IoT.)

Tabela 18: Questões sobre a relevância e efetividade do catálogo

Questão 11	Com base em sua experiência, haveria alguma outra categoria que poderia ser utilizada para classificar as vulnerabilidades de segurança de sistemas de software IoT?
Questão 12	Dentre as vulnerabilidades de segurança de sistemas de software IoT categorizadas e listadas no catálogo, existe alguma que você desconhecia?
Questão 13	Você conhece alguma vulnerabilidade de segurança em sistemas de software IoT que não foi apresentada nas categorias que você observou?

Sugestões de Melhoria (Sugestões para aprimorar o catálogo, incluindo ajustes nas descrições de vulnerabilidades, formato das informações, etc.)

Tabela 19: Questões para sugestões de melhoria no catálogo

Questão 14	A organização geral do catálogo de vulnerabilidades de segurança em sistemas de software IoT é adequada?

Questão 15	Você usaria o Catálogo de Vulnerabilidades de Segurança como instrumento de apoio a tomada de decisão em seu próximo projeto de sistemas de software IoT?
Questão 16	Existe alguma informação adicional que você gostaria de obter ao consultar um catálogo de vulnerabilidades de segurança em sistemas de software IoT?

Vale ressaltar que, para o refinamento da organização das questões do formulário online, foi conduzido um estudo piloto inicial. Esse estudo envolveu um grupo reduzido de participantes, buscando identificar possíveis equívocos na estrutura do questionário e verificar se as métricas adotadas eram adequadas para a coleta dos dados desejados. Após a aplicação inicial, os participantes forneceram *sua opinião* sobre a formulação das questões, o tempo necessário para preenchimento e a usabilidade do catálogo elaborado.

Esse processo permitiu identificar oportunidades de melhoria, ajustar a clareza das perguntas e garantir um fluxo mais intuitivo para os respondentes. Esse refinamento foi essencial não apenas para aprimorar a qualidade dos dados coletados na aplicação final do estudo, mas também para aprimorar a estrutura e a apresentação de algumas das informações no próprio catálogo.

5.4 Discussão e Avaliação dos Participantes

Nesta seção, são apresentados os resultados obtidos a partir das respostas dos participantes do *survey*, analisando suas percepções sobre o Catálogo de Vulnerabilidades IoT. A discussão aborda aspectos como a clareza e relevância das descrições, a organização do repositório e a aplicabilidade prática do catálogo. Além disso, são destacadas as opiniões e sugestões dos participantes, destacando pontos fortes e identificando áreas de melhoria que podem orientar futuros aprimoramentos no catálogo.

A partir dos dados de caracterização coletados dos participantes, alguns detalhes podem ser observados, como:

Figura 12: Gráfico do papel do participante na sua organização.

Apesar da pequena população, a diversidade dos perfis dos participantes do *survey* contribuiu para uma avaliação abrangente do Catálogo de Vulnerabilidades IoT. Como apresentado na Figura 12, os participantes desempenham diferentes papéis, destacando com 25% de representatividade cada: Técnico de Desenvolvimento de Sistemas e Engenheiro em Computação. Essa distribuição reflete a relevância do catálogo tanto para profissionais com foco técnico quanto para aqueles envolvidos em aspectos mais gerenciais. Além disso, a presença de analistas de segurança da informação (12,5%) reforça a adequação do catálogo como uma ferramenta alinhada às demandas práticas de segurança.

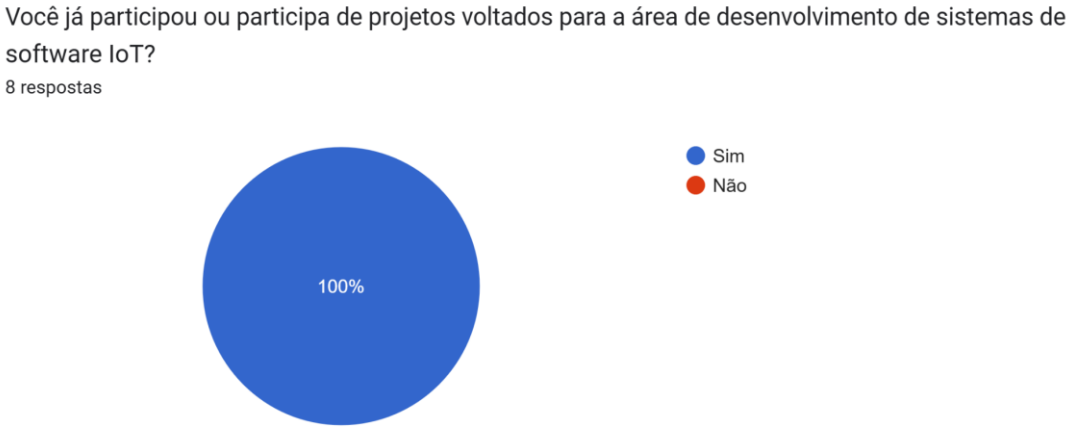


Figura 13: Gráfico sobre a participação em projetos de IoT.

Um dado importante a ressaltar é que 100% dos participantes já possuem experiência em projetos voltados para o desenvolvimento de sistemas de software IoT, como apontado no gráfico da Figura 13. Esse domínio nos proporciona percepções valiosas sobre a aplicabilidade do catálogo em contextos reais de desenvolvimento IoT, a experiência prática dos respondentes nos confere maior credibilidade às respostas do formulário, visto que os participantes têm vivência prática no domínio abordado pelo catálogo.

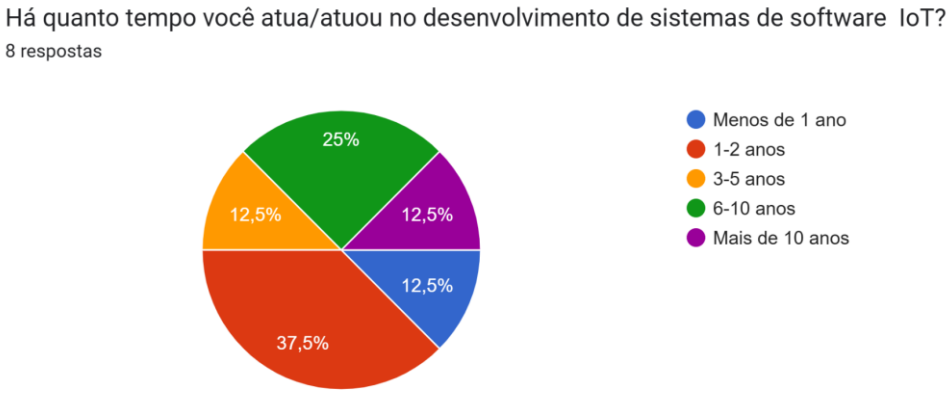


Figura 14: Gráfico sobre o tempo de atuação com desenvolvimento IoT.

O gráfico da Figura 14 evidencia a participação de profissionais tanto com pouca quanto com extensa vivência no campo de IoT, permitindo que o catálogo fosse avaliado sob perspectivas diferentes. Como observado no gráfico, a maior parte dos respondentes (37,5%) possui entre 1 e 2 anos de experiência, enquanto 25% relatam mais de 10 anos de atuação. Outros 12,5% possuem menos de 1 ano, 3-5 anos e 6-10 anos de experiência, respectivamente.

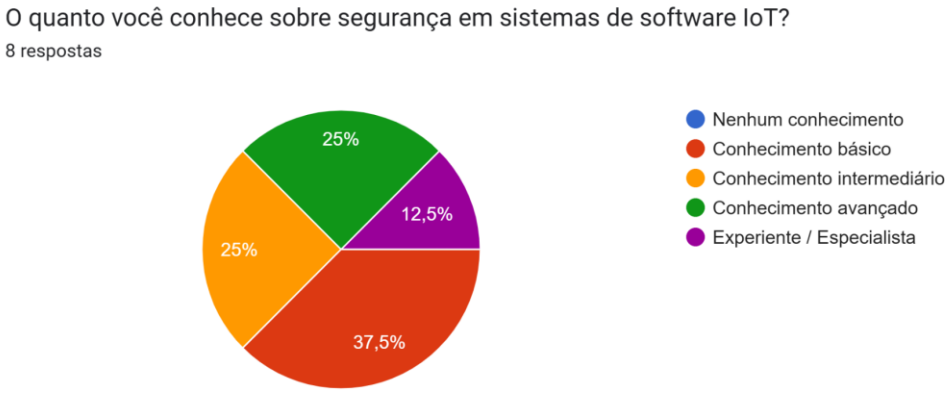


Figura 15: Gráfico sobre o conhecimento prévio sobre segurança em IoT.

Acerca dos dados apresentados no gráfico da Figura 15, podemos observar que a maior parte dos participantes (37,5%) indicam ter ao menos um conhecimento básico no domínio de segurança em sistema IoT. Mantendo nossa base de informações relevantes para o estudo, pois reflete uma base de respondentes com vivências práticas na área em que este estudo se propõe.

Figura 16: Gráfico sobre a participação em projetos de desenvolvimento IoT.

Podemos observar, no gráfico da Figura 16, que, no que diz respeito à participação em projetos IoT, os maiores percentuais estão relacionados à atuação em ao menos 2 projetos e 5 projetos (ambos com 37,5%). Esse dado impacta positivamente a avaliação, pois reflete uma base de participantes com boa experiência prática, o que contribui para uma análise mais robusta do catálogo.

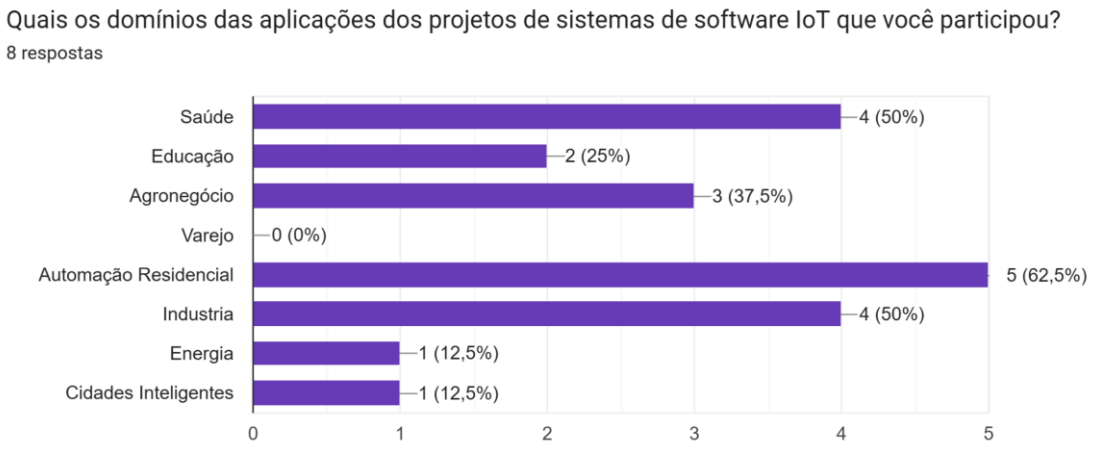


Figura 17: Gráfico dos Domínios de aplicações de IoT que já atuou.

Com base nos dados apresentados no gráfico da Figura 17, é possível observar que os domínios de maior aplicação dos projetos de sistemas de software IoT entre os participantes se destacam Automação Residencial (62,5%), Saúde (50%) e Indústria (50%). Esses resultados indicam uma predominância de áreas tradicionalmente associadas ao uso de IoT para otimização de processos, aumento da eficiência e melhoria da qualidade de vida (REGGIO *et al*., 2020; LOHIYA e THAKKAR, 2021).

Outros domínios, também foram mencionados, o que demonstra a abrangência da IoT em diversos setores. No entanto, áreas como Varejo, Energia e Cidades Inteligentes tiveram pouca ou nenhuma representação, o que pode sugerir um menor nível de adoção do IoT ou uma menor experiência dos participantes nesses campos específicos.

Esses resultados destacam a importância de adaptar o catálogo de vulnerabilidades para atender às demandas de domínios variados, garantindo que ele seja relevante tanto para os setores mais representados quanto para os emergentes.

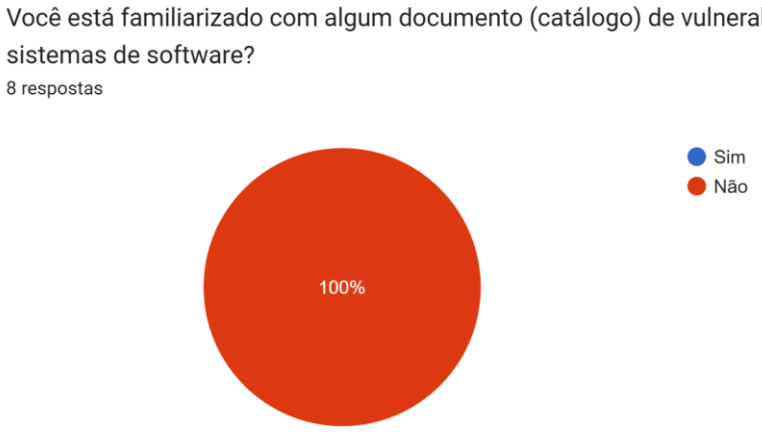


Figura 18: Gráfico sobre a familiaridade com catálogos de vulnerabilidades.

O resultado apresentado no gráfico da Figura 18, indicando que 100% dos participantes não estão familiarizados com documentos ou catálogos de vulnerabilidades de segurança para sistemas de software, reforça a relevância do trabalho desenvolvido, ao apontar uma lacuna de conhecimento ou de materiais acessíveis nesta área específica. Isso sugere que o catálogo de vulnerabilidades IoT criado pode desempenhar um papel importante como um recurso necessário para orientar profissionais e organizações.

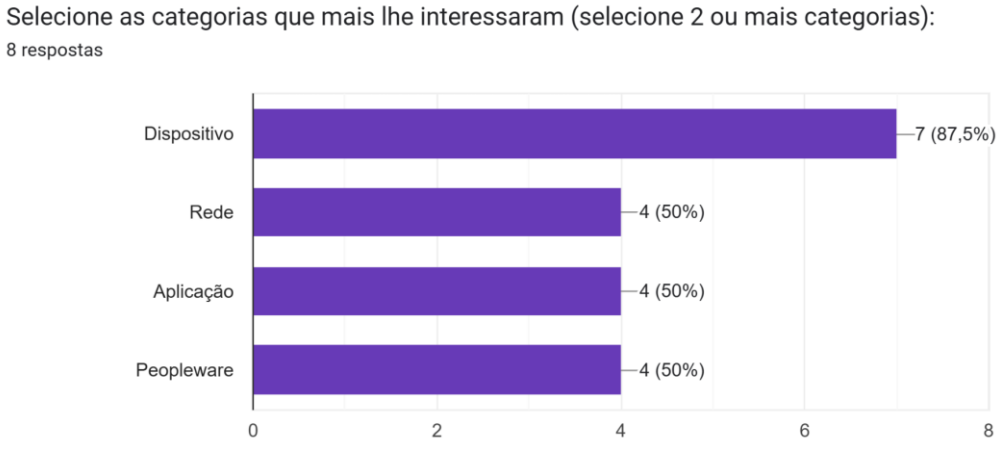


Figura 19: Categorias de interesse.

Os participantes foram solicitados a indicar pelo menos duas das categorias apresentadas no estudo, com o objetivo de obter maior confiança nas informações fornecidas e validar a familiaridade dos respondentes com a estrutura do catálogo.

A categoria que apresentou maior destaque entre as existentes, segundo o gráfico da Figura 19, foi “Dispositivo” (87,5%). Esse resultado pode estar relacionado ao fato de que vulnerabilidades nessa categoria são o foco principal em estudos sobre segurança em sistemas de software IoT, despertando maior interesse pelos participantes. Além disso, questões ligadas à segurança física, integridade e confiabilidade dos dispositivos IoT costumam receber maior atenção, pois representam pontos críticos no contexto de segurança desses sistemas.

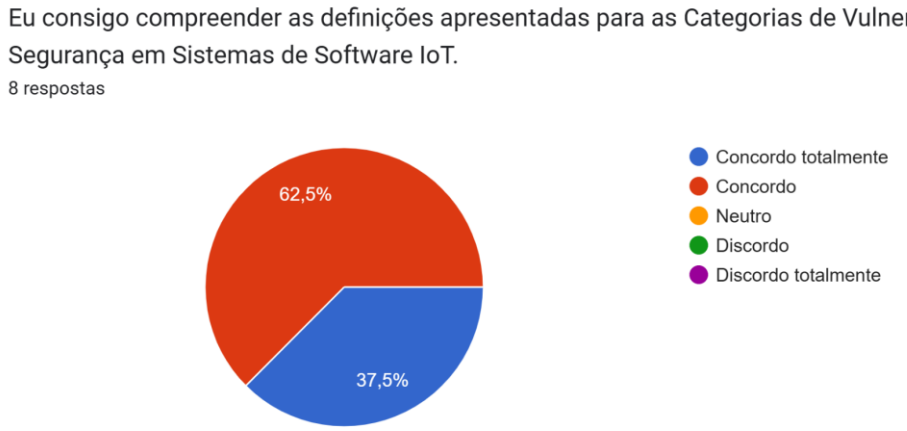


Figura 20: Gráfico sobre a compreensão acerca das definições incluídas no catálogo.

O resultado do gráfico da Figura 20 demonstra que a maioria dos participantes (62,5%) concorda que consegue compreender as definições apresentadas para as categorias de vulnerabilidades de segurança em sistemas de software IoT, enquanto 37,5% concordam totalmente. Esses resultados indicam que as definições e explicações oferecidas no material são claras e acessíveis para os participantes. Além disso, a ausência de respostas indicando discordância ou neutralidade sugere que as definições foram bem comunicadas.

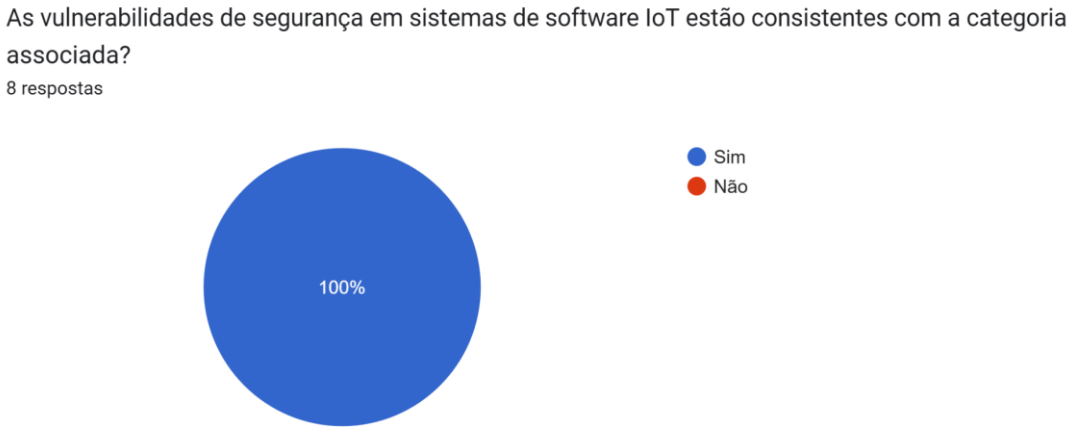


Figura 21: Gráfico sobre a consistência das associações apontados no catálogo.

O gráfico da Figura 21 indica que 100% dos participantes consideram que as vulnerabilidades de segurança em sistemas de software IoT estão consistentes com as categorias associadas. Essa consistência valida a estrutura proposta para categorizar as vulnerabilidades, reforçando a confiabilidade do catálogo como um recurso para auxiliar na prevenção e análise de riscos em sistemas IoT.

Além disso, o alinhamento entre vulnerabilidades e categorias mostra que os conceitos foram apresentados de maneira clara e lógica, o que pode aumentar a aceitação e utilidade do catálogo em cenários reais de desenvolvimento e manutenção de sistemas IoT.

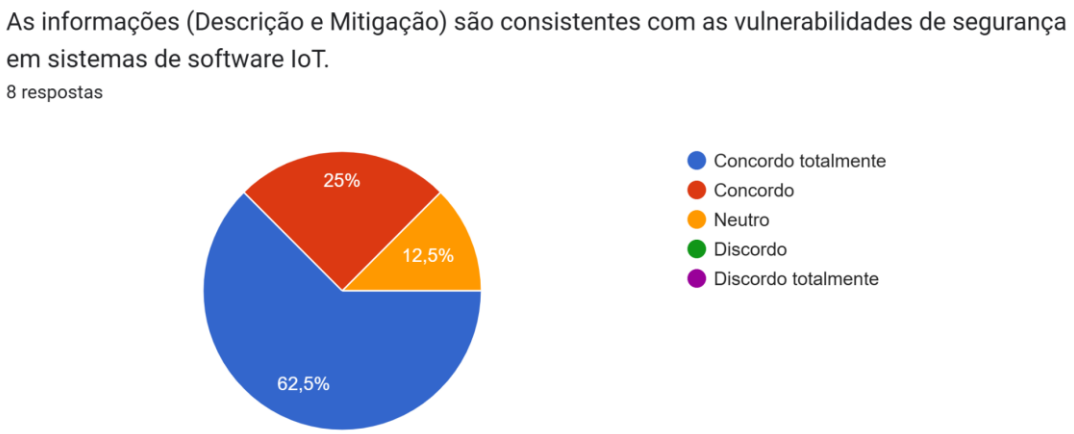


Figura 22: Gráfico sobre a consistência das informações do catálogo.

O gráfico da Figura 22 mostra que a maioria dos participantes (62,5%) concorda totalmente que as informações de descrição e mitigação são consistentes com as vulnerabilidades de segurança em sistemas de software IoT. Além disso, 25% concordam, enquanto 12,5% estão neutros. Nenhum dos participantes discordou ou discordou totalmente.

Esse resultado reforça a qualidade do catálogo utilizado no estudo, na perspectiva dos participantes. A consistência entre as descrições, mitigações e as vulnerabilidades indicam que os dados fornecidos são minimamente claros, sugerindo que o catálogo pode ser um recurso útil para orientar profissionais no entendimento e na aplicação de medidas corretivas para as vulnerabilidades identificadas. No entanto, também observamos a necessidade de revisões e aprimoramentos de algumas das informações descritas, para maximizar a clareza e a correlação entre a vulnerabilidade e as descrições e mitigações apresentadas.

Dentre os questionamentos presentes no *survey*, foi questionado se haveria outra categoria que poderia ser utilizada para classificar as vulnerabilidades de segurança em ambientes IoT. Tivemos uma margem de 75% dos respondentes afirmando não identificar outra categoria, e apenas 25% (dois participantes) sugerindo haver outra categoria a ser considerada. Apenas um deles indicou devidamente a categoria referida: “Falta de fortalecimento físico”.

Ao observamos o conjunto de vulnerabilidades categorizadas, observamos que esse conceito está contemplado na categoria de Dispositivo, com a vulnerabilidade de “Dano Físico”, cuja descrição é “*O dano físico ao equipamento pode ser natural, como resultado de uma calamidade ou mesmo resultante de um ataque físico direto de alguém. Isso pode levar a valores nulos no destino ou valores perdidos, o que pode causar um desequilíbrio no processamento em tempo real dos dados*”.

Dessa forma, podemos inferir que o participante pode não ter percebido essa informação previamente existente no catálogo, visto que, como ele explorou outras categorias além daquelas de seu interesse inicial, é possível que essa exposição a diferentes classificações tenha causado alguma confusão na sua percepção dada a quantidade de vulnerabilidades disponíveis no catálogo.

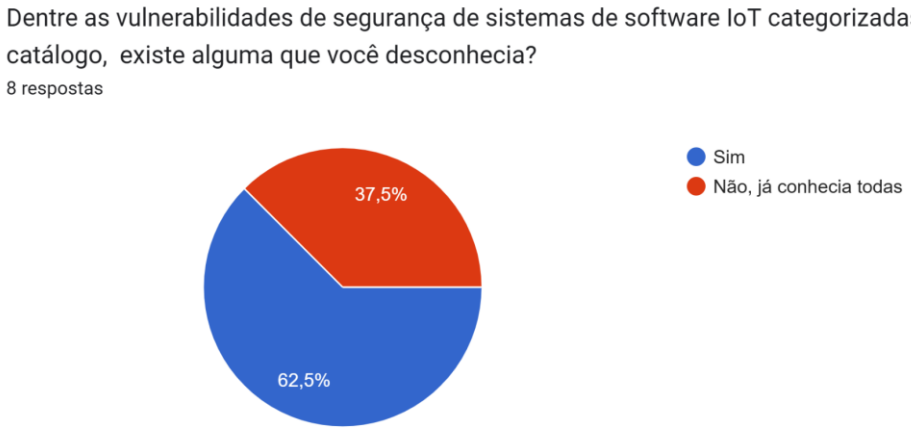


Figura 23: Gráfico sobre vulnerabilidades desconhecidas das fornecidas.

Questionamos também se haveria dentro do conjunto de vulnerabilidades que fornecemos, algumas que ele desconhecia, e o resultado indicou que 62,5% dos participantes desconheciam pelo menos uma das vulnerabilidades listadas no catálogo, como indicado no gráfico da Figura 23.

Esse dado reforça a importância do catálogo como uma ferramenta educativa, ajudando a ampliar o conhecimento sobre vulnerabilidades de segurança em sistemas IoT. Além disso, o fato de 37,5% dos participantes já conhecerem todas as categorias indica que o catálogo está alinhado com as práticas do setor, sem apresentar categorias irrelevantes ou desconhecidas pela comunidade técnica.

Os resultados obtidos podem ser visualizados nos gráficos das figuras abaixo:

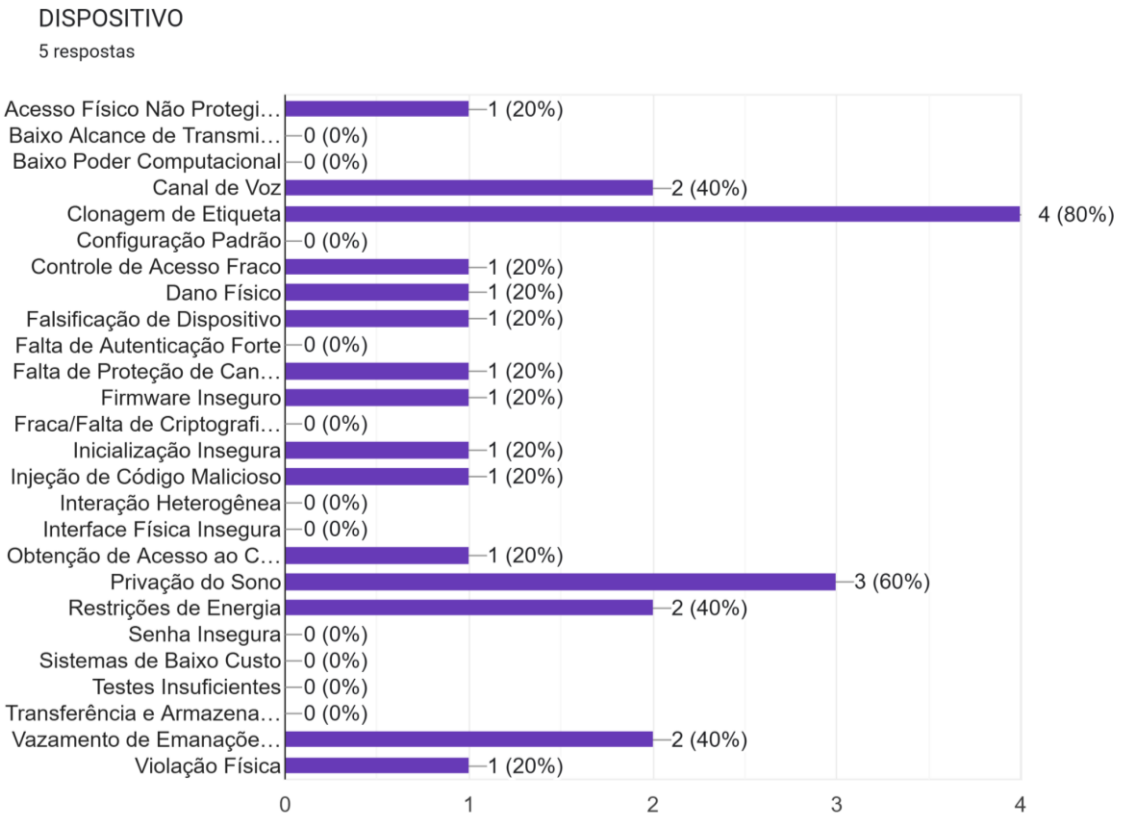


Figura 24: Vulnerabilidades desconhecidas da categoria de Dispositivo.

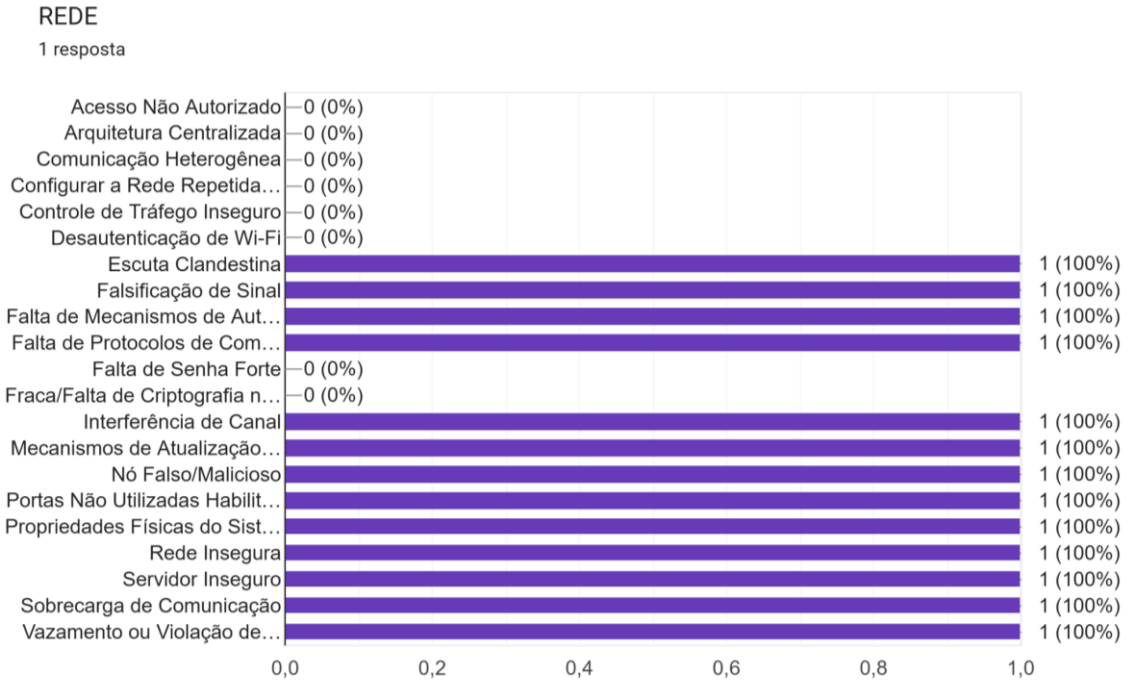


Figura 25: Vulnerabilidades desconhecidas da categoria de rede.

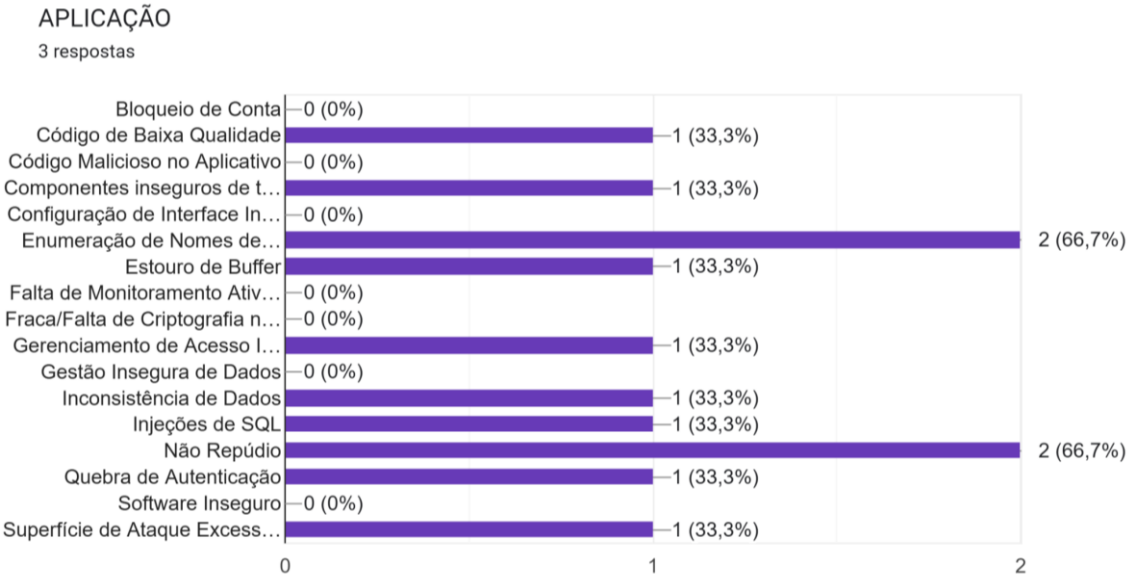


Figura 26: Vulnerabilidades desconhecidas da categoria de aplicação.

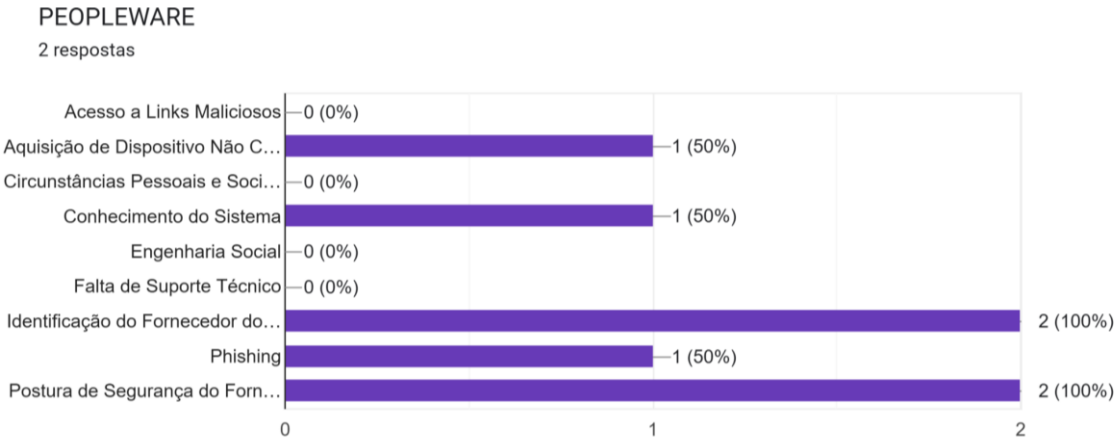


Figura 27: Vulnerabilidades desconhecidas da categoria de *Peopleware*.

Do total de vulnerabilidades identificadas, pelo menos 43 das 73 receberam ao menos uma indicação de desconhecimento por parte dos respondentes. Esse resultado sugere que o material apresentado pode conter informações realmente novas e potencialmente valiosas para profissionais da área de IoT, contribuindo para ampliar o conhecimento sobre riscos e mitigação de vulnerabilidades nesse domínio.

Foi questionado aos participantes sobre o conhecimento de alguma vulnerabilidade que não consta no catálogo, a única sugestão recebida foi do participante que indicou "Falta de fortalecimento físico" como uma nova categoria. Essa indicação corresponde aos 12,5% apontados no gráfico. No entanto, conforme mencionado

anteriormente, esse aspecto já está contemplado no catálogo dentro da categoria Dispositivo, por meio da vulnerabilidade "Dano Físico", conforme discutido anteriormente.

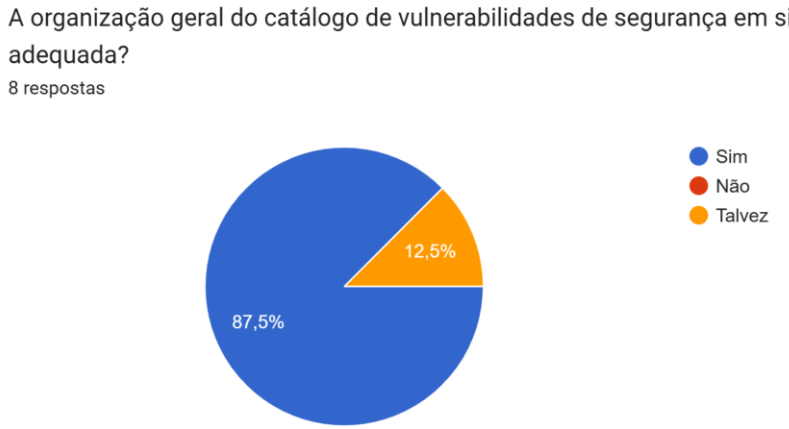


Figura 28: Gráfico sobre a qualidade da organização geral do catálogo.

O gráfico da Figura 28 indica que a grande maioria dos participantes (87,5%) considera a organização geral do catálogo de vulnerabilidades IoT adequada. Apenas 12,5% demonstraram incerteza, respondendo "Talvez", enquanto nenhum participante respondeu "Não".

Esse resultado reforça a validade da estrutura do catálogo e sugere que ele está bem organizado e compreensível para os usuários. No entanto, a presença da resposta "Talvez" sugere que pode haver oportunidades de refinamento. A resposta do participante que selecionou essa opção foi o seguinte:

> “Acredito que mais investigação deveria ser conduzida, uma vez que as tecnologias IOT evoluem e com isso novas vulnerabilidades surgem”

Embora compreendamos a preocupação levantada pelo participante, a justificativa apresentada não está diretamente relacionada à questão avaliada. Isso sugere que a resposta pode ter sido influenciada por uma interpretação diferente do questionamento, o que pode distorcer os resultados apresentados no gráfico.

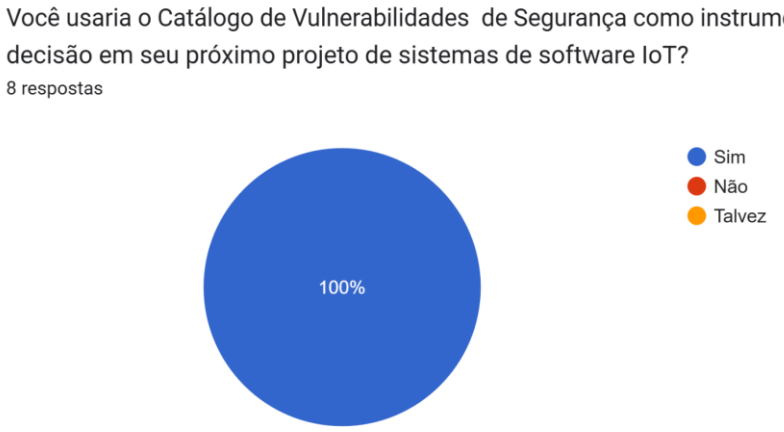


Figura 29: Gráfico sobre a decisão de uso ou não do catálogo para tomada de decisão.

Com 100% dos participantes afirmando que usariam o catálogo como instrumento de apoio à tomada de decisão em seus próximos projetos de sistemas de software IoT, fica fortalecida a percepção de que o material pode ter aplicabilidade prática e é considerado útil pelos participantes do *survey*. Isso sugere uma certa relevância do catálogo e que ele atende a proposta pela qual foi desenvolvido, podendo fornecer informações relevantes para mitigar vulnerabilidades de segurança em sistemas de software IoT.

Dos oito participantes, apenas um deles mencionou um ponto de melhoria e evolução para o catálogo:

> "O catálogo já é bem completo com as descrições e mitigações. Ajuda muito a tomada de decisões relacionadas à segurança de um sistema IoT. Talvez uma informação que poderia ser adicionada ao catálogo seria o nível de risco de segurança que a vulnerabilidade pode trazer ao sistema, considerando as ameaças que ela representa caso não seja mitigada. Porém, não sei se já existe algum tipo de classificação de referência ou estratégia de "*benchmarking*" (ou algo desse tipo) para a avaliação do nível de risco de segurança (ou se isso dependeria do tipo de sistema e do domínio de aplicação)."

Diante disso, um possível avanço para o catálogo seria a inclusão de parâmetros de avaliação para mensurar o nível de impacto das vulnerabilidades de segurança identificadas em sistemas de software IoT. Para isso, poderíamos adotar o *Common Vulnerability Scoring System* (CVSS-SIG) como referência. Essa abordagem pode ser

considerada como um direcionamento para trabalhos futuros, visando a evolução e aprimoramento dos resultados apresentados no catálogo.

5.5 Síntese dos Resultados

Os dados coletados revelam um panorama animador quanto à utilidade e relevância do Catálogo de Vulnerabilidades IoT, indicando que pode ter um potencial como ferramenta eficaz no apoio à segurança desses sistemas. Os principais achados podem ser destacados a seguir:

Nível de Conhecimento e Experiência dos Participantes

A maioria dos participantes já atuou em pelo menos dois projetos de IoT, sendo a Automação Residencial (62,5%), Saúde (50%) e Indústria (50%) os domínios mais frequentes. Nenhum dos participantes estava previamente familiarizado com catálogos de vulnerabilidades de segurança, evidenciando uma lacuna de conhecimento na área.

Relevância do Catálogo

Os participantes indicaram que o catálogo supre uma lacuna importante na área de segurança de sistemas de software IoT, visto que nenhum deles estava familiarizado com documentos semelhantes anteriormente. Além disso, a descoberta de vulnerabilidades desconhecidas por 62,5% dos respondentes reforça o papel instrucional do catálogo e sua pertinência para diferentes domínios de aplicação, como Automação Residencial, Saúde e Indústria.

Usabilidade do Catálogo

A organização do catálogo foi avaliada como adequada pela maioria dos participantes (87,5%), indicando facilidade de navegação e clareza das informações. A ausência de respostas negativas quanto à estrutura sugere que as escolhas de formatação, categorização e linguagem técnica estão alinhadas às expectativas e necessidades dos usuários.

Efetividade na Identificação de Vulnerabilidades

A totalidade dos participantes (100%) concordou que as vulnerabilidades de segurança listadas estão corretamente associadas às categorias definidas. Esse dado sugere existir coerência e precisão do modelo de classificação adotado, indicando que as

informações de descrição e mitigação apresentadas são consideradas consistentes e úteis para o entendimento e enfrentamento de potenciais riscos em sistemas de software IoT.

Satisfação e Utilidade Geral

Todos os respondentes (100%) afirmaram que utilizariam o catálogo como instrumento de apoio à tomada de decisões em projetos futuros, indicando um alto nível de satisfação e percepção de utilidade do catálogo. Esse resultado sugere que o catálogo não apenas auxilia nas necessidades para conhecimento prévio, mas também se apresenta como um possível recurso prático para aplicação no dia a dia profissional.

5.6 Limitações

A aplicação deste estudo de viabilidade apresenta algumas limitações, que devem ser consideradas na interpretação dos resultados, são elas:

Tamanho e Representatividade da Amostra

O estudo foi conduzido com um grupo relativamente pequeno (8 participantes), o que pode não ser representativo de toda a comunidade de profissionais que atuam com segurança em sistemas IoT. A diversidade dos participantes (formação, experiência e áreas de atuação) pode influenciar os resultados e limitar a generalização das conclusões.

Conhecimento Prévio dos Participantes

Como 100% dos participantes indicaram que não estão familiarizados com catálogos de vulnerabilidades, isso pode ter impactado sua percepção inicial sobre a usabilidade e organização do catálogo apresentado. Alguns podem ter dificuldade em avaliar a aplicabilidade do catálogo por falta de experiência prévia com ferramentas similares.

Viés de Resposta e Interpretação

O formato das perguntas pode ter influenciado as respostas, especialmente se não houve opções para críticas detalhadas. Participantes podem ter respondido de forma positiva por viés de cortesia, evitando dar feedbacks negativos.

Avaliação da Efetividade na Prática

O estudo se baseia principalmente em percepções e opiniões, sem uma validação prática do uso do catálogo em projetos reais de IoT. Não há testes práticos medindo se o catálogo realmente ajuda a identificar e mitigar vulnerabilidades em um ambiente real.

5.7 Considerações Finais

Os resultados indicam que o catálogo está bem estruturado, compreensível e relevante, sendo observado como um possível recurso útil na prática de segurança em sistema de software IoT. A ausência de familiaridade prévia com catálogos de segurança reforça a importância desse material como ferramenta educativa. Além disso, a indicação unânime do catálogo como suporte à tomada de decisões sugere que ele pode ser incorporado como possível referencial na área.

Com base nos achados, seria interessante também explorar melhorias na apresentação das informações, utilizando como gancho para estudos futuros a avaliação do impacto do uso do catálogo em projetos reais, verificando sua efetividade na mitigação de vulnerabilidades. Buscando dessa forma fortalecer ainda mais as percepções dos participantes, com iterações em exemplos práticos, ou mesmo, casos de uso para maximizar a aplicabilidade das descrições e mitigações.

6 Conclusão

Este capítulo apresenta os principais resultados obtidos ao longo do estudo para a construção de um catálogo de vulnerabilidades IoT. Além disso, são expostas as considerações finais, destacando as principais contribuições da pesquisa, bem como as perspectivas para trabalhos futuros e possíveis aprimoramentos do catálogo.

6.1 Considerações Finais

Para compreender as conclusões desta pesquisa, é necessário resgatar a questão central que norteou este estudo: **"Quais vulnerabilidades de segurança afetam e podem ser identificadas em sistemas de software IoT?"**. Para responder essa pergunta, foi necessário explorar três aspectos fundamentais:

- Investigar as vulnerabilidades de segurança mais comuns em sistemas de software IoT;
- Elaborar um catálogo de vulnerabilidades IoT como corpo de conhecimento para apoiar a identificação, compreensão e mitigação de riscos em sistemas de software IoT;
- Avaliar a usabilidade e a eficácia de um catálogo de vulnerabilidades para IoT para fornecer uma referência estruturada para os profissionais e pesquisadores da área;

Como resultado dos estudos de revisão aplicados, foi possível identificar e organizar um conjunto com 73 vulnerabilidades de segurança para sistemas IoT, categorizando-as em quatro grupos: “Dispositivo”, “Rede”, “Aplicação” e “*Peopleware*”. Essa classificação teve por objetivo facilitar a compreensão e o tratamento das vulnerabilidades, além de revelar uma necessidade em aplicar investigações adicionais acerca do impacto do fator humano na segurança desses sistemas, classificadas neste estudo como “*Peopleware*”. Vale destacar ainda, em relação ao nível de granularidade das vulnerabilidades identificadas, optou-se por uma abordagem mais abrangente, evitando restringir-se apenas a vulnerabilidades muito específicas que surgem e

desaparecem rapidamente. Essa decisão buscou garantir que o catálogo mantenha certa relevância ao longo do tempo, apoiando a identificação e mitigação de possíveis ameaças em sistemas de software IoT.

A elaboração do catálogo considerou todas as vulnerabilidades mapeadas, organizando-as de forma estruturada e disponibilizando informações sobre sua categoria, descrição, possíveis formas de mitigação e referências, tanto das descrições quanto das possíveis formas de mitigações apresentadas. O catálogo foi desenvolvido no formato de uma wiki de consulta, hospedada no GitHub, buscando garantir maior acessibilidade, flexibilidade para atualizações e maior disseminação do conhecimento em uma plataforma conhecida pela comunidade técnica.

A avaliação realizada com profissionais da área indicou uma percepção positiva quanto à relevância e à utilidade do catálogo de vulnerabilidades proposto. Os resultados, apesar da pequena população, apontaram que a maioria dos respondentes considerou as descrições e medidas de mitigação consistentes e aplicáveis aos contextos práticos de desenvolvimento de sistemas IoT. Além disso, a estrutura do catálogo foi considerada adequada para consulta, com informações organizadas e consistentes.

Dessa forma, este trabalho busca servir como um recurso de apoio para a aplicação de práticas de segurança na construção de sistemas de software IoT, fornecendo uma abordagem estruturada com classificação, identificação e mitigação de diversas vulnerabilidades de segurança Além de contribuir para o entendimento dessas vulnerabilidades, espera-se que os achados apresentados sirvam como base para investigações futuras, possibilitando a ampliação do conhecimento na área e incentivando a evolução contínua das práticas de segurança nesses sistemas.

6.2 Contribuições

As principais contribuições desta pesquisa incluem:

- Identificação e classificação das vulnerabilidades mais frequentes e críticas em sistemas de software IoT, com base em uma revisão *Ad-hoc* de relatórios e diretrizes de organizações do setor, e em uma revisão estruturada da literatura técnica.

- Desenvolvimento de um catálogo estruturado de vulnerabilidades de segurança para sistemas IoT, que pode ser utilizado por profissionais da área para melhor compreender e mitigar riscos associados as vulnerabilidades desses sistemas.
- A identificação de melhorias, desafios e limitações através da avaliação empírica da usabilidade e relevância do catálogo na percepção de profissionais que lidam com segurança de sistemas de software IoT.
- A proposição de uma estrutura que abre caminho para estudos futuros, especialmente na avaliação quantitativa do impacto das vulnerabilidades identificadas e na criação de ferramentas automatizadas para análise de riscos em IoT, permitindo uma abordagem mais dinâmica e eficiente na mitigação das vulnerabilidades.

6.3 Limitações da Pesquisa

As principais limitações desta dissertação são:

- A amostra de profissionais consultados para avaliação do catálogo foi relativamente pequena, que pode impactar significativamente na generalização dos achados.
- O catálogo foi desenvolvido com base em literatura e avaliações um pouco mais qualitativas, sendo necessária uma validação quantitativa mais ampla, possivelmente em cenários reais de implementação.
- A percepção das vulnerabilidades e a capacidade de percepção das formas de mitigação podem variar entre os profissionais, o que pode influenciar na adoção do catálogo.
- O contexto de segurança em IoT está em constante evolução, demandando revisões e atualizações frequentes, uma vez que novas vulnerabilidades podem emergir, acompanhadas de diferentes focos e estratégias de ataque.
- Uma investigação complementar utilizando a base taxonômica do CWE (*Common Weakness Enumeration*), por meio de buscas sistemáticas com palavras-chave relacionadas a fraquezas específicas no contexto de IoT, poderia ter ampliado o mapeamento inicial, possibilitando a identificação de fraquezas estruturais relevantes que não emergiram diretamente dos

estudos identificados por meio da revisão *Ad-hoc*, o que poderia fornecer algum alinhamento com padrões de segurança reconhecidos internacionalmente.

6.4 Perspectivas e Desafios Futuros

Com base nos resultados obtidos, algumas direções para pesquisas futuras são sugeridas:

- **Integração do nível de impacto das vulnerabilidades,** permitindo dessa forma uma classificação com base em métricas como CVSS, para atribuir gravidade e prioridade aos diferentes tipos de vulnerabilidades identificadas.
- **Desenvolvimento de mecanismos automatizados** para a identificação e classificação de vulnerabilidades, reduzindo a necessidade de análise manual das avaliações.
- **Estudos sobre o impacto do fator humano na segurança de IoT**, considerando aspectos como erros de configuração, comportamento do usuário, desafios de treinamento, entre outros fatores levantados junto às vulnerabilidades classificadas na categoria de *Peopleware*.
- **Análise das políticas e regulamentações de segurança** para IoT, investigando como normas e padrões podem ser incorporados ao desenvolvimento de sistemas mais seguros.
- **Integração entre os achados experimentais e a taxonomia formal da CWE**, visando identificar pontos de alinhamento, sobreposição, lacunas e, sobretudo, as contribuições inovadoras que este catálogo oferece. Esse alinhamento poderá contribuir tanto para o enriquecimento do catálogo quanto para fortalecer seu entendimento em conjunto com padrões de segurança reconhecidos internacionalmente.

Referências Bibliográficas

ABDALLA, P. AND VAROL, C. (2020). “Testing IoT Security: The Case Study of an IP Camera”. 8th IEEE ISDFS. Beirut, Lebanon, pp. 1–5. https://doi.org/10.1109/ISDFS49300.2020.9116392

AHLUWALIA, A., GARG, D.V., KAPOOR, D.S., & GUPTA, D.L. (2024). “The Internet of Things (IoT): Transformations and Challenges in the Modern World”. African Journal of Biological Sciences. DOI: 10.48047/AFJBS.6.3.2024.764-769

ALDAHMANI, A., OUNI, B., LESTABLE, T., DEBBAH, M. (2023). “Cyber-Security of Embedded IoTs in Smart Homes: Challenges, Requirements, Countermeasures, and Trends”. IEEE Open Journal of Vehicular Technology. 4, 281–292. https://doi.org/10.1109/OJVT.2023.3234069

ALI, R.F., MUNEER, A., DOMINIC, P.D., TAIB, S.M. AND GHALEB, E.A. (2021). “Internet of Things (IoT) Security Challenges and Solutions: A Systematic Literature Review”. In: Abdullah, N., Manickam, S., Anbar, M. (eds) Advances in Cyber Security. Communications in Computer and Information Science, vol 1487. Springer, Singapore. https://doi.org/10.1007/978-981-16-8059-5_9

ALFADEL, M., COSTA, D., SHIHAB, E. (2023). “Empirical Analysis of Security Vulnerabilities in Python Packages”. Empirical Software Engineering 28, 59. https://doi.org/10.1007/s10664-022-10278-4

ALQASSEM, I. AND SVETINOVIC, D. (2014). “A Taxonomy of Security and Privacy Requirements for the Internet of Things (IoT)”. IEEE International Conference on Industrial Engineering and Engineering Management, pp. 1244–1248. https://doi.org/10.1109/IEEM.2014.7058837

AL ABDULWAHID, A., CLARKE, N., FURNELL, S., STENGEL, I. AND REICH, C. (2015). “The Current Use of Authentication Technologies: An Investigative Review”. International Conference on Cloud Computing (ICCC), Riyadh, Saudi Arabia, 2015, pp. 1-8, doi: 10.1109/CLOUDCOMP.2015.7149658

AMMAYAPPAN, K., PUTHUPARAMBIL, A.B., AND NEGI, A. (2020). "Key Vulnerabilities in Internet of Things: A Holistic View." Applied Approach to

Privacy and Security for the Internet of Things, edited by Parag Chatterjee, et al., IGI Global, 2020, pp. 38-54. https://doi.org/10.4018/978-1-7998-2444-2.ch002

ARORA, A., KAUR, A., BHUSHAN, B., SAINI, H. (2019). “Security Concerns and Future Trends of Internet of Things. International Conference on Intelligent Computing”. Instrumentation and Control Technologies, pp. 891–896. https://doi.org/10.1109/ICICICT46008.2019.8993222

ATZORI, L., IERA, A. AND MORABITO, G. (2010). “The Internet of Things: A Survey”. Computer Networks, vol. 54, nº 15, p. 2787–2805, out. 2010, doi: 10.1016/j.comnet.2010.05.010

BAHO, S. AND ABAWAJY, J. (2023). “Analysis of Consumer IoT Device Vulnerability Quantification Frameworks”. Electronics, 12, 1176. https://doi.org/10.3390/electronics12051176

BARISIC, A. AND CUNHA, J. (2017). “Sustainability in Modelling of Cyber-Physical Systems: A Systematic Literature Review”. Intermediate Technical Report (Research Report). Universidade NOVA de Lisboa. https://hal.science/hal-03168839

BELLI, L. (2020). “Uma Perspectiva de Direitos Humanos para Decriptar a Ascensão da Internet das Coisas (IoT)”. Revista Brasileira De Direitos Fundamentais & Justiça, 13(41), 157–181. https://doi.org/10.30899/dfj.v13i41.775

BIOLCHINI, J., MIAN, P. G., NATALI, A. C. C. AND TRAVASSOS, G. H. (2005). “Systematic Review in Software Engineering”. Technical Report-ES 679/05. Systems Engineering and Computer Science Department COPPE/UFRJ. Access in: https://www.cos.ufrj.br/uploadfile/es67905.pdf

BOCHIE, K., GONZALEZ, E., GISERMAN, L., CAMPISTA, M., COSTA, L. (2020). “Detecção de Ataques a Redes IoT Usando Técnicas de Aprendizado de Máquina e Aprendizado Profundo”. XX SBSEG. SBC, Brasil, pp. 257–270. https://doi.org/10.5753/sbseg.2020.19242

BROWN, E., & KETEL, M. (2020). “The Internet of Things: Architecture, Security Threats, and Risk Mitigation Techniques”. International Journal of Computer Science and Security (IJCSS). vol. 14, 5, pp. 187-199.

CARLOS, R. e MATTOS, C. (2021). “O Impacto da Internet das Coisas como Facilitadora para Práticas de Economia Circular”. XLI Encontro Nacional de Engenharia de Produção (ENEGEP 2021). Online.

CHHETRI, C. AND MOTTI, V. (2021). “Identifying Vulnerabilities in Security and Privacy of Smart Home Devices”. Advances in Intelligent Systems and Computing, 1271, 211–231. https://doi.org/10.1007/978-3-030-58703-1_13

DA SILVA, D., SOUZA, B. P., GONÇALVES, T., AND TRAVASSOS, G. (2020). “Uma Tecnologia para Apoiar a Engenharia de Requisitos de Sistemas de Software IoT”. XXIII Ibero-American Conference on Software Engineering. Curitiba, Brazil (Online), p S09 P3:14 pages.

DAVIS, B., MASON, J., ANWAR, M. (2020). “Vulnerability Studies and Security Postures of IoT Devices: A Smart Home Case Study”. IEEE Internet of Things Journal, 7, 10102–10110. https://doi.org/10.1109/JIOT.2020.2983983

EASTERBROOK, S., SINGER, J., STOREY, M.-A., & DAMIAN, D. (2008). “Selecting Empirical Methods for Software Engineering Research”. In F. Shull, J. Singer, & D. Sjøberg (Eds.), *Guide to Advanced Empirical Software Engineering* (pp. 285–311). Springer. https://doi.org/10.1007/978-1-84800-044-5_11

EJAZ, W., ANPALAGAN, A., IMRAN, M.A., JO, M., NAEEM, M., QAISAR, S.B., & WANG, W. (2016). “Internet of Things (IoT) in 5G Wireless Communications”. IEEE Access, 4, 10310-10314.

FORTUNA, B., RUPNIK, J., BRANK, J., FORTUNA, C., JOVANOSKI, V., MARIO, KARLOVCEC, KAZIC, B.M., KENDA, K., LEBAN, G., MUHIC, A., NOVAK, B., JOST, NOVLJAN, PAPLER, M., REI, L., SOVDAT, B., STOPAR, L., GROBELNIK, M., DUNJA, & MLADENIĆ. (2014). “QMiner: Data Analytics Platform for Processing Streams of Structured and Unstructured Data”.

GROMOV, M., ARNOLD, D., AND SANIIE, J. (2022). “Tackling Multiple Security Threats in an IoT Environment”. 2022 IEEE International Conference on Electro Information Technology (eIT), 290-295.

GUBBI, J., BUYYA, R., MARUSIC, S., PALANISWAMI, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation

Computer Systems, v. 29, n. 7, p. 1645-1660, doi: 10.1016/j.future.2013.01.010

HARBI, Y., ALIOUAT, Z., HAROUS, S., BENTALEB, A., REFOUFI, A. (2019). “A Review of Security in Internet of Things”. Wireless Personal Communications, 108, 325–344. https://doi.org/10.1007/s11277-019-06405-y

ISO/IEC 27000. (2018). “Information technology — Security techniques — Information security management systems — Overview and vocabulary”. Acessado em 05/10/2023. Disponível em: https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html

KAMORU, O.K., FRANK, I., & YEMI, A. (2014). “Computer Security Measures, Tools and Best Practices”. British Journal of Applied Science and Technology, 4, 4380-4394.

KARIE, N. M., SAHRI, N. M., YANG, W., VALLI, C., KEBANDE, V. R. (2021). "A Review of Security Standards and Frameworks for IoT-Based Smart Environments." IEEE Access, 9, 121975–121995. https://doi.org/10.1109/ACCESS.2021.3109886

KARIRI, E. (2022). “IoT Powered Agricultural Cyber-Physical System: Security Issue Assessment”. IETE Journal of Research. https://doi.org/10.1080/03772063.2022.2032848

KHAN, M., AND SALAH, K. (2018). "IoT Security: Review, Blockchain Solutions, and Open Challenges”. Future Generation Computer Systems, 82, 395–411. https://doi.org/10.1016/j.future.2017.11.022

KHAN, W., AHMED, E., HAKAK, S., YAQOOB, I., AHMED, A. (2019). Edge computing: A survey. Future Generation Computer Systems, v. 97, p. 219-235, doi: 10.1016/j.future.2019.02.050

KOZIOLEK, H. (2011). "Sustainability Evaluation of Software Architectures: A Systematic Review". QoSA-ISARCS '11, Association for Computing Machinery, pp. 3–12. https://doi.org/10.1145/2000259.2000263

KORONA, M., ZABOŁOTNY, B., KOZIOŁ, F., BIERNACKI, M., GIERMAKOWSKI, R., RURKA, P., CHMIEL, M., & RAWSKI, M. (2023). “IoTrust - a HW/SW Framework Supporting Security Core Baseline Features for IoT”. 2023 18th

Conference on Computer Science and Intelligence Systems (FedCSIS), 1029-1034.

KUHRMANN, M., FERNÁNDEZ, D. M., DANEVA, M. (2017). "On the Pragmatic Design of Literature Studies in Software Engineering: An Experience-Based Guideline". Empirical Software Engineering, 22(6).

LACERDA, F., & LIMA-MARQUES, M. (2015). "Da Necessidade de Princípios de Arquitetura da Informação para a Internet das Coisas". Perspectivas em Ciência da Informação, 20(2), 158–171. https://doi.org/10.1590/1981-5344/2356

LI, Y. (2024). "Ensuring the Security of the Internet of Things: A Deep Dive Into Current Network Weaknesses and Approaches for Strengthening". Applied and Computational Engineering.

LIU, X., QIAN, C., HATCHER, W.G., XU, H., LIAO, W., & YU, W. (2019). "Secure Internet of Things (IoT)-Based Smart-World Critical Infrastructures: Survey, Case Study and Research Opportunities". IEEE Access, 7, 79523-79544.

LOHIYA, R. AND THAKKAR, A. (2021). “Application Domains, Evaluation Data Sets, and Research Challenges of IoT: A Systematic Review”. IEEE Internet of Things Journal, 8, 8774-8798.

LUIGI ATZORI, ANTONIO IERA, GIACOMO MORABITO. (2010). "The Internet of Things: A Survey". Computer Networks, 54(15), 2787-2805. https://doi.org/10.1016/j.comnet.2010.05.010

MENEGHELLO, F., CALORE, M., ZUCCHETTO, D., POLESE, M., & ZANELLA, A. (2019). "IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices". IEEE Internet of Things Journal, 6, 8182-8201.

MITRE. *Common Vulnerabilities and Exposures (CVE)*. Disponível em: https://cve.mitre.org/. Acesso em: 09 de junho de 2025

MOHER, D., STEWART, L., SHEKELLE, P. (2015). "All in the Family: Systematic Reviews, Rapid Reviews, Scoping Reviews, Realist Reviews, and More". Systematic Reviews, 4, 183. https://doi.org/10.1186/s13643-015-0163-7

MOTTA[1], R. C., SILVA, V., TRAVASSOS, G. H. (2019). "Towards a More In-Depth

Understanding of the IoT Paradigm and Its Challenges". JSERD, 7, 3. https://doi.org/10.5753/jserd.2019.14

MOTTA², R., OLIVEIRA, K., TRAVASSOS, G. (2019). "A Conceptual Perspective on Interoperability in Context-Aware Software Systems". Information and Software Technology, 114, 231–257. https://doi.org/10.1016/j.infsof.2019.07.001

MOURÃO, E., PIMENTEL, J., MURTA, L., KALINOWSKI, M., MENDES, E., WOHLIN, C. (2020). "On the Performance of Hybrid Search Strategies for Systematic Literature Reviews in Software Engineering". Information and Software Technology, 123, 106294. https://doi.org/10.1016/j.infsof.2020.106294

NIST. *National Vulnerability Database (NVD)*. Disponível em: https://nvd.nist.gov/. Acesso em: 09 de junho de 2025

NOBLE, H., AND MITCHELL, G. (2016). "What is Grounded Theory?" Evidence Based Nursing, 19, 34–35. https://doi.org/10.1136/eb-2016-102306

ONGUN, T., SPOHNGELLERT, O., OPREA, A., NITA-ROTARU, C., CHRISTODORESCU, M., & SALAJEGHEH, N. (2018). "The House That Knows You: User Authentication Based on IoT Data". Proceedings of the ACM SIGSAC Conference on Computer and Communications Security.

OWASP. (2016). “Category: Vulnerability”. Acessado em 05/10/2023. Disponível em: https://wiki.owasp.org/index.php/Category:Vulnerability

PAES, V., PESSOA, C., COSTA, V., OLIVEIRA, L, SOUZA, J. (2022). "IoE Knowledge Flow Model in Smart Cities". IEEE SMC, pp. 982–987. https://doi.org/10.1109/SMC53654.2022.9945275

PANCHAL, A. C., KHADSE, V. M., MAHALLE, P. N. (2018). "Security Issues in IIoT: A Comprehensive Survey of Attacks on IIoT and Its Countermeasures". IEEE Global Conference on Wireless Computing and Networking (GCWCN), Lonavala, India, pp. 124-130. https://doi.org/10.1109/GCWCN.2018.8668630

PATIL, A., RANA, D., VICHARE, S., AND RAUT, C. (2018). "Effective Authentication for Restricting Unauthorized Users". International Conference on Smart City and Emerging Technology (ICSCET), Mumbai, India, pp. 1-4. https://doi.org/10.1109/ICSCET.2018.8537323

PEDREIRA, V., BARROS, D., PINTO, P. (2021). "A Review of Attacks, Vulnerabilities, and Defenses in Industry 4.0 with New Challenges on Data Sovereignty Ahead". Sensors, 21(15), 5189. https://doi.org/10.3390/s21155189

PESSOA, C. AND TRAVASSOS, G. Categorizing IoT Software Systems Security Vulnerabilities Through Literature Studies. In: SIMPÓSIO BRASILEIRO DE ENGENHARIA DE SOFTWARE (SBES), 38. , 2024, Curitiba/PR. Anais [...]. Porto Alegre: Sociedade Brasileira de Computação, 2024. p. 169-180. ISSN 2833-0633. DOI: https://doi.org/10.5753/sbes.2024.3346

PETTICREW, M., AND ROBERTS, H. (2006). “Systematic Reviews in the Social Sciences”. Blackwell Publishing Ltd, Oxford, UK. https://doi.org/10.1002/9780470754887

PRAKASH, R., JYOTI, N., MANJUNATHA, S. (2024). "A Survey of Security Challenges, Attacks in IoT". E3S Web of Conferences.

RALPH, P., & BALTES, S. (2022). "Paving the Way for Mature Secondary Research: The Seven Types of Literature Review". Proceedings of the 30th ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering.

REGGIO, G., LEOTTA, M., CERIOLI, M., SPALAZZESE, R., & ALKHABBAS, F. (2020). “What Are IoT Systems for Real? An experts' Survey on Software Engineering Aspects”. Internet Things, 12, 100313.

RIGATIERI, V. (2018). "IoT e a Nova Fronteira para os ISP Regionais no Brasil". Revista Segurança Eletrônica. Disponível em: https://revistasegurancaeletronica.com.br/iot-e-a-nova-fronteira-para-os-isp-regionais-no-brasil.

ROOHI, A., ADEEL, M., & SHAH, M. A. (2019). "DDoS in IoT: A Roadmap Towards Security & Countermeasures". 25th International Conference on Automation and Computing (ICAC), Lancaster, UK, pp. 1-6. https://doi.org/10.23919/IConAC.2019.8895034

SAHMI, I., MAZRI, T., & HMINA, N. (2019). "Study of the Different Security Threats on the Internet of Things and Their Applications". ACM International Conference

Proceeding Series. https://doi.org/10.1145/3320326.3320402

SEVERI, L. D. M. (2024). “Conectividade e Saúde: Uma Revisão Crítica da Literatura Sobre a Inserção da IoT no Contexto Médico”. Trabalho de Conclusão de Curso (Graduação em Engenharia de Computação) – Universidade Federal de São Carlos, São Carlos. Disponível em: https://repositorio.ufscar.br/handle/20.500.14289/19341

SHEIKH, Z., & SINGH, Y. (2022). "A Hybrid Threat Assessment Model for Security of Cyber Physical Systems". 7th IEEE International Conference on Parallel, Distributed and Grid Computing (PDGC), pp. 582–587. https://doi.org/10.1109/PDGC56933.2022.10053332

SHAH, Y., & SENGUPTA, S. (2020). "A Survey on Classification of Cyber-attacks on IoT and IIoT Devices". 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York, NY, USA, pp. 0406-0413. https://doi.org/10.1109/UEMCON51285.2020.9298138

SILVA, H. A. (2019). "A Caixa de Ferramentas Conceituais de Richard Rorty: O Uso de Técnicas Ad Hoc". Cognitio-Estudos: Revista Eletrônica de Filosofia, 16, 257–267. https://doi.org/10.23925/1809-8428.2019v16i2p257-267

SIBONI, S., SACHIDANANDA, V., MEIDAN, Y., BOHADANA, M., MATHOV, Y., BHAIRAV, S., SHABTAI, A., & ELOVICI, Y. (2019). "Security Testbed for Internet-of-Things Devices". IEEE Transactions on Reliability, 68, 23–44. https://doi.org/10.1109/TR.2018.2864536

SMXPLUS. (2024). “Hacker Cibercriminoso com Laptop Roubando Dados Pessoais do Usuário, Ataque de hacker e Segurança na Web, Conceito de Phishing na Internet, Hacker em Capuz Preto com Laptop Tentando Ciberataque Código de Programação”. Freep!k - Vetor Premium. Acessado em: 12-06-2024. Disponível em: https://br.freepik.com.

SONG, L., & GARCÍA-VALLS, M. (2022). "Improving Security of Web Servers in Critical IoT Systems through Self-Monitoring of Vulnerabilities". Sensors, 22, 5004. https://doi.org/10.3390/s22135004

SONI, T., KAUR, R., GUPTA, D., SHARMA, A., & GUPTA, G. (2023). "The

Cybersecurity Ecosystem: Challenges, Risk and Emerging Technologies". 7th International Conference on Trends in Electronics and Informatics (ICOEI), pp. 699-703.

SOOKHAK, M., TANG, H., HE, Y., & YU, F. (2019). "Security and Privacy of Smart Cities: A Survey, Research Issues and Challenges". IEEE Communications Surveys and Tutorials, 21, 1718–1743. https://doi.org/10.1109/COMST.2018.2867288

TAKADA, T. (2017). "Authentication Shutter: Alternative Countermeasure against Password Reuse Attack by Availability Control". Proceedings of the 12th International Conference on Availability, Reliability and Security.

TOMUR, E., GÜLEN, U., SOYKAN, E., ERSOY, M. A., KARAKOÇ, F., KARAÇAY, L., & ÇOMAK, P. (2021). "SoK: Investigation of Security and Functional Safety in Industrial IoT". IEEE International Conference on Cyber Security and Resilience (CSR), Rhodes, Greece, pp. 226-233. https://doi.org/10.1109/CSR51186.2021.9527921

TORRE, D., MESADIEU, F., & CHENNAMANENI, A. (2023). "Deep Learning Techniques to Detect Cybersecurity Attacks: A Systematic Mapping Study". Empirical Software Engineering, 28, 76. https://doi.org/10.1007/s10664-023-10302-1

VILLAMIL, S., HERNÁNDEZ, C., & TARAZONA, G. (2020). "An Overview of Internet of Things". TELKOMNIKA Telecommunication, Computing, Electronics and Control, 18(5), 2320–2327.

WANG, W., XU, P., & YANG, L. (2018). "Secure Data Collection, Storage and Access in Cloud-Assisted IoT". IEEE Cloud Computing, 5(4), 77-88. https://doi.org/10.1109/MCC.2018.111122026

WATSON, V., TELLABI, A., SASSMANNSHAUSEN, J., & LOU, X. (2017). "Interoperability and Security Challenges of Industry 4.0". GI-Jahrestagung.

WOHLIN, C., RUNESON, P., HÖST, M., OHLSSON, M. C., REGNELL, B., & WESSLÉN, A. (2012). “Experimentation in Software Engineering”. Springer. https://doi.org/10.1007/978-3-642-29044-2

XU, H., SGANDURRA, D., MAYES, K., LI, P., & WANG, R. (2017). "Analysing the Resilience of the Internet of Things Against Physical and Proximity Attacks". Security, Privacy, and Anonymity in Computation, Communication, and Storage. Springer International Publishing, pp. 291–301. https://doi.org/10.1007/978-3-319-72395-2_27

XU, L. D.; HE, W.; LI, S. (2014). Internet of Things in Industries: A Survey. IEEE Transactions on Industrial Informatics, v. 10, n. 4, p. 2233-2243, doi: 10.1109/TII.2014.2300753

YADAV, E., MITTAL, E., & YADAV, H. (2018). "IoT: Challenges and Issues in Indian Perspective". 3rd IEEE IoT-SIU, pp. 1–5. https://doi.org/10.1109/IoT-SIU.2018.8519869

ZANON, V., ROMANCINI, E., MANOEL, B., LAU, J., OURIQUE, F., & MORALES, A. (2022). "Avaliação Experimental de uma Camada de Segurança Implementada em Dispositivo Vestível Cardíaco para Internet das Coisas Médicas". XXII SBSEG, SBC, Brasil, pp. 97–110. https://doi.org/10.5753/sbseg.2022.224659

ZHAO, W., YANG, S., & LUO, X. (2020). "On Threat Analysis of IoT-Based Systems: A Survey". IEEE SmartIoT, Beijing, China, pp. 205–212. https://doi.org/10.1109/SmartIoT49966.2020.00038

Apêndice A – Processo de Extração da Revisão Estruturada

Processo de Extração

Para cada fonte candidata, o procedimento de extração é realizado utilizando o modelo apresentado abaixo.

Modelo de Extração

A) Dados da publicação	
Título:	indica o título do trabalho
Autor(es):	nome dos autores
Fonte de Publicação:	local de publicação
Ano da Publicação:	ano de publicação
Resumo:	texto contendo uma descrição do resumo
B) Dados derivados do objetivo	
Vulnerabilidades	Quais as vulnerabilidades em sistemas de software IoT são destacadas no estudo?

Relatório da Execução

- Data de Execução Scopus: 08/2022 (atualizada em 20/01/25)

Foram identificados 638 resultados de documentos inicialmente. Após a eliminação de *proceedings* e livros, restaram 491. Com a atualização da busca pela *string*, foram incluídos mais 321 estudos, resultando em um total de 812 artigos identificados

- Incluídos para extração de dados:

Após a análise do título, resumo e palavras-chave, o número de documentos selecionados foi reduzido para 85. Em seguida, aplicamos o filtro de leitura de texto completo, reduzindo-o para **44 documentos finais**, utilizados para a extração e análise das informações relevantes para o estudo.

- Incluídos pelo *Snowballing*
    - *Backward snowballing:* Foram identificados e incluídos um total de 90 artigos;
    - *Forward snowballing*: Foram identificados e incluídos um total de 45 artigos

O conjunto final de artigos selecionados na revisão (motor de busca da Scopus):

[A1]. Saha. T. et al. (2022), "SHARKS: Smart Hacking Approaches for RisK Scanning in Internet-of-Things and Cyber-Physical Systems Based on Machine

Learning," in IEEE Transactions on Emerging Topics in Computing, vol. 10, no. 2, pp. 870-885, doi: 10.1109/TETC.2021.3050733.

[A2]. AbuEmera, E. A., ElZouka H. A. and Saad A. A. (2022), "Security Framework for Identifying threats in Smart Manufacturing Systems Using STRIDE Approach," 2nd International Conference on Consumer Electronics and Computer Engineering (ICCECE), Guangzhou, China, pp. 605-612, doi: 10.1109/ICCECE54139.2022.9712770.

[A3]. Auliar, R. B. and Bekaroo G. (2021). "Security in IoT-based Smart Homes: A Taxonomy Study of Detection Methods of Mirai Malware and Countermeasures," 2021 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME), Mauritius, Mauritius, pp. 1-6, doi: 10.1109/ICECCME52200.2021.9590841.

[A4]. Tomur, E. et al. (2021) "SoK: Investigation of Security and Functional Safety in Industrial IoT," 2021 IEEE International Conference on Cyber Security and Resilience (CSR), Rhodes, Greece, pp. 226-233, doi: 10.1109/CSR51186.2021.9527921.

[A5]. Karie N. M. et al. (2021). "A Review of Security Standards and Frameworks for IoT-Based Smart Environments," in IEEE Access, vol. 9, pp. 121975-121995, doi: 10.1109/ACCESS.2021.3109886.

[A6]. Davis B. D., Mason J. C. and Anwar M. (2020). "Vulnerability Studies and Security Postures of IoT Devices: A Smart Home Case Study," in IEEE Internet of Things Journal, vol. 7, no. 10, pp. 10102-10110, doi: 10.1109/JIOT.2020.2983983.

[A7]. Akhunzada A., Islam S. U. and Zeadally S. (2020), "Securing Cyberspace of Future Smart Cities with 5G Technologies," in IEEE Network, vol. 34, no. 4, pp. 336-342, doi: 10.1109/MNET.001.1900559.

[A8]. Sengupta, J., Ruj, S. and Das Bit, S. (2020). A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT. Journal of Network and Computer Applications, 149, art. no. 102481. doi: 10.1016/j.jnca.2019.102481.

[A9]. Roohi A., Adeel M. and Shah M. A. (2019), "DDoS in IoT: A Roadmap Towards Security & Countermeasures," 2019 25th International Conference on Automation and Computing (ICAC), Lancaster, UK, pp. 1-6, doi: 10.23919/IConAC.2019.8895034.

[A10]. Akbar M. A. et al. (2021) "A Multicriteria Decision Making Taxonomy of IOT Security Challenging Factors," in IEEE Access, vol. 9, pp. 128841-128861, doi: 10.1109/ACCESS.2021.3104527.

[A11]. Mahapatra, S.N., Singh, B.K. and Kumar, V. (2020). A Survey on Secure Transmission in Internet of Things: Taxonomy, Recent Techniques, Research

Requirements, and Challenges. Arab J Sci Eng 45, 6211–6240. https://doi.org/10.1007/s13369-020-04461-2.

[A12]. Wustrich L., Pahl M. and Liebald S. (2020)."Towards an Extensible IoT Security Taxonomy," 2020 IEEE Symposium on Computers and Communications (ISCC), Rennes, France, pp. 1-6, doi: 10.1109/ISCC50000.2020.9219584.

[A13]. Mrabet, H. et al. (2020). A Survey of IoT Security Based on a Layered Architecture of Sensing and Data Analysis. Sensors, 20(13), 3625. https://doi.org/10.3390/s20133625.

[A14]. Yang P., Xiong N. and Ren J. (2020). "Data Security and Privacy Protection for Cloud Storage: A Survey," in IEEE Access, vol. 8, pp. 131723-131740, doi: 10.1109/ACCESS.2020.3009876.

[A15]. Yin, X.C. et al. (2019). Toward an Applied Cyber Security Solution in IoT-Based Smart Grids: An Intrusion Detection System Approach. Sensors, 19(22), 4952. https://doi.org/10.3390/s19224952.

[A16]. Wazid, M et al. (2019). Authentication in cloud-driven IoT-based big data environment: Survey and outlook. Journal of Systems Architecture, 97, pp. 185-196. doi: 10.1016/j.sysarc.2018.12.005.

[A17]. Sicato, J. C. S. et al. (2019). VPNFilter Malware Analysis on Cyber Threat in Smart Home Network. Appl. Sci. 9, 2763. https://doi.org/10.3390/app9132763.

[A18]. Panchal A. C., Khadse V. M. and Mahalle P. N. (2018). "Security Issues in IIoT: A Comprehensive Survey of Attacks on IIoT and Its Countermeasures". IEEE Global Conference on Wireless Computing and Networking (GCWCN), Lonavala, India, pp. 124-130, doi: 10.1109/GCWCN.2018.8668630.

[A19]. Heartfield, R., Loukas, G., Budimir, S., Bezemskij, A., Fontaine, J.R.J., Filippoupolitis, A., Roesch, E. (2018). A taxonomy of cyber-physical threats and impact in the smart home (Open Access). *Computers and Security*, 78, pp. 398-428. doi: 10.1016/j.cose.2018.07.011.

[A20]. Hayashi, Y., Verbauwhede I. and Radasky, W. A. (2018). "Introduction to EM information security for IoT devices". IEEE International Symposium on Electromagnetic Compatibility and IEEE Asia-Pacific Symposium on Electromagnetic Compatibility (EMC/APEMC), Suntec City, Singapore, pp. 735-738, doi: 10.1109/ISEMC.2018.8393878.

[A21]. Alqassem, I. and Svetinovic, D. (2014). "A taxonomy of security and privacy requirements for the Internet of Things (IoT)". IEEE International Conference on Industrial Engineering and Engineering Management, Selangor, Malaysia, pp. 1244-1248, doi: 10.1109/IEEM.2014.7058837.

[A22]. Reda, H.T., Anwar, A., Mahmood, A. (2022). Comprehensive survey and taxonomies of false data injection attacks in smart grids: attack models, targets, and impacts (Open Access). Renewable and Sustainable Energy Reviews, 163, art. no. 112423. doi: 10.1016/j.rser.2022.112423.

[A23]. Shah, Y. and Sengupta, S. (2020). "A survey on Classification of Cyber-attacks on IoT and IIoT devices," 2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York, NY, USA, pp. 0406-0413, doi: 10.1109/UEMCON51285.2020.9298138.

[A24]. Zhao, W., Yang, S. and Luo X. (2020). "On Threat Analysis of IoT-Based Systems: A Survey," 2020 IEEE International Conference on Smart Internet of Things (SmartIoT), Beijing, China, pp. 205-212, doi: 10.1109/SmartIoT49966.2020.00038.

[A25]. Kamaldeep, Dutta, M. and Granjal, J. (2020). "Towards a Secure Internet of Things: A Comprehensive Study of Second Line Defense Mechanisms," in IEEE Access, vol. 8, pp. 127272-127312, doi: 10.1109/ACCESS.2020.3005643.

[A26]. Sookhak, M., Tang H. and Yu F. R. (2018). "Security and Privacy of Smart Cities: Issues and Challenge," 2018 IEEE 20th International Conference on High Performance Computing and Communications; IEEE 16th International Conference on Smart City; IEEE 4th International Conference on Data Science and Systems (HPCC/SmartCity/DSS), Exeter, UK, pp. 1350-1357, doi: 10.1109/HPCC/SmartCity/DSS.2018.00224.

[A27]. Prakash S. and Jaiswal S. (2018). "Security Challenges in IoT enabled Smart Grid: Taxonomy of Novel Techniques and Algorithm," 3rd International Conference on Inventive Computation Technologies (ICICT), Coimbatore, India, pp. 577-582, doi: 10.1109/ICICT43934.2018.9034345.

[A28]. Sfar, A. R., Chtourou Z. and Challal Y. (2017). "A systemic and cognitive vision for IoT security: A case study of military live simulation and security challenges". International Conference on Smart, Monitored and Controlled Cities (SM2C), Sfax, Tunisia, pp. 101-105, doi: 10.1109/SM2C.2017.8071828.

[A29]. Thing V. L. L. and Wu J. (2016). "Autonomous Vehicle Security: A Taxonomy of Attacks and Defences". IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Chengdu, China, pp. 164-170, doi: 10.1109/iThings-GreenCom-CPSCom-SmartData.2016.52.

[A30]. Sookhak, M., Tang, H., He, Y. and Yu, F. R. (2019). "Security and Privacy of Smart Cities: A Survey, Research Issues and Challenges," in IEEE Communications

Surveys & Tutorials, vol. 21, no. 2, pp. 1718-1743, Secondquarter, doi: 10.1109/COMST.2018.2867288.

[A31]. Patnaik, R., Srujan Raju, K., Sivakrishna, K. (2021). Internet of Things-Based Security Model and Solutions for Educational Systems. In: Kumar, R., Sharma, R., Pattnaik, P.K. (eds) Multimedia Technologies in the Internet of Things Environment. Studies in Big Data, vol 79. Springer, Singapore. https://doi.org/10.1007/978-981-15-7965-3_11.

[A32]. Han, T., Jan, S. R. U., Tan, Z., Usman, M., Jan, M. A., Khan, R., & Xu, Y. (2020). A comprehensive survey of security threats and their mitigation techniques for next-generation SDN controllers. Concurrency and Computation: Practice and Experience, 32(16), e5300.

[A33]. Sahmi, I., Mazri, T. and Hmina, N. (2019). Study of the Different Security Threats on the Internet of Things and their Applications. In Proceedings of the 2nd International Conference on Networking, Information Systems & Security (NISS19). Association for Computing Machinery, New York, NY, USA, Article 68, 1–6. https://doi.org/10.1145/3320326.3320402.

[A34]. Benzarti, S., Triki, B. and Korbaa, O. (2017). "A survey on attacks in Internet of Things based networks," 2017 International Conference on Engineering & MIS (ICEMIS), Monastir, Tunisia, pp. 1-7, doi: 10.1109/ICEMIS.2017.8273006.

[A35]. Xu, H., Sgandurra, D., Mayes, K., Li, P., Wang, R. (2017). Analysing the Resilience of the Internet of Things Against Physical and Proximity Attacks. In: Wang, G., Atiquzzaman, M., Yan, Z., Choo, KK. (eds) Security, Privacy, and Anonymity in Computation, Communication, and Storage. SpaCCS 2017. Lecture Notes in Computer Science, vol 10658. Springer, Cham. https://doi.org/10.1007/978-3-319-72395-2_27.

[A36]. Gupta, A., and Gupta, S. K. (2022). Flying through the secure fog: A complete study on UAV-Fog in heterogeneous networks. International Journal of Communication Systems, 35(13), e5237.

[A37]. Ali, R.F., Muneer, A., Dominic, P.D.D., Taib, S.M., Ghaleb, E.A.A. (2021). Internet of Things (IoT) Security Challenges and Solutions: A Systematic Literature Review. In: Abdullah, N., Manickam, S., Anbar, M. (eds) Advances in Cyber Security. ACeS 2021. Communications in Computer and Information Science, vol 1487. Springer, Singapore. https://doi.org/10.1007/978-981-16-8059-5_9.

[A38]. Rahimi, H., Zibaeenejad, A., Rajabzadeh, P. and Safavi A. A. (2018). On the Security of the 5G-IoT Architecture. In Proceedings of the international conference on smart cities and internet of things (SCIOT '18). Association for Computing Machinery, New York, NY, USA, Article 10, 1–8. https://doi.org/10.1145/3269961.3269968.

[A39]. Elham Kariri. (2022). IoT Powered Agricultural Cyber-Physical System: Security Issue Assessment, IETE Journal of Research, DOI: 10.1080/03772063.2022.2032848.

[A40]. Zhukabayeva, T., Zholshiyeva, L. and Karabayev, N. (2024). Future Directions of Cybersecurity in Industrial Internet of Things Through Edge Computing. 9th International Conference on Computer Science and Engineering (UBMK), Antalya, Turkiye, pp. 1-6, doi: 10.1109/UBMK63289.2024.10773586.

[A41]. Alguliyev, R., Aliguliyev, R. and Sukhostat, L. (2024). Radon Transform Based Malware Classification in Cyber-Physical System Using Deep Learning. Results in Control and Optimization, volume 14, 100382, ISSN 2666-7207, https://doi.org/10.1016/j.rico.2024.100382.

[A42]. Bharathi V., Vinoth Kumar C. (2024). Vulnerability Detection in Cyber-Physical System Using Machine Learning. Scalable Computing: Practice and Experience, ISSN 1895-1767, Volume 25, Issues 1, pp. 577–591, DOI 10.12694/scpe.v25i1.2405.

[A43]. Peggs, C., Jackson, T., Tittlebaugh, A., Olp, T., Tyler, J., Reising, D., Loveless, T. (2023). Preamble-based RF-DNA Fingerprinting Under Varying Temperatures. 12th Mediterranean Conference on Embedded Computing (MECO), Budva, Montenegro, pp. 1-8, doi: 10.1109/MECO58584.2023.10155035.

[A44]. Ajao, L. and Apeh, S. (2023). Blockchain Integration with Machine Learning for Securing Fog Computing Vulnerability in Smart City Sustainability. 1st International Conference on Advanced Innovations in Smart Cities (ICAISC), Jeddah, Saudi Arabia, pp. 1-6, doi: 10.1109/ICAISC56366.2023.10085192.

Relatório da Revisão

Nesta seção serão apresentados a listagem das vulnerabilidades identificadas na revisão executada. Foram identificadas 69 vulnerabilidades, em uma listagem não envolvendo os resultados do *snowballing*, destacadas na tabela abaixo. As vulnerabilidades foram organizadas inicialmente em quatro categorias: *Device*, *Application, Network* e *Peopleware*.

Artigos	Vulnerabilidades	Categoria
13, 5, 23, 4, 17	Quebra de Autenticação	Aplicação
9, 31, 38, 1, 25, 17, 6	Estouro de Buffer	Aplicação
8	Inconsistência de Dados	Aplicação
8, 13, 11, 21, 9, 37, 27, 18, 4, 24	Gerenciamento de Acesso Inseguro	Aplicação

11, 31	Configuração de Interface Insegura	Aplicação
11, 5, 37, 33, 26	Gestão Insegura de Dados	Aplicação
5, 23, 31, 33, 15, 24	Software Inseguro	Aplicação
5	Falta de Monitoramento Ativo de Dispositivo	Aplicação
9	Código de Baixa Qualidade	Aplicação
19, 21, 2, 24	Não Repúdio	Aplicação
32, 18, 33, 17, 6, 24	Injeções de SQL	Aplicação
11, 27, 43	Fraca/Falta de Criptografia na Aplicação	Aplicação
38, 26, 24	Código Malicioso no Aplicativo	Aplicação
24, 40, 43	Sistemas de Baixo Custo	Dispositivo
8, 19	Canal de Voz	Dispositivo
19, 10, 23, 35, 24	Configuração Padrão	Dispositivo
8, 5, 21, 39, 18, 25	Falsificação de Dispositivo	Dispositivo
19, 10, 30, 20, 24	Vazamento de Emanações Eletromagnéticas	Dispositivo
16, 22, 30, 24, 26	Restrições de Energia	Dispositivo
8, 11, 19, 10	Interação Heterogênea	Dispositivo
11, 19, 10, 5, 16, 9, 37, 39, 38, 30, 25, 26, 36, 42	Transferência e Armazenamento Inseguro de Dados	Dispositivo
10, 5, 23, 35, 31, 1, 4, 24, 41	Firmware Inseguro	Dispositivo
31, 30, 24	Inicialização Insegura	Dispositivo
5, 37, 3, 36	Senha Insegura	Dispositivo
5, 24	Testes Insuficientes	Dispositivo
8, 23, 16, 29, 30, 4, 12, 6, 20, 24	Falta de Proteção de Canal Lateral	Dispositivo
10, 5, 23, 28, 21, 35, 29, 9, 37, 30, 4, 33, 25, 41	Falta de Autenticação Forte	Dispositivo
11, 10, 28, 16, 9, 37, 30, 33, 25, 12, 6, 24, 43	Baixo Poder Computacional	Dispositivo
35, 9	Baixo Alcance de Transmissão de Dados	Dispositivo
8, 34, 35, 29, 33, 24	Injeção de Código Malicioso	Dispositivo
35, 39, 7, 12, 20, 24	Obtenção de Acesso ao Console	Dispositivo
16, 39, 33, 12, 17, 24, 42	Dano Físico	Dispositivo
8, 19, 5, 34, 23, 39, 7, 33, 25,	Violação Física	Dispositivo

17, 20, 24, 36, 42		
8, 31, 37, 33, 12, 17, 6, 24	Privação do Sono	Dispositivo
35, 38	Clonagem de Etiquetas	Dispositivo
11, 23, 35, 16, 39, 38, 7, 4, 33, 12, 6, 24	Acesso Físico Não Protegido	Dispositivo
5, 23, 28, 21, 35, 29, 37, 38, 30, 27, 18, 4, 25, 42	Controle de Acesso Fraco	Dispositivo
10, 5, 29, 31, 38, 30, 27, 25, 36, 43	Fraco/Falta de Criptografia nos Dispositivos	Dispositivo
31	Interface Física Insegura	Dispositivo
8, 19, 34, 35, 29, 31, 38, 7, 33, 6, 36	Interferência de Canal	Rede
32	Sobrecarga de Comunicação	Rede
8, 13, 34, 23, 22, ´14, 37, 7, 30, 1, 25, 26, 36, 40, 42, 44	Vazamento ou Violação de Dados	Rede
11, 19, 5, 23, 22, 39, 38, 33, 17, 24	Escuta Clandestina	Rede
8, 11, 10, 34, 38, 7, 4, 33, 12, 17, 6, 24	Nó Falso/Malicioso	Rede
11, 19, 10, 35, 30, 25, 26, 40	Comunicação Heterogênea	Rede
14, 30, 18	Servidor Inseguro	Rede
11	Mecanismos de Atualização Inseguros	Rede
8, 11,5, 28, 21, 16, 37, 38, 30, 27, 18, 25, 6, 2, 36	Falta de Mecanismos de Autenticação Adequados	Rede
23, 18, 4	Falta de Senha Forte	Rede
19, 5, 22, 31, 25, 24	Falta de Protocolos de Comunicação Seguros	Rede
10	Configurar a Rede Repetidamente	Rede
32, 8, 11	Falsificação de Sinal	Rede
32, 8, 11, 19, 28, 21, 29, 14, 37, 39, 38, 7, 30, 27, 33, 25, 2, 24, 40	Acesso Não Autorizado	Rede
5, 23, 18	Rede Insegura	Rede
23, 7, 3, 18, 15, 41	Portas Não Utilizadas Habilitadas	Rede
19, 5, 29, 14, 31, 37, 39, 30,	Fraca/Falta de Criptografia na Comunicação	Rede

27, 18, 1, 2, 26, 43		
22, 36	Propriedades Físicas do Sistema de Energia	Rede
19	Desautenticação de Wi-Fi	Rede
29, 44	Controle de Tráfego Inseguro	Rede
24, 32, 36, 40	Arquitetura Centralizada	Rede
8, 35, 17, 41	Acesso a Links Maliciosos	*Peopleware*
19	Identificação do Fornecedor do Produto	*Peopleware*
5, 15, 12	Conhecimento do Sistema	*Peopleware*
10	Falta de Suporte Técnico	*Peopleware*
19, 10, 28, 39, 17	Circunstâncias Pessoais e Sociais	*Peopleware*
34, 23, 39, 38, 18, 33, 12, 6, 24, 36, 41	*Phishing*	*Peopleware*
19, 5, 39, 7, 33, 6, 41	Engenharia Social	*Peopleware*
5	Aquisição de Dispositivo Não Confiável	*Peopleware*
5	Postura de Segurança do Fornecedor	*Peopleware*

Extração de Dados da Revisão Estruturada

A) Dados da publicação:	
Título:	SHARKS: Smart Hacking Approaches for RisK Scanning in Internet-of-Things and Cyber-Physical Systems Based on Machine Learning
Autor(es):	Saha, T. and Aaraj, N. and Ajjarapu, N. and Jha, N.K.
Fonte de Publicação:	IEEE Transactions on Emerging Topics in Computing
Ano da Publicação:	2022
Resumo:	Cyber-physical systems (CPS) and Internet-of-Things (IoT) devices are increasingly being deployed across multiple functionalities, ranging from healthcare devices and wearables to critical infrastructures, e.g., nuclear power plants, autonomous vehicles, smart cities, and smart homes. These devices are inherently not secure across their comprehensive software, hardware, and network stacks, thus presenting a large attack surface that can be exploited by hackers. In this article, we present an innovative technique for detecting unknown system vulnerabilities, managing these vulnerabilities, and improving incident response when such vulnerabilities are exploited. The novelty of this approach lies in extracting intelligence from known real-world CPS/IoT attacks, representing them in the form of regular expressions, and employing machine learning (ML) techniques on this ensemble of regular expressions to

	generate new attack vectors and security vulnerabilities. Our results show that 10 new attack vectors and 122 new vulnerability exploits can be successfully generated that have the potential to exploit a CPS or an IoT ecosystem. The ML methodology achieves an accuracy of 97.4 percent and enables us to predict these attacks efficiently with an 87.2 percent reduction in the search space. We demonstrate the application of our method to the hacking of the in-vehicle network of a connected car. To defend against the known attacks and possible novel exploits, we discuss a defense-in-depth mechanism for various classes of attacks and the classification of data targeted by such attacks. This defense mechanism optimizes the cost of security measures based on the sensitivity of the protected resource, thus incentivizing its adoption in real-world CPS/IoT by cybersecurity practitioners
B) Dados derivados do objetivo:	
Vulnerabilidades	“Due to the absence of sender and receiver addresses in the data frames, every ECU can freely publish and receive messages from the bus. While this enables easier addition of new ECUs to the network, it poses a grave security threat to the system.” “This allows a malicious node on the CAN bus to receive all the data frames through sniffing. The absence of encryption makes it easier to analyze the collected frames.” “Using the details of the data frames, the adversary can broadcast malicious frames on the bus by spoofing a particular node. Absence of authentication schemes compromises the integrity of messages on the CAN bus” “Denial of Service (DoS): The CAN protocol implements a priority-based broadcasting communication scheme. For example, messages from the anti-lock braking system, which are critical to the safety of the passengers, are given higher priority for transmission on the bus than messages from climate control sensors.“ “Since the CAN protocol is bereft of authentication schemes and time-stamp verification, the recorded frame packets can be sent on the CAN bus at inconvenient time instances to launch various attacks.” “The other vulnerabilities that we consider in our experiments are ECU buffer overflows" “and malware injection through ECU firmware updates”

A) Dados da publicação:	
Título:	Security Framework for Identifying threats in Smart Manufacturing Systems Using STRIDE Approach
Autor(es):	Abuemera, E.A. and Elzouka, H.A. and Saad, A.A.
Fonte de Publicação:	2nd International Conference on Consumer Electronics and Computer Engineering, ICCECE
Ano da Publicação:	2022
Resumo:	Cyber security is still the main argument in any system development lifecycle that needs more concern. There are still numerous challenges associated with conducting a threat modeling approach for smart manufacturing systems. One of these challenges is the lack of a threat database based on the expertise of highly skilled researchers in this field. Hence this study attempts to address this gap by developing a components catalog and a rule-based threat database to address potential security threats in smart manufacturing systems saving time and effort. Specifically, it performs STRIDE-based threat modeling against a smart factory use case using Microsoft Threat Modelling Tool. The threat evaluation process is conducted with this research to determine the severity of threats and give a preliminary estimation of the overall system's risk
B) Dados derivados do objetivo:	
Vulnerabilidades	“Due to a lack of authentication across communicating processes, spoofing the processes” “In the use case, there is no method for logging and recording events. As a result, the processes are vulnerable to repudiation threats and might deny previous events” “Information disclosure threats are due to the lack of encryption. Attackers can simply decode and understand unencrypted messages.” “Although most elevation of privilege threats is due to the lack of access control rules based on authorization, the elevation of privilege on EE-1 by tricking the operator into opening a crafted PowerPoint document is due to Windows OLE Remote Code Execution vulnerability”

A) Dados da publicação:	
Título:	Security in IoT-based smart homes: A taxonomy study of detection methods of mirai malware and countermeasures
Autor(es):	Auliar, R.B. and Bekaroo, G.

Fonte de Publicação:	International Conference on Electrical, Computer, Communications and Mechatronics Engineering, ICECCME
Ano da Publicação:	2021
Resumo:	During recent years, there has been widespread adoption of the Internet and swift digitization within various sectors, including smart homes. These also led to the rapid growth of the Internet of Things (IoT), which is expected to proliferate further, where 50 billion IoT devices are estimated to be connected to the Internet by 2030. However, the growth in connected IoT devices to the Internet has not been without challenges. IoT devices are known to have various vulnerabilities that could be exploited by attackers, thus hindering security of devices and users. Recently, the use of Mirai malware by attackers gained significant attention as it has the capability to transform IoT connected devices into remotely controlled bots, which can be utilized as part of a botnet in large-scale network attacks. Taking cognizance of the importance to secure against this type of malware, this study presents a taxonomy review on the techniques that can potentially be used to detect Mirai malware along with countermeasures for securing against such malware
B) Dados derivados do objetivo:	
Vulnerabilidades	"Strengthening Password Protection - Each device must consist of a unique password instead of common passwords for specific model since Mirai botnets target lists of hardcoded passwords" "Disabling Unused Ports - Unused ports such as SSH, and Telnet among others should be disabled by default for end users might not be aware of open ports and could hence be targeted by Mirai botnets." "Monitoring Open Ports - Open ports should be monitored to analyze traffic that could source from a malicious origin." "Restructuring Device Firmware - Device firmware are often exploited via the use of various methods and tools that analyze firmware for issues pertaining to authentication and to bypass backdoors" "Ensuring Proper Configuration - In addition, open connections must not be with default configuration for wireless communications."

A) Dados da publicação:	
Título:	SoK: Investigation of security and functional safety in industrial IoT
Autor(es):	Tomur, E. and Gulen, U. and Soykan, E.U. and Akif Ersoy, M. and Karakoc, F. and Karacay, L. and Comak, P.
Fonte de Publicação:	IEEE International Conference on Cyber Security and Resilience, CSR
Ano da Publicação:	2021
Resumo:	There has been an increasing popularity of industrial usage of Internet of Things (IoT) technologies in parallel to advancements in connectivity and automation. Security vulnerabilities in industrial systems, which are considered less likely to be exploited in conventional closed settings, have now started to be a major concern with Industrial IoT. One of the critical components of any industrial control system turning into a target for attackers is functional safety. This vital function is not originally designed to provide protection against malicious intentional parties but only accidents and errors. In this paper, we explore a generic IoT-based smart manufacturing use-case from a combined perspective of security and functional safety, which are indeed tightly correlated. Our main contribution is the presentation of a taxonomy of threats targeting directly the critical safety function in industrial IoT applications. Besides, based on this taxonomy, we identified particular attack scenarios that might have severe impact on physical assets like manufacturing equipment, even human life and cyber-assets like availability of Industrial IoT application. Finally, we recommend some solutions to mitigate such attacks based mainly on industry standards and advanced security features of mobile communication technologies.
B) Dados derivados do objetivo:	
Vulnerabilidades	“Unauthorized physical access of any malicious party to the devices belonging to the safety control system may present a threat to take control of a safety-related asset like Safety Program” “Manipulation of Software - Attacks are possible on assets which can be used to configure and parameterize the safety systems like Engineering Workstation. Malicious modifications of safety programs, safety parameters or any other software/hardware on safety controller, safety actuator and safety sensor can be done to adversely affect the operation of functional safety”

	"There can be attacks that aim malicious intervening with cyclic communication between Safety Controller (Safety Program), Safety Actuator and Safety Sensor. Attacker may aim to obstruct, destruct or modify" "Attacks can be performed on the Safety Controller over network via its remote programming or monitoring interfaces. Similar to the reported weaknesses in IoT devices, safety controllers are also prone to weak authentication and authorization practices." "If they are accessible remotely, any type of attacker may try to break authentication, for instance, by using unchanged default passwords or applying a brute force attack" "Vulnerabilities in built-in security features of safety devices (actuator, sensor or controller) can be exploited because of weak credential management, firmware update from untrusted source or lack of side channel protection". "Malware injected into Safety Program either directly or indirectly via Engineering Workstation can allow attackers to manipulate safety program code in such a way that it does not command switching into fail-safe mode when there is potentially dangerous situation or it commands to do so when there is no such situation." "(Denial of Service): Injection of a high volume of packets in the OT network or flooding of malicious traffic to overload system resources in Safety Program by attackers can cause disruption in timely operation of the overall safety function."

A) Dados da publicação:	
Título:	A Review of Security Standards and Frameworks for IoT-Based Smart Environments
Autor(es):	Karie, N.M. and Sahri, N.M. and Yang, W. and Valli, C. and Kebande, V.R.
Fonte de Publicação:	IEEE Access
Ano da Publicação:	2021
Resumo:	Assessing the security of IoT-based smart environments such as smart homes and smart cities is becoming fundamentally essential to implementing the correct control measures and effectively reducing security threats and risks brought about by deploying IoT-based smart technologies. The problem, however, is in finding security standards and assessment frameworks that best meets the security

	requirements as well as comprehensively assesses and exposes the security posture of IoT-based smart environments. To explore this gap, this paper presents a review of existing security standards and assessment frameworks which also includes several NIST special publications on security techniques highlighting their primary areas of focus to uncover those that can potentially address some of the security needs of IoT-based smart environments. Cumulatively a total of 80 ISO/IEC security standards, 32 ETSI standards and 37 different conventional security assessment frameworks which included 7 NIST special publications on security techniques were reviewed. To present an all-inclusive and up-to-date state-of-the-art research, the review process considered both published security standards and assessment frameworks as well as those under development. The findings show that most of the conventional security standards and assessment frameworks do not directly address the security needs of IoT-based smart environments but have the potential to be adapted into IoT-based smart environments. With this insight into the state-of-the-art research on security standards and assessment frameworks, this study helps advance the IoT field by opening new research directions as well as opportunities for developing new security standards and assessment frameworks that will address future IoT-based smart environments security concerns. This paper also discusses open problems and challenges related to IoT-based smart environments security issues. As a new contribution, a taxonomy of challenges for IoT-based smart environment security concerns drawn from the extensive literature examined during this study is proposed in this paper which also maps the identified challenges to potential proposed solutions.
B) Dados derivados do objetivo:	
Vulnerabilidades	"Data and Information Leakage: In any IoT smart environment, without proper security mechanisms that protect data and information from malware and other malicious intruders, personal information could easily be leaked resulting in security breaches." "With information moving in and around IoT-based smart environments and over to the Internet, malicious attackers can take advantage of unsecured network communications and steal data as it is being transmitted between the connected IoT devices which can lead to other serious security breaches."

	"Many cloud-based IoT devices and systems are known to have security vulnerabilities and can easily be victims of hacking and cyberattacks as data transmission like video data from cameras may not even be encrypted when sent over the internet." "Because of the lack of standardization in many IoT-based smart environments, rogue software can easily find its way into IoT devices through firmware upgrade and trusted boot, device acquisition as well as apps and services." "Because of the lack of specialized universal approved IoT security standards or security assessment frameworks, some devices may be manufactured with poor security baselines such as old and unpatched embedded operating systems and software, weak, guessable, or hard-coded passwords, insecure data transfer and storage, among others. This makes such IoT devices vulnerable to different security threats and attacks." "With the growing innovation of IoT technologies, many users are yet to understand how modern IoT devices are designed and function. This makes it easy for attackers to use social engineering to trick IoT device users into providing sensitive data or information which can be used to gain access into smart environment networks, such as smart homes and smart cities, putting everyone's life at risk." "Insufficient IoT Device Testing and Updates: Most of the IoT devices are produced quickly to meet the increasing market demands and hence do not undergo proper testing or follow any acceptable security standards or assessment frameworks" "Users mostly put their trust in the manufactures to test the IoT devices as well as provide security control measures. However, due to high demands, many manufacturers focus more on creating and releasing new products to the market without having proper testing or putting security control measures in place." "Lack of Active Device Monitoring: Monitoring IoT devices can be challenging. This is because most of the existing monitoring tools and practices especially those focusing on the cloud were traditionally designed to monitor time-series metric data with no focus on modern IoT devices or their processes."

	“The lack of efficient and robust security protocols including proper IoT security standards, assessment frameworks and safeguards could lead to security breaches in smart environments leading to personal data exfiltration.” “With many IoT devices in smart environments lacking strong authentication or access control mechanisms, it becomes easy for intruders to impersonate a legitimate user and use the credentials or any other information that gives them access to existing IoT resources in an IoT-based smart environment.” “Denial of Service (DoS/DDoS): With the advancement in technology, hackers can try to cause a DoS/DDoS to existing hubs in IoT-based smart environment networks or the sensors themselves.” “With the rapid growth in the number and usage of IoT devices, other security threats may also exist in IoT-based smart environments such as home invasions, trespass, falsification rogue and counterfeit IoT devices, botnet attacks, physical attacks, unintentional damage or loss, disasters and outages, failures or malfunctions, dynamic systems, authentication, unsecured wireless network problems, side-channel attack, man-in-the-middle, identity theft, advanced persistent threat (APT), jamming, function creep, buffer overflow, large-scale unauthorized data mining, surveillance, unauthorized access or deletion or modification of data, worms, viruses and malicious code, the openness of the networked systems, weak passwords, fixed firmware, resource constraints, headless nature of IoT devices, tamper-resistant packages, heterogeneous protocols, dynamic characteristics, longevity expectations among many other security threats.”

A) Dados da publicação:	
Título:	Vulnerability Studies and Security Postures of IoT Devices: A Smart Home Case Study
Autor(es):	Davis, B.D. and Mason, J.C. and Anwar, M.
Fonte de Publicação:	IEEE Internet of Things Journal
Ano da Publicação:	2020
Resumo:	Internet-of-Things (IoT) technology has revolutionized our daily lives in many ways-whether it is the way we conduct our day-to-day activities inside our home, or the way we control our home environments remotely. Unbeknownst to the users, with the adoption of these 'smart home'

	technologies, their personal space becomes vulnerable to security and privacy attacks. We conducted studies of vulnerabilities and security posture of smart home IoT devices. We started with a literature review on known vulnerability studies of the IoT devices, considering four categories of attacks: 1) physical; 2) network; 3) software; and 4) encryption. We then conducted our own vulnerability experiments that compared security postures between well known and lesser known vendors through misuse and abuse case analysis, followed by a review of coverage in major vulnerability databases. Based on our analysis, the main finding was the need for a stronger focus on the security posture of lesser known vendor devices as they are often less regulated and faceless scrutiny.
B) Dados derivados do objetivo:	
Vulnerabilidades	1) Physical: "Some physical attacks are as follows: node tampering, radio-frequency (RF) interference on RF identifiers (RFIDs), node jamming in wireless sensor networks, malicious node injection, physical damage, social engineering, sleep deprivation, and malicious code injection." 2) Network: "The network attacks identified in [9] are traffic analysis, RFID spoofing/cloning/unauthorized access, sinkhole, man in the middle, Denial of Service (DoS), routing information, and sybil." 3) Software: "Some of the software attacks that have been presented in [9] are phishing, malicious scripts, Trojan horse, spyware, adware, and DoS that exploit buffer overflows, SQL injections, and other types of vulnerabilities." 4) Encryption: "Because IoT devices have limited computing power to support strong cryptographic protocols, they are vulnerable to the side channel, cryptanalysis, and man-in-the-middle attacks." "The main vulnerability that exists is the "motherboard hack" vulnerability. The motherboard hack is an attack where the bulb is cracked open gaining access to the motherboard within the smart light bulb. Some manufactures store unencrypted information, e.g., WiFi SSID and encryption key in plaintext, in this location."

A) Dados da publicação:	
Título:	Securing Cyberspace of Future Smart Cities with 5G Technologies
Autor(es):	Akhunzada, A. and Islam, S.U. and Zeadally, S.
Fonte de Publicação:	IEEE Network
Ano da Publicação:	2020
Resumo:	Future smart cities promise to dramatically improve the quality of life and have been attracting the attention of many researchers in recent years. The integration of IoT with their corresponding service delivery models to manage a city's asset securely remains a significant challenge. The deployment of diverse IoT technologies and several architectural components and novel entities of emerging ICT solutions opens up new security threats and vulnerabilities. Large-scale, seamless communication among multiple IoT technologies is highly dependent on the operations of the underlying wireless access technologies such as WSNs, SDR, CR and RFID. We present thematic layered taxonomies to highlight the potential security vulnerabilities, attacks, and challenges of key IoT enabling technologies which underpin the development of smart cities. We also identify potential requirements and key enablers that play a vital role in the development of secure smart cities. Finally, we discuss various open issues that need to be addressed to unlock the full potential of 5G for future smart cities.
B) Dados derivados do objetivo:	
	"To start with, the wide deployment of SDR requires an adequate level of physical safety and security. SDR (Software Defined Radio) has reconfiguration capabilities which enable it to download various new radio applications and diverse communication links. Consequently, SDR is vulnerable to malicious modifications and injections due to its open communication without any integrity checks on the transmitted data."
Vulnerabilidades	"Device cloning is a frequently used term in traditional wireless communications. It represents unauthorized access to diverse services offered by another SDR device. Device cloning is a major security threat to the emerging 5G communication networks." "Moreover, SDR devices and components are easily programmable and accessible in an open environment and are vulnerable to sophisticated MATE attacks."

	“The physical layer is vulnerable to sophisticated attacks such as unauthorized access, which subsequently leads to alteration of cognitive messages, and jamming attacks that severely affect spectrum sensing and sharing abilities. Moreover, the physical layer is also vulnerable to disruption of the cognitive engine as well as masquerading both as a primary user and a cognitive node.” “Moreover, the physical layer is also vulnerable to manipulation of various control messages and system commands. The physical layer is also vulnerable to channel interference.” “The strategic layer of RFID is vulnerable to location privacy attacks and social engineering attacks.” “The network layer can also experience spoofing attacks, selective forwarding attacks, and is vulnerable to a variety of DoS attacks.” “For instance, to ensure the availability of the SDR, the underlying operating system must be designed with features that do not allow backdoor accounts and patches with vulnerable open ports and services.”

A) Dados da publicação:	
Título:	A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT
Autor(es):	Sengupta, J. and Ruj, S. and Das Bit, S.
Fonte de Publicação:	Journal of Network and Computer Applications
Ano da Publicação:	2020
Resumo:	In recent years, the growing popularity of Internet of Things (IoT) is providing a promising opportunity not only for the development of various home automation systems but also for different industrial applications. By leveraging these benefits, automation is brought about in the industries giving rise to the Industrial Internet of Things (IIoT). IoT is prone to several cyberattacks and needs challenging approaches to achieve the desired security. Moreover, with the emergence of IIoT, the security vulnerabilities posed by it are even more devastating. Therefore, in order to provide a guideline to researchers, this survey primarily attempts to classify the attacks based on the objects of vulnerability. Subsequently, each of the individual attacks is mapped to one or more layers of the generalized IoT/IIoT architecture followed by a discussion on the countermeasures proposed in literature.

	Some relevant real-life attacks for each of these categories are also discussed. We further discuss the countermeasures proposed for the most relevant security threats in IIoT. A case study on two of the most important industrial IoT applications is also highlighted. Next, we explore the challenges brought by the centralized IoT/IIoT architecture and how blockchain can effectively be used towards addressing such challenges. In this context, we also discuss in detail one IoT specific Blockchain design known as Tangle, its merits and demerits. We further highlight the most relevant Blockchain-based solutions provided in recent times to counter the challenges posed by the traditional cloud-centered applications. The blockchain-related solutions provided in the context of two of the most relevant applications for each of IoT and IIoT is also discussed. Subsequently, we design a taxonomy of the security research areas in IoT/IIoT along with their corresponding solutions. Finally, several open research directions relevant to the focus of this survey are identified.
B) Dados derivados do objetivo:	
Vulnerabilidades	"Refers to the act of physically modifying a device (e.g. RFID) or communication link." "Here the attacker injects malicious code onto a physical device by compromising it which may help him/her launch other attacks too." "RF Interference/Jamming: Attacker creates and sends noise signals over the Radio Frequency (RF)/WSN signals to launch DoS attacks on the RFID tags/sensor nodes thereby hindering communication." "Fake Node Injection: Attacker drops a fake node between two legitimate nodes of the network to control data flow between them." "Sleep Denial Attack: Attacker keeps the battery powered devices awake by feeding them with wrong inputs. This causes exhaustion in their batteries leading to shutdown." "Side Channel Attack: In this attack, the attacker collects the encryption keys by applying timing, power, fault attack etc." "Permanent Denial of Service (PDoS): Also known as phlashing, is a type of DoS attack, wherein an IoT device is completely damaged via hardware sabotage. The attack is launched by destroying firmware or uploading a corrupted BIOS using a malware."

	“For example, using device spoofing attack, attackers can obtain a camera's password of any length and combination. Also by enumerating all possible MAC addresses the attacker can launch device scanning attack to find all online cameras.” “Their experiments reveal that the home automation system is vulnerable to brute force attacks revealing the passwords. It also reveals that the smart meters can be hijacked to launch ransomware attacks against other systems.” “security vulnerabilities of Virtual Personal Assistant (VPA) based IoT devices such as Amazon Echo and Google Home. These systems are vulnerable to attacks like voice squatting and voice masquerading.” “RFID Spoofing: The attacker first spoofs an RFID signal to get access of the information imprinted on the RFID tag.” “RFID Unauthorized Access: An attacker is able to read, modify or delete data present on RFID nodes because of the lack of proper authentication mechanisms. “In a wormhole attack, an attacker maliciously prepares a low-latency link and then tunnels packets from one point to another through this link.” “Here, a single malicious node claims multiple identities (known as sybil nodes) and locates itself at different places in the network.” “An attacker may capture a signed packet and resend the packet multiple number of times to the destination. This keeps the network busy leading to a DoS attack. “in DDoS multiple compromised nodes attack a specific target by flooding messages, or connection requests to slow down or even crash the system server/network resource.” “Data Inconsistency: In IoT, attack on data integrity leading to inconsistency of data in transit or data stored in a central database is referred to as Data Inconsistency.” “Access control implies giving access to authorized users and denying access to unauthorized users. With unauthorized access, malicious users can gain data ownership or access sensitive data.”

	“Data breach or memory leakage refers to the disclosure of personal, sensitive or confidential data in an unauthorized manner.”

A) Dados da publicação:	
Título:	DDoS in IoT: A roadmap towards security countermeasures
Autor(es):	Roohi, A. and Adeel, M. and Shah, M.A.
Fonte de Publicação:	25th IEEE International Conference on Automation and Computing
Ano da Publicação:	2019
Resumo:	In this era of digitization, more and more technologies are spurring up but are failing to make a successful impact due to the security and privacy issues. Internet of Things (IoT) has made its mark recently and being end-consumer oriented, makes it more prone towards being exploited. There are many types of security attacks in the IoT which can compromise the end user data and services. The most common and devastating security attack in the IoT is a Denial of Service (DoS)/Distributed Denial of Service (DDoS) attack. In this paper, the contributions are: we provide a structured comprehensive overview of the existing research on DDoS Attacks, its security countermeasures in the context of IoT. We survey latest vulnerabilities and their security solutions over the period 2014-2019. With elaborate discussion on IoT architecture and underlying security threats impacting each layer in the IoT, we have grouped existing approaches and derived taxonomy. With this concise overview, the paper seeks to provide an understanding of the pertaining models adopted by different researchers.
B) Dados derivados do objetivo:	
Vulnerabilidades	“Devices being used at Perception Layer experience resource constraints with respect to their application at the user end. Moreover, technologies such as RFID, NFC, Bluetooth, ZigBee e.t.c lack data transmission range which can be exploited by the intruder.” “Middleware layer is responsible for analyzing the data which has been collected via the sensor nodes. Computational and processing resources are required extensively on this layer. Securing data in this layer which is usually referred as cloud and authentication are concerns which are to be addressed” “Attacker usually targets unauthorized access towards the Application being used which is usually available via the Internet. This User Interface extends attackers access to

	sensitive data of the user which through different penetration techniques, vulnerabilities, bugs in the programs, low quality level code, inducing buffer overflow e.t.c.”

A) Dados da publicação:	
Título:	A Multicriteria Decision Making Taxonomy of IOT Security Challenging Factors
Autor(es):	Akbar, M.A. and Alsanad, A. and Mahmood, S. and Alothaim, A.
Fonte de Publicação:	IEEE Access
Ano da Publicação:	2021
Resumo:	Internet of things (IoT) is leading a new digital age. IoT is regarded as the significant frontier that can improve almost all aspect of our lives. Currently, the IoT technology faces several challenges to academic researchers and industry practitioners, mainly that related with security of data. The objective of this study is to develop a prioritization-based taxonomy of the challenging factors that could hinders the security of IoT. By conducting the literature review and questionnaire survey studies 21 challenging factors were identified that are reported in existing literature and in real-world practices. Moreover, the identified challenging factors are mapped in the core domain of IoT (i.e. smart city, smart home, smart wearable's and smart health care); and apply the fuzzy-AHP approach to rank the identified challenging factors with respect to their criticality for security of IoT technology. The application of fuzzy-AHP is novel in this research area as it is successfully applied in other domains of information technology to address the multi-criterion decision making problems. This study is contributing by providing a prioritization-based taxonomy of the IoT security challenging factors that could help the practitioners and research community to revise and develop the new strategies for the secure IoT.
B) Dados derivados do objetivo:	
Vulnerabilidades	“Smart cities comprised of several heterogenous IoT devices in order to achieve various objectives. However, malicious IoT node could be connected to IoT system in order to collect and exchange data from other devices.“ “Increasing number of IoT devices connected to smart city will generate huge amount of data. However, these devices do not have potential to store and process data, therefore data

	generated by these devices need to be sent to cloud in order to process and analyze." "Thus, IoT devices do not have enough capability to encrypt and decrypt data that pose the integrity and authenticity of data as critical challenge." "Generally, cryptographic algorithms are used to ensure data privacy from unauthorized access. Due to low power and computation of IoT devices there is a risk of malicious attacks and leakage of personal information, as advanced cryptographic techniques could not be employe" "The smart world anticipated that several smart home appliances will be interconnected to home network. However, these devices need to be configured to home network repetitively and may prone to different security attacks. This could be tedious task for householder in order to manage these devices manually so external expert need to be called to control several security threats." "However, IoT devices consisting of software and hardware are less in numbers and due to heterogeneous nature, firmware is not updated frequently that causes a variety of security threats." "Thus, firmware of IoT devices for smart homes need to be updated automatically in order to cope with novel security vulnerability, as there is lack of technical support." "Smart home network could be compromised by attacker and permit them to send RTS (Request to send)/CTS (clear to send) messages in bulk. Thus, smart devices should be capable enough to stop these devices from receiving messages in bulk and deplete their resources." "Interdependence Behavior of Devices - Various smart home devices connected each other in a network in order to achieve a particular objective. " "However, location could be altered by attackers if he/she could receive radio signal and analyze them, if the location

	information altered by attacker this could impede emergency services.” “Smart devices come without any built-in security mechanism and these devices store data locally without any encryption method.” “Furthermore, strong cryptographic algorithm could not be implemented because these devices are resource constrained.”

A) Dados da publicação:	
Título:	A Survey on Secure Transmission in Internet of Things: Taxonomy, Recent Techniques, Research Requirements, and Challenges
Autor(es):	Mahapatra, S.N. and Singh, B.K. and Kumar, V.
Fonte de Publicação:	Arabian Journal for Science and Engineering
Ano da Publicação:	2020
Resumo:	Internet of things (IoT) is one of the emerging paradigms in the current era that has attracted many researchers due to its widespread applications. Due to the open nature of the device accessibility and heterogeneity, a rapid increase in connected devices leads to several vulnerabilities and threats in the IoT devices. Hence, security is one of the important concern and main challenge to be addressed for the guaranteed data transmission in IoT environment. In this review work, we analyze the secure transmission of data in IoT and investigate the recent approaches in IoT security and their requirements and open issues. We present a taxonomy model for the secure transmission in IoT security which includes architecture/layers, communication topology, and classification techniques which are categorized under cluster, trust, routing, blockchain, and location-based approaches. First, we briefly discuss the architecture of the IoT ecosystem that consists of three layers namely perception, network, and application layer which support the basic task such as transmission, sensing, and processing. Next, we classify the communication mechanism into different scenarios involved in the various network for the transmission of data in the IoT environment. Then, we investigate the recent approaches for secure communication to overcome certain attacks in IoT and analyze their strength and limitations. Finally, we discuss the security requirements, threats, and vulnerabilities faced by the current IoT system, and numerous open research

	challenges that are needed to be addressed for the efficient transmission of data as future research directions.
B) Dados derivados do objetivo:	
Vulnerabilidades	"Currently, security factors such as privacy, secure storage and management, authorization, and communication as well as access control are the critical and challenging issues in the IoT environment." "Due to the limited processing capability, traditional security methods suffer from various setbacks and often do not detect the physical threats in the network." "So, proper authentication and encryption are required for preventing such attacks from the spiteful users." "In this technology, there are some of the possible vulnerabilities, unauthorized tag cloning, attacks on availability and authenticity, spoofing, counterfeiting, DoS attack, eavesdropping, and replay attacks." "However, there are several security threats and vulnerabilities faced by cloud users, such as identity management, and heterogeneity issues in IoT devices that makes the data transmission unreachable to an user identity authentic node, physical and infrastructure security, encryption, data access controls, system complexity, and misconfiguration of software." "There are several reasons in observing the cyber-attacks are: Many IoT devices can be operated by unattended humans, thus it is easy for an attacker to access and an adversary can steal sensitive data over wireless networks by eavesdropping." "Some of the security issues with IoT devices such as insecure mobile interface, insufficient authentication, and insecure network service, and poor physical security, lack of transport encryption, privacy concerns, and insecure web interface insufficient security configurability." "The IoT connected resources have more demand for updating and the frequency of the messages causes latency which results in network vulnerabilities."

	“Due to the hardware limitations on storage, processing, and energy, high overhead and data traffic is a critical criterion in the field of secure data transmission.”

A) Dados da publicação:	
Título:	Towards an Extensible IoT Security Taxonomy
Autor(es):	Wüstrich, L. and Pahl, M.-O. and Liebald, S.
Fonte de Publicação:	IEEE Symposium on Computers and Communications , Vol. 2020-July
Ano da Publicação:	2020
Resumo:	Security is essential in the Internet of Things (IoT). IoT threat classifications are often non-intuitive to use. Identifying relevant properties of an attack is difficult and requires reading details of the attack. We therefore propose a simple-to-use naming scheme for IoT threat classification. It is based on the affected layers and the affected security goals. We evaluate the usefulness of the chosen approach by applying it to common IoT threats.
B) Dados derivados do objetivo:	
Vulnerabilidades	“Access to devices and the capability to record and replay a signal are sufficient for this attack. As the attacker then impersonates a legitimate sender” “In order to save energy, some devices have a sleep mode. The attacker interacts with the device to prevent it from entering the low powered mode to drain its battery.” “This renders the device unavailable (CP.AVAIL). For a success, adversary needs network access to interact with the node. It also needs knowledge about the commands it can send to the node to keep it from the sleep mode.” “IoT devices embedded into the environment they can also be physically damaged” “Another class of attacks that predominantly affects devices on CP due to their limited computing power and level of exposure are side channel attacks” “By analyzing physical characteristics like power consumption of the device during computations the secret is inferred”

	“In a Sybil attack, the adversary assumes multiple identities of other nodes in the network” “In case an attacker is able modify the running application by using malware, a Trojan horse or is able to install a malicious update, the integrity on the application layer is violated”

A) Dados da publicação:	
Título:	A survey of IoT security based on a layered architecture of sensing and data analysis
Autor(es):	Mrabet, H. and Belguith, S. and Alhomoud, A. and Jemai, A.
Fonte de Publicação:	Sensors (Switzerland)
Ano da Publicação:	2020
Resumo:	The Internet of Things (IoT) is leading today’s digital transformation. Relying on a combination of technologies, protocols, and devices such as wireless sensors and newly developed wearable and implanted sensors, IoT is changing every aspect of daily life, especially recent applications in digital healthcare. IoT incorporates various kinds of hardware, communication protocols, and services. This IoT diversity can be viewed as a double-edged sword that provides comfort to users but can lead also to a large number of security threats and attacks. In this survey paper, a new compacted and optimized architecture for IoT is proposed based on five layers. Likewise, we propose a new classification of security threats and attacks based on new IoT architecture. The IoT architecture involves a physical perception layer, a network and protocol layer, a transport layer, an application layer, and a data and cloud services layer. First, the physical sensing layer incorporates the basic hardware used by IoT. Second, we highlight the various network and protocol technologies employed by IoT, and review the security threats and solutions. Transport protocols are exhibited and the security threats against them are discussed while providing common solutions. Then, the application layer involves application protocols and lightweight encryption algorithms for IoT. Finally, in the data and cloud services layer, the main important security features of IoT cloud platforms are addressed, involving confidentiality, integrity, authorization, authentication, and encryption protocols. The paper is concluded by presenting the open research issues and future directions towards securing IoT, including the lack of standardized lightweight encryption algorithms, the use of machine-learning algorithms to enhance security and the related challenges, the

	use of Blockchain to address security challenges in IoT, and the implications of IoT deployment in 5G and beyond.
B) Dados derivados do objetivo:	
Vulnerabilidades	"According to the 2017 OWASP application security flaws review, the ten most critical web application security risks are: injection, broken authentication, sensitive data exposure, XML external entities (XXE), broken access control, security misconfiguration, cross-site scripting (XSS), insecure deserialization, and using components with known vulnerabilities."

A) Dados da publicação:	
Título:	Data Security and Privacy Protection for Cloud Storage: A Survey
Autor(es):	Yang, P. and Xiong, N. and Ren, J.
Fonte de Publicação:	IEEE Access
Ano da Publicação:	2020
Resumo:	The new development trends including Internet of Things (IoT), smart city, enterprises digital transformation and world's digital economy are at the top of the tide. The continuous growth of data storage pressure drives the rapid development of the entire storage market on account of massive data generated. By providing data storage and management, cloud storage system becomes an indispensable part of the new era. Currently, the governments, enterprises and individual users are actively migrating their data to the cloud. Such a huge amount of data can create magnanimous wealth. However, this increases the possible risk, for instance, unauthorized access, data leakage, sensitive information disclosure and privacy disclosure. Although there are some studies on data security and privacy protection, there is still a lack of systematic surveys on the subject in cloud storage system. In this paper, we make a comprehensive review of the literatures on data security and privacy issues, data encryption technology, and applicable countermeasures in cloud storage system. Specifically, we first make an overview of cloud storage, including definition, classification, architecture and applications. Secondly, we give a detailed analysis on challenges and requirements of data security and privacy protection in cloud storage system. Thirdly, data encryption technologies and protection methods are summarized. Finally, we discuss several open research topics of data security for cloud storage.
B) Dados derivados do objetivo:	

Vulnerabilidades	“When data is outsourced to the cloud, its security is vulnerable. Encryption is an effective technique to protect data security. The essence of data encryption is to transform the original plaintext file or data into an string of unreadable code by some algorithms, which is usually called ciphertext.” “Besides, identity and attribute leakage issues are also threatening the privacy of data owners and authorized users.”

A) Dados da publicação:	
Título:	Toward an applied cyber security solution in iot-based smart grids: An intrusion detection system approach
Autor(es):	Yin, X.C. and Liu, Z.G. and Nkenyereye, L. and Ndibanje, B.
Fonte de Publicação:	Sensors (Switzerland)
Ano da Publicação:	2019
Resumo:	We present an innovative approach for a Cybersecurity Solution based on the Intrusion Detection System to detect malicious activity targeting the Distributed Network Protocol (DNP3) layers in the Supervisory Control and Data Acquisition (SCADA) systems. As Information and Communication Technology is connected to the grid, it is subjected to both physical and cyber-attacks because of the interaction between industrial control systems and the outside Internet environment using IoT technology. Often, cyber-attacks lead to multiple risks that affect infrastructure and business continuity; furthermore, in some cases, human beings are also affected. Because of the traditional peculiarities of process systems, such as insecure real-time protocols, end-to-end general-purpose ICT security mechanisms are not able to fully secure communication in SCADA systems. In this paper, we present a novel method based on the DNP3 vulnerability assessment and attack model in different layers, with feature selection using Machine Learning from parsed DNP3 protocol with additional data including malware samples. Moreover, we developed a cyber-attack algorithm that included a classification and visualization process. Finally, the results of the experimental implementation show that our proposed Cybersecurity Solution based on IDS was able to detect attacks in real time in an IoT-based Smart Grid communication environment.
B) Dados derivados do objetivo:	
Vulnerabilidades	“Attacks often happen by using steps such as reconnaissance, which consists of gathering information about the targeted system; scanning, which is about finding any weakness or

	vulnerability in the system by looking for any open ports; and running a service through the port.”

A) Dados da publicação:	
Título:	Authentication in cloud-driven IoT-based big data environment: Survey and outlook
Autor(es):	Wazid, M. and Das, A.K. and Hussain, R. and Succi, G. and Rodrigues, J.J.P.C.
Fonte de Publicação:	Journal of Systems Architecture
Ano da Publicação:	2019
Resumo:	The Internet of Things (IoT) is composed of different networked objects (i.e., smart devices) which are interconnected to gather, process, refine, and exchange meaningful data over the Internet. These objects are assigned to their respective IP addresses, and they are able to send and receive data over a network without any human assistance. IoT offers different types of applications, such as, but not limited to, smart traffic monitoring, smart home, smart health care and smart cities, to name a few. In a Cyber-Physical System (CPS), computing elements coordinate and communicate with sensor devices, which monitor cyber and physical indicators, and actuators, and also modify the cyber and physical environment where they run. The synergy of computational as well as physical components, specifically the use of CPSs, led to the advancement of IoT implementations. In a cloud-driven IoT-based big data environment, a cloud-based platform is used to store the data generated by IoT devices (normally by sensor devices) which further can be considered as a big data warehouse. This environment is highly scalable and provides important real-time event processing (for example, in critical scenarios like surveillance and monitoring of an industrial plant). In IoT-based critical applications, the real-time data access is obligatory as and when it is required. Such access is possible if we permit only authorized external users to access the real-time data directly from the IoT sensors. Sometimes authorized user may also request for big data query processing and big data analytics over the data stored in cloud servers to figure out hidden patterns of some phenomena (i.e., chances of fire in an industrial plant in future). Therefore, we need secure authentication schemes for cloud-driven IoT-based big data environment in which a legitimate user and an IoT sensor can mutually authenticate each other and establish a common session key for secure communication. In this context, this paper first discusses the network and threat models of the authentication schemes for cloud-driven IoT-based big data

	environment. Some security requirements, issues and challenges of this environment are then discussed. A taxonomy of various existing authentication schemes applicable for cloud-driven IoT-based big data environment is also discussed, which covers a comparative study of these schemes. We identify and briefly discuss some future research challenges in designing the authentication schemes and other security protocols for cloud-driven IoT-based big data environment that need to be addressed in the future.
B) Dados derivados do objetivo:	
Vulnerabilidades	"we need secure authentication schemes for cloud-driven IoT-based big data environment in which a legitimate user and an IoT sensor can mutually authenticate each other, and then can establish a common session key for their secure communication" "Furthermore, "A" can physical capture some IoT sensors or smart sensing devices to obtain the stored credentials in those devices with the help of sophisticated power analysis attacks." "The smart devices, such as IoT sensors, in the cloud-driven IoT-based big data environment may be failed due to energy issue or can be physically stolen by the adversary." "Some identified issues and challenges include limited computation power and memory storage, energy requirement, scalability, mobility, support for heterogeneous devices, dynamic security updates, protection against physical capturing, and security and privacy of IoT sensors data at the big data warehouse." "This phase is required when some sensing nodes are physically captured by an adversary or some sensing nodes are exhausted because of a power failure"

A) Dados da publicação:	
Título:	Vpnfilter malware analysis on cyber threat in smart home network
Autor(es):	Sicato, J.C.S. and Sharma, P.K. and Loia, V. and Park, J.H.
Fonte de Publicação:	Applied Sciences (Switzerland)
Ano da Publicação:	2019
Resumo:	Recently, the development of smart home technologies has played a crucial role in enhancing several real-life smart applications. They help improve the quality of life through systems designed to enhance convenience, comfort, entertainment, health of the householders, and security. Note,

	however, that malware attacks on smart home devices are increasing in frequency and volume. As people seek to improve and optimize comfort in their home and minimize their daily home responsibilities at the same time, this makes them attractive targets for a malware attack. Thus, attacks on smart home-based devices have emerged. The goals of this paper are to analyze the different aspects of cyber-physical threats on the smart home from a security perspective, discuss the types of attacks including advanced cyber-attacks and cyber-physical system attacks, and evaluate the impact on a smart home system in daily life. We have come up with a taxonomy focusing on cyber threat attacks that can also have potential impact on a smart home system and identify some key issues about VPNFilter malware that constitutes large-scale Internet of Things (IoT)-based botnet malware infection. We also discuss the defense mechanism against this threat and mention the most infected routers. The specific objective of this paper is to provide efficient task management and knowledge related to VPNFilter malware attack.
B) Dados derivados do objetivo:	
Vulnerabilidades	"This type of attack depends on the injection of data in web applications wherein it facilitates the interpretation and execution of malicious data in an unexpected way by exploiting program errors" "A buffer whose memory is allocated by a program is an example of temporary storage to deal with a surplus of data" "Authentication attack plays an important role in the protection of IoT security and privacy. The process of confirming the identity or truth of an object is known as authentication. This kind of attack is a way of exploiting and discovering security holes in web applications." "Denial of service attack: in this type of attack, a hacker denies a service to authorize the user or even creates delays through resources, generating a large amount of data." "Sybil attack: in this kind of attack, a single attacker can actually take over the networking, and multiple identities in the network are presented to the victim's node, which allows the victim's node to perform multiple operations, thus defeating the purpose of redundancy." "Sleep deprivation attack: The perception layer is limited by the battery power in the node. To prolong the life of the battery, it is necessary for the device to sleep when not in

	operation. This type of attack attempts to subvert this process by constantly controlling and sending information to the network devices." "Radio frequency jamming attack: This attack targets one of the key technologies of this layer, which consists of sensor nodes, cameras, actuators, tags / RFID readers, cell phones, tablets, GPS, and others to communicate in the smart home." "Tampering attack: This type of attack is launched when the attacker is much closer to the network device and is forced to break hardware without any permission." "Router platforms belonging to Linksys, TP-Link, Qnap, Netgear, and MikroTik implement home networks on internet gateways, making them more susceptible to the VPNFilter malware attack." "Several technical vulnerabilities are found to have been caused by human weaknesses."

A) Dados da publicação:	
Título:	Security Issues in IIoT: A Comprehensive Survey of Attacks on IIoT and Its Countermeasures
Autor(es):	Panchal, A.C. and Khadse, V.M. and Mahalle, P.N.
Fonte de Publicação:	IEEE Global Conference on Wireless Computing and Networking, GCWCN
Ano da Publicação:	2019
Resumo:	Industrial Internet of Things (IIoT) applications connect machines, sensors and actuators in high-stake manufacturing industries. Industrial systems are using the potential of IoT to reduce the unnecessary operational cost and increase the usability and reliability of the industrial assets to achieve more profits. However, such smart Industries need connectivity and interoperability to enhance performance which makes them susceptible to various attacks. Recent attacks on Cyber-physical systems raise a strong security concern as such attacks causes a huge property loss and may also lead to life threatening situations. In this paper we discuss the potential security threats to the Industries adapting to IIoT and study the various attacks that are possible on the components in the layered IIoT architecture and some of the preventive measures. Finally, we propose IIoT attack taxonomy which would help in mitigating the risks of the attacks.

B) Dados derivados do objetivo:	
Vulnerabilidades	"DoS is an attack performed on a network to restrict a server from serving its client, DoS attacks target network bandwidth or services." "Firewalls can be used to allow or deny access to the requests, DoS attack detection using IDS and better authentication and authorization system can help to avoid such attacks." "To perform a side channel attacks on cloud a malicious virtual machine is placed in cloud to target the system implementation of cryptographic algorithms." "Today most of the services in cloud still use simple username and password type of single factor knowledge-based authentication." "Phishing attacks happen when the attackers trick user to interact with the original looking fake webpages or emails, and gain access to one's confidential data. Educating people about such attack is the best way to defense against phishing." "SQL Injection: SQLi refers to an injection attack wherein attacker injects malicious input to get confidential data stored in database, delete database and bypass authentication." "Remote Code Execution occurs when an attacker exploits vulnerability in the system to introduce a malware that can control the target system remotely." "IP Spoofing: An attacker purposefully impersonates as another device by modifying the packet header with a forged IP address." "The best way to defend against sniffing attacks is to encrypt all the data passing over the communication channel."

A) Dados da publicação:	
Título:	A taxonomy of cyber-physical threats and impact in the smart home
Autor(es):	Heartfield, R. and Loukas, G. and Budimir, S. and Bezemskij, A. and Fontaine, J.R.J. and Filippoupolitis, A. and Roesch, E.
Fonte de Publicação:	Computers and Security
Ano da Publicação:	2018
Resumo:	In the past, home automation was a small market for technology enthusiasts. Interconnectivity between devices was down to the owner's technical skills and creativity, while security was non-existent or primitive, because cyber threats

	were also largely non-existent or primitive. This is not the case any more. The adoption of Internet of Things technologies, cloud computing, artificial intelligence and an increasingly wide range of sensing and actuation capabilities has led to smart homes that are more practical, but also genuinely attractive targets for cyber attacks. Here, we classify applicable cyber threats according to a novel taxonomy, focusing not only on the attack vectors that can be used, but also the potential impact on the systems and ultimately on the occupants and their domestic life. Utilising the taxonomy, we classify twenty five different smart home attacks, providing further examples of legitimate, yet vulnerable smart home configurations which can lead to second-order attack vectors. We then review existing smart home defence mechanisms and discuss open research problems.
B) Dados derivados do objetivo:	
Vulnerabilidades	"a breach of confidentiality, integrity and availability resulting from a vulnerability in a single device may result in shared exploitation across interdependent systems" "As the vast majority of smart home platforms rely on the home Internet gateway to reach respective cloud services in order to function, if an attacker can compromise a smart home Internet gateway they may be able to disrupt or gain control of almost every Internet-connected device in the household." "this does not protect against attacks that have penetrated the network and may originate from the Internet or from inside the network, such as malware infections and social engineering." "as HAPCAN utilises the CAN protocol, the protocol itself is at risk to several additional CAN vulnerabilities, such as request overload and false request to send" "UPB has no encryption and therefore any attack that is able to sniff data from the powerline (such as using a rogue UPB node) is able to read and inject data in the network." "the signals containing sensor data or actuation commands can be captured by an adversary in the vicinity, which makes strong encryption and countermeasures against replay attacks particularly important. At the same time, wireless control can be rather trivially disrupted via communication jamming."

	"WiFi de-authentication is by no means new, but in the context of the smart home, the loss of WiFi means loss of Internet connectivity in the household, on which IoT platforms are increasingly dependent in order to function." "then identifying the product vendor allows attackers to analyse the smart home and target known vulnerabilities in its devices." "Within the context of the smart home, it is the occupants who make the ultimate decision to install a new wireless security lock, presence sensor or voice-controlled assistant, as privacy and security concerns are carried out according to occupants' risk attitude, personal and social circumstances" "The threat landscape relates to the communication medium and control software used, as well as threats in the supply chain, side channel attacks and the sensory channel." "NFC is vulnerable to remote eavesdropping attacks assuming that an attacker has a powerful enough receiver to capture a NFC signal" "As workflow automation platforms can gain significant access in defining, controlling and triggering system behaviour and interaction in the smart home, this makes them a prime target for semantic social engineering attacks." "Here, an example would be the electromagnetic emanations leaking from unfiltered powerlines." "Increasingly, smart home devices come equipped with Internet access which are left poorly secured and as a result expose vulnerabilities over physical privacy." "Unauthorised access to this information would likely lead to unauthorised physical actuation as a second-order physical effect (P-UA)." "Within the smart home, non-repudiation is associated to an occupant's ability to provide evidence that distinguishes legitimate computer activity generated by themselves or fellow occupants and activity which has been executed by a malicious actor." "In the smart home, this information may now be picked up more easily by exploiting poorly protected IoT devices with

	built-in microphone systems, such as personal assistant services “

A) Dados da publicação:	
Título:	A taxonomy of cyber-physical threats and impact in the smart home
Autor(es):	Heartfield, R. and Loukas, G. and Budimir, S. and Bezemskij, A. and Fontaine, J.R.J. and Filippoupolitis, A. and Roesch, E.
Fonte de Publicação:	Computers and Security
Ano da Publicação:	2018
Resumo:	In the past, home automation was a small market for technology enthusiasts. Interconnectivity between devices was down to the owner's technical skills and creativity, while security was non-existent or primitive, because cyber threats were also largely non-existent or primitive. This is not the case any more. The adoption of Internet of Things technologies, cloud computing, artificial intelligence and an increasingly wide range of sensing and actuation capabilities has led to smart homes that are more practical, but also genuinely attractive targets for cyber attacks. Here, we classify applicable cyber threats according to a novel taxonomy, focusing not only on the attack vectors that can be used, but also the potential impact on the systems and ultimately on the occupants and their domestic life. Utilising the taxonomy, we classify twenty five different smart home attacks, providing further examples of legitimate, yet vulnerable smart home configurations which can lead to second-order attack vectors. We then review existing smart home defence mechanisms and discuss open research problems.
B) Dados derivados do objetivo:	
Vulnerabilidades	A consequence of technology convergence in the smart home is the cascading effect of compromise of one system to others. For example, a breach of confidentiality, integrity and availability resulting from a vulnerability in a single device may result in shared exploitation across interdependent systems. A secure system may be rendered vulnerable by the insecurities of a lesser protected platform on which it relies.[...] As the vast majority of smart home platforms rely on the home Internet gateway to reach respective cloud services in order to function, if an attacker can compromise a smart home Internet gateway they may be able to disrupt or gain control of almost every Internet-connected device in the household.[...] As of May 2018, an initial report by Cisco

	Talos dramatically reinforced the growing vulnerability of home internet gateways by identifying a large scale advanced persistent threat against SOHO routers titled VPNFilter.[...] [...], this does not protect against attacks that have penetrated the network and may originate from the Internet or from inside the network, such as malware infections and social engineering. [...], UPB has no encryption and therefore any attack that is able to sniff data from the powerline (such as using a rogue UPB node) is able to read and inject data in the network. [...], the signals containing sensor data or actuation commands can be captured by an adversary in the vicinity, which makes strong encryption and countermeasures against replay attacks particularly important. At the same time, wireless control can be rather trivially disrupted via communication jamming. [...]WiFi de-authentication is by no means new, but in the context of the smart home, the loss of WiFi means loss of Internet connectivity in the household, on which IoT platforms are increasingly dependent in order to function. Whilst the vulnerability in question was addressed in 2009 by introduction of the 802.11w RFC, which strengthened the authenticity and integrity of WiFi management packets, consumer-based router manufacturers do not often implement this extension into their WiFi protocol stack. So, even though 802.11w is available in most recent Linux kernels and Windows OS (since Windows 8), often this feature must be disabled in order for it to be compatible with household WiFi routers. [...] then identifying the product vendor allows attackers to analyse the smart home and target known vulnerabilities in its devices. Within the context of the smart home, it is the occupants who make the ultimate decision to install a new wireless security lock, presence sensor or voice-controlled assistant, as privacy and security concerns are carried out according to occupants' risk attitude (Rahmati et al., 2018), personal and social circumstances[...] For the immediate future, the smart home technology landscape is likely to be volatile, consisting of both legacy

	and emerging IoT platforms, each with their own security risks. The threat landscape relates to the communication medium and control software used, as well as threats in the supply chain, side channel attacks and the sensory channel. However, due to a lack of definable NFC wireless communication standards and a proliferation of NFC-enabled systems, a number of vulnerabilities have been found across a range of NFC implementations. For example, NFC is vulnerable to remote eavesdropping attacks assuming that an attacker has a powerful enough receiver to capture a NFC signal (Kennedy and Hunt, 2008) (by design, NFC requires extremely close proximity between the transponder and receiver, e.g., up to 10 cm).[...] As workflow automation platforms can gain significant access in defining, controlling and triggering system behaviour and interaction in the smart home, this makes them a prime target for semantic social engineering attacks (Heartfield and Loukas, 2016). Whilst an attacker may not necessarily target a specific vulnerability in workflow automation platforms themselves, a successfully crafted phishing email that deceives a user into divulging their account's username and password potentially provides an attacker with the ability to edit, delete and create new workflow automation rules in the target household.[...] Here, an example would be the electromagnetic emanations leaking from unfiltered powerlines. Enev et al. (2011) have demonstrated the viability of measuring a home's powerline activity with such accuracy that they could identify what the occupants were watching on television. Their method was reproducible and accurate enough across a wide range of modern television sets. Increasingly, smart home devices come equipped with Internet access which are left poorly secured and as a result expose vulnerabilities over physical privacy. For example, Internet device scanning search engines (such as Shodan), allow attackers to identify open ports of nodes, indexing the header or banner information of responsive nodes; which can include information such device type, model, vendor, firmware version other open protocols.[...] [...] Unauthorised access to this information would likely lead to unauthorised physical actuation as a second-order physical effect (P-UA).

	Within the smart home, non-repudiation is associated to an occupant's ability to provide evidence that distinguishes legitimate computer activity generated by themselves or fellow occupants and activity which has been executed by a malicious actor. [...] [...]In the past, threats to this communication medium were low as only very targeted attacks (such as physical bugging) posed a risk. In the smart home, this information may now be picked up more easily by exploiting poorly protected IoT devices with built-in microphone systems, such as personal assistant services (e.g., Google Home, Amazon Echo), children toys and other voice-controlled house-hold appliances.

A) Dados da publicação:	
Título:	Introduction to em information security for IoT devices
Autor(es):	Hayashi, Y. and Verbauwhede, I. and Radasky, W.A.
Fonte de Publicação:	IEEE International Symposium on Electromagnetic Compatibility
Ano da Publicação:	2018
Resumo:	With the advent of the Internet of Things (IoT), many electronic devices (e.g., smart meters, surveillance cameras, mobile devices, and multiple sensors) are interconnected. Each device gathers data and uploads it to servers via communication networks. Servers store the large volumes of received data in databases. Applications analyze this data and extract valuable information. Finally, based on this information, new services (in domains such as smart cities, public safety, e-commerce, medical, healthcare, or automobile) are provided. In this data flow, systems and applications in the upper layer trust the hardware in the lower layer, which includes data-gathering devices. If the collected information is intentionally modified by adversaries, services in the upper layer could be disrupted. Therefore, to ensure service continuity in the IoT, it is important to secure the hardware layer in which data are harvested and transmitted. In this paper, we focus on hardware-level security in IoT systems and classify the schemes proposed for physical security of IoT into three categories. We also provide examples for each of these and explain threats and countermeasures.
B) Dados derivados do objetivo:	
Vulnerabilidades	The vulnerability due to electromagnetic waves can be largely classified into three categories: (1) electromagnetic emanation resulting from information processing within devices, (2)

	intentional electromagnetic interference to devices, and (3) intentional modification of system circuit configuration

A) Dados da publicação:	
Título:	A taxonomy of security and privacy requirements for the Internet of Things (IoT)
Autor(es):	Alqassem, I. and Svetinovic, D.
Fonte de Publicação:	International Conference on Industrial Engineering and Engineering Management
Ano da Publicação:	2014
Resumo:	Capturing security and privacy requirements in the early stages of system development is essential for creating sufficient public confidence in order to facilitate the adaption of novel systems such as the Internet of Things (IoT). However, security and privacy requirements are often not handled properly due to their wide variety of facets and aspects which make them difficult to formulate. In this study, security-related requirements of IoT heterogeneous systems are decomposed into a taxonomy of quality attributes, and existing security mechanisms and policies are proposed to alleviate the identified forms of security attacks and to reduce the vulnerabilities in the future development of the IoT systems. Finally, the taxonomy is applied on an IoT smart grid scenario.
B) Dados derivados do objetivo:	
Vulnerabilidades	Access control mechanisms limit access to various system's resources (e.g., data, services, hardware, etc.) by identifying who can access what resources, and constrain what a legitimate user can do by controlling who is doing what in the system. - 1) Identification The focus of the identification is to uniquely identify objects and manage their identities while considering security and high scalability aspects of the IoT. Reaching a consensus on how to identify objects involved in the IoT and managing their identities is fundamental for constructing robust authentication and authorization mechanisms. - 2) Authentication While authorization defines the rights and privileges after an entity gains access to a system, authentication, i.e., identity verification, plays a vital role before establishing a communication channel between two entities. In the IoT, authentication protocol should be developed to confirm

	mutual trust between different objects, users or systems by verifying their identities - 3) Authorization Authorization is the process of granting, denying or limiting access to data, resources or applications within a system. One possible approach for object and user authorization in the IoT is Role-Based Access Control (RBAC). RBAC is an access management technique for multi user and multi-application online systems. In RBAC each role has different functions, an entity can have one or more roles and management of permission is carried out based on entity's role(s) Dealing with transaction disputes to assure fair exchange is a common security concern in the business field which will be engaged in the IoT. Thus, it is necessary to build in non-repudiation into the design of the appropriate transport protocol that deals with network failures and prevents a dishonest entity from cheating, deceiving about its real identity or aborting a transaction (i.e., roll-back attack)

A) Dados da publicação:	
Título:	Comprehensive survey and taxonomies of false data injection attacks in smart grids: attack models, targets, and impacts
Autor(es):	Reda, H.T. and Anwar, A. and Mahmood, A.
Fonte de Publicação:	Renewable and Sustainable Energy Reviews
Ano da Publicação:	2022
Resumo:	Smart Grid is organically growing over the centrally controlled power system and becoming a massively interconnected cyber–physical system with advanced technologies of fast communication and intelligence (such as Internet of Things, smart meters, and intelligent electronic devices). While the convergence of a significant number of cyber–physical elements has enabled the Smart Grid to be far more efficient and competitive in addressing the growing global energy challenges, it has also introduced a large number of vulnerabilities in the cyber–physical space culminating in violations of data availability, integrity, and confidentiality. Recently, false data injection (FDI) has become one of the most critical types of cyberattacks, and appears to be a focal point of interest for both research and industry. To this end, this paper presents a comprehensive review in the recent advances of the FDI attacks, with particular emphasis on adversarial models, attack targets, and

	impacts on the Smart Grid infrastructure. This review paper aims to provide a thorough understanding of the incumbent threats affecting the entire spectrum of the Smart Grid. Related literature are analyzed and compared in terms of their theoretical and practical implications to the Smart Grid cybersecurity. In conclusion, a vast range of technical limitations of existing false data attack research is identified, and a number of future research directions is recommended.
B) Dados derivados do objetivo:	
Vulnerabilidades	[...] Moreover, as attacks from cyber criminals on the power grid continue to rise in complexity and frequency, it is inevitable that various parts of the Smart Grid are vulnerable to the incumbent attacks. Therefore, it is required to provide strong attack defence across the EMS and to deploy secure communication protocols. [...]For example, in wireless sensor networks (WSNs), the inherent wireless communication and broadcast channels between the nodes increase the vulnerability of adversaries that may eavesdrop on all traffic, inject false data reports containing erroneous sensor readings, or can even deplete the already limited energy capacity of sensor nodes[...] [...]The vulnerability issues in the SE problem can be investigated with respect to the various cyber-and physical elements, including Physical properties of the power system, communication systems, IEDs, and AMIs. Related attack targets also include transmission lines [101], [112], topology [69], [99], [132], and system observability [106].

A) Dados da publicação:	
Título:	A survey on Classification of Cyber-attacks on IoT and IIoT devices
Autor(es):	Shah, Y. and Sengupta, S.
Fonte de Publicação:	Annual Ubiquitous Computing, Electronics and Mobile Communication Conference
Ano da Publicação:	2020
Resumo:	Internet of Things (IoT) devices have gained popularity in recent years. With the increased usage of IoT devices, users have become more prone to Cyber-attacks. Threats against IoT devices must be analyzed thoroughly to develop protection mechanisms against them. An attacker's purpose behind launching an attack is to find a weak link within a network and once discovered, the devices connected to the network become the primary target for the attackers.

	Industrial Internet of Things (IIoT) emerged due to the popularity of IoT devices and they are used to interconnect machines, sensors, and actuators at large manufacturing plants. By incorporating IIoT at their facilities companies have benefited by reducing operational costs and increasing productivity. However, as IIoT relies on utilizing the Internet to operate it is vulnerable to Cyber-attacks if security is not taken into consideration. After seeing the advantages of IIoT, a new version of smart industries has been introduced called Industry 4.0. Industry 4.0 combines cloud and fog computing, cyber-physical systems (CPS), and data analytics to automate the manufacturing process. This paper surveys the different classifications of attacks that an attacker can launch against these devices and mentions methods of mitigating such attacks1
B) Dados derivados do objetivo:	
Vulnerabilidades	[...]However, if the data is encrypted and the attackers obtain the key that's used to encrypt the data, the information can be modified.[...] Once the malicious firmware has been transferred to the intended device the only other piece of information that the attacker needs is the architecture of the device's processor which can be easily located by looking at the device's manual. The attacker uses the flaws which exist in the verification of firmware updates to their advantage and the malicious code runs once the firmware updates are installed. Software failure: Smart home systems depend on software to be controlled and operated upon. Any existence of vulnerabilities in the implementation of the software makes those systems a primary target for attackers. [...]DoS and DDoS attacks target a vulnerability that is found in the Transmission Control Protocol (TCP) [11]. In order to connect to the Internet, devices use the TCP's three-way handshake methodology. These attacks exploit TCP's handshake by directing a high volume of requests to establish a TCP connection with the target server. Eavesdropping involves illegally listening to personal conversations in real-time by monitoring emails, phone calls, or video conferences [...]An attacker can listen in on the conversations when the data is being transferred through unsecured servers, when

	unwanted ports are left open, or when the device is connected to unsecured public Wi-Fi networks. Passwords are often considered as important keys which are used to unlock personal information. Password attacks are carried out using various methods such as password guessing, password resetting, and password capturing. Password guessing, as the name suggests, involves the attacker inputting commonly used password combinations until they find a match. Password re-usage is also another major problem as once the attacker knows the password they can use it to access multiple accounts[...] Side Channel Attacks: Performing side channel attacks on M2M machines requires physical access to these machines. Attackers can use the peripheral information of the physical devices to extract confidential information from them. These types of attacks can also help attackers retrieve cryptography algorithms keys from the devices [...] An attacker requires physical access to an M2M device and takes full control of it. This form of attack is achieved by physically damaging or replacing a node in the device.[...] When accessing cloud services a user must enter authentic credentials. However, the authentication process and mechanisms are highly vulnerable and often targeted. Many cloud services still utilize single-factor authentication and a simple username and password requirements. Attackers use this vulnerability to their advantage when trying to disrupt services or steal information from an enterprise taking advantage of cloud computing. Phishing is used to trick people into entering their personal information or downloading malicious software that is capable of spreading malware. The most common form of phishing attacks are emails that contain links to fake websites, and/or malicious attachments [...] Implementing poor password requirements is the primary reason IoT/IIoT networks are targeted. Outdated software may contain flaws that allow attackers to gain access to personal information. Companies often release software updates when the current version contains security vulnerabilities or bugs that can be exploited by attackers. Always ensure to download updates from trusted sources and

	if possible enroll the device to automatically install updates from the manufacturer's website. When setting up the environment for IoT/IIoT devices ensure that they are kept separate from the rest of the devices to limit the possibility of an external device causing problems. Keeping these devices in a separate private network also eliminates the possibility of an attacker infecting other devices and spreading the malware in the network. Another benefit of this implementation is that only authorized users are going to have the ability to access and modify data. Changing default settings: Many times the default settings that are assigned by the device manufacturers benefit the company rather than its users. Manufacturers often add or enable features that are not essential in the operation of the device that aids attackers in launching their attacks. These settings should be checked and changed immediately after the device is purchased and setup.

A) Dados da publicação:	
Título:	On Threat Analysis of IoT-Based Systems: A Survey
Autor(es):	Zhao, W. and Yang, S. and Luo, X.
Fonte de Publicação:	IEEE International Conference on Smart Internet of Things, SmartIoT
Ano da Publicação:	2020
Resumo:	In this paper, we provide a survey on threat analysis of systems based on Internet of Things (IoT), and how the blockchain technology can help mitigate the threats. Although the topic of IoT security (and previously the security of wireless sensor networks) has been reviewed extensively, we believe that the topic deserves a more in-depth examination towards a more systematic threat analysis, which is not only necessary to better understand the threats against IoT-based systems, but also paves the way to effectively improve the security of IoT-based systems by integrating with the blockchain technology. The major research contributions of this paper include a new taxonomy of the threats against IoT-based systems, identify what threats can be effectively mitigated by integrating IoT with with blockchain technology, the challenges faced by the blockchain-enabled IoT-based systems, and the likely approaches to overcoming these challenges.

B) Dados derivados do objetivo:	
Vulnerabilidades	At the sensing layer: Eavesdropping. Because the IoT devices are transmitting wirelessly, it is easier to intercept the transmitted signals even if the IoT devices are protected with physical security. Sleep deprivation. Many IoT devices use battery as the power sources, hence, they only sense and transmit periodically and go to a sleep state in between. The aim of this attack is to somehow prevent the devices from going to sleep or to minimize the sleep period, thereby drain the batter much faster than normal usage. Eventually, this attack will lead to the battery-drained IoT devices to be out of the service. Side channel attacks. This kind of attacks aim to gather sensitive information without actually intercepting the message transmitted. Instead, the information gathering is based on observing the electromagnetic fields from the IoT devices, or the power assumption of the IoT devices. Booting attacks. Because the firmware/operating systems used by low-cost IoT devices might not have been as robustly tested as desktop/server operating systems, the boot process might be exploited to compromise the device. Obviously, this would require the device to be physically captured first. Malicious code injection. An adversary aims to install a compromised version of the software/firmware during wireless updates of the IoT device, which could give the adversary full remote control over the compromised device. The network layer: Phishing site attack. It is no different from the regular phishing attack where a link is sent to a user pretending to be a legitimate site and if the user clicked the link, the user might be tricked to provide confidential information. We are puzzled as to why this is classified as a network layer attack. Access attack. It is also called advanced persistent threat, which refers to the gaining of unauthorized access to the IoT network with the aim of collecting sensitive information. Denial of service (DoS) or distributed denial of service attacks (DDoS). These types of attacks aim to overwhelm

	the target system with network traffic to essentially make it unable to provide services to legitimate clients. Like any other online systems, IoT devices are vulnerable to DoS/DDoS attacks as well. The middleware layer: Signature wrapping. This attack exploits a vulnerability exists in XML signatures, which effectively invalidate the properties offered by the digital signature, such as non-repudiation. Man-in-the-middle. This attack would be successful if the MQTT publish-subscribe protocol is used and the proxy for the protocol is compromised. At the application layer: Access control attack. This attack exploits the vulnerability in access control and an adversary may gain access to resources illegally, which could lead to the theft of confidential information or compromise the integrity of the entire system. Physical Layer: Insecure configuration. If the IoT software configuration and initiation are not done properly, the devices might be compromised remotely. Not only the data collected by the devices may be stolen, the devices themselves could be used to launch a DDoS attack, as the malware Mirai has demonstrated. Physical security. Low-cost IoT devices that must be deployed in unprotected field are inevitably facing physical threats. Network Layer: Resource depletion. This includes all attacks that aim to render the device unavailable due to exhaustion of available memory to perform its normal operations, such as the replay, duplicate, and fragmentation attacks that exploit the vulnerabilities of the 6LoWPAN protocol used by IoT devices.

	Routing protocols. This include all attacks on routing protocols used by IoT devices. One routing protocol is the RPL, which was designed to run on top of low power and lossy networks.

A) Dados da publicação:	
Título:	Towards a Secure Internet of Things: A Comprehensive Study of Second Line Defense Mechanisms
Autor(es):	Kamaldeep and Dutta, M. and Granjal, J.
Fonte de Publicação:	IEEE Access
Ano da Publicação:	2020
Resumo:	The Internet of Things (IoT) exemplifies a large network of sensing and actuating devices that have penetrated into the physical world enabling new applications like smart homes, intelligent transportation, smart healthcare and smart cities. Through IoT, these applications have consolidated in the modern world to generate, share, aggregate and analyze large amount of security-critical and privacy sensitive data. As this consolidation gets stronger, the need for security in IoT increases. With first line of defense strategies like cryptography being unsuited due to the resource constrained nature, second line of defense mechanisms are crucial to ensure security in IoT networks. This paper presents a comprehensive study of existing second line of defense mechanisms for standardized protocols in IoT networks. The paper analyzes existing mechanisms in three aspects: Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS) and Intrusion Response Systems (IRS). We begin by providing an overview of standardized protocol stack, its layers and defensive security systems in IoT. From there, we build our narrative by presenting an extended taxonomy of IDS, IPS and IRS classifying them on their techniques, deployment, attacks, datasets, evaluation metrics and data pre-processing methods. We then thoroughly review, compare and analyze the research proposals in this context, considering the unique characteristics involved in these systems. Based on the extensive analysis of the existing defensive security systems, the paper also identifies open research challenges and directions for effective design of such systems for IoT networks, which could guide future research in the area.
B) Dados derivados do objetivo:	
Vulnerabilidades	6LoWPAN mechanisms often suffer a bottleneck in processing and forwarding fragmented packets that further lead to problems of buffer overflow in constrained devices.

	UDP, being an unreliable, connectionless and lighter protocol, has been accepted as de facto standard in IoT. But, UDP has inherent weakness whereby attackers can launch DDoS attacks, one them being the UDP flooding attack. The most promising standard application layer protocol for small IoT devices is CoAP [14]. As an extremely heterogeneous technology, security is a critical aspect of IoT on multiple levels of securing data, communication and networks. Attacks on IoT have become extremely targeted and sophisticated. As already discussed, first line of defense mechanisms like cryptography are insufficient due to the resource constrained nature of IoT devices which limits their ability to host and implement sophisticated cryptographic algorithms in real time. Also, the ad hoc nature of IoT networks lets devices connect to each other at runtime, typically for shorter durations, consequently creating a collaborative network. Denial of Service (DoS) Attacks: The second most common and the easiest to launch is the DoS attack and when this attack is launched by multiple compromised systems on a single victim, it is termed as Distributed Denial of Service (DDoS) attacks. Also present in the IoT, DoS tries to put a node or a network out of operation by flooding it with (possibly incorrect) requests, preventing the node to accept and process legitimate requests.[...] Spoofing Attacks: Various other classes of attacks detected in the IoT include impersonation or spoofing attack, physical tampering of devices, man-in-the-middle, data integrity, authentication and adversarial attacks. Penetration Attacks: Penetration attacks exploit vulnerabilities in the system and involve any unauthorized access or modifications to system's resources and data. In such attacks, attackers gain control of the system by exploiting a number of software flaws.[...]

A) Dados da publicação:	
Título:	Security and Privacy of Smart Cities: Issues and Challenge
Autor(es):	Sookhak, M. and Tang, H. and Yu, F.R.
Fonte de Publicação:	International Conference on High Performance Computing and Communications

Ano da Publicação:	2019
Resumo:	Smart city has been emerged as a new paradigm to dynamically optimize the resources in cities and provide better facilities and quality of life for the citizens. Despite the potential vision of smart cities, security and privacy issues remain to be carefully addressed. In this paper, we present a comprehensive survey of security and privacy issues of smart cities, and categorize the present and future developments within this area. We also describe a thematic taxonomy of security and privacy issues of smart cities to highlight the requirements for designing a secure smart city, identify the existing security and privacy solutions, and present open research issues and challenges of security and privacy in smart cities.
B) Dados derivados do objetivo:	
Vulnerabilidades	Heterogeneous Interaction and the Requirement of the Lightweight Cryptographic Algorithm: The connected devices and smart objects usually interact in heterogeneous environments due to the diversity of manufacturers and enterprises for designing such devices under different standards, protocols, and technical requirements. As a result, it is very difficult to propose a security method that can meet the requirements, homogeneity, and interoperability criteria of all smart city devices. Secure Storage and Transaction Logging: [...]because of the presence of unverified storage services and mismatched security policies, there are several vulnerabilities that threaten the security of auto-tiering databases: (i) The auto-tiering databases automatically reallocate the data based on the rate of the access requests with the range of rarely accessed to critical information. Data and Computation Outsourcing: Cloud computing provides an effective way to store the huge amount of collected data and perform the computation with minimum overhead on connected devices in the smart cities. However, by outsourcing the data in the remote servers, the physical control over the data is taken away and the management of data is delegated to an untrusted CSP. Anonymity: [...]Designing an efficient end-to-end anonymity method to protect user privacy on the basis of concealing data communication paths is still a critical challenge in smart cities because of the large number of IoT devices (e.g., sensors) for data collection.[...]

A) Dados da publicação:	
Título:	Security Challenges in IoT enabled Smart Grid: Taxonomy of Novel Techniques and Algorithm
Autor(es):	Prakash, S. and Jaiswal, S.
Fonte de Publicação:	International Conference on Inventive Computation Technologies
Ano da Publicação:	2018
Resumo:	The traditional power system network is under a process of evolution to Smart Grids (SGs) to take care of the issues like uni-directional communication, energy wastage, information flow, security and resource sharing. Smart grid is an electrical grid which provides energy to the end users with effectiveness efficiency. Smart grid offer bi-directional information flow between service providers and consumers, including power generation, transmission, consumption, distribution and its use frameworks. Due to its vast usage and huge network electronic power conditioning, power distribution, control of the production of energy and its distribution becomes difficult. To overcome such problems Internet of Things will provide the necessary support to smart grid so that easy transmission and power distribution will take place with much needed convenient system to operate. Smart grid is also using the internet facility for exchange of data which makes the system more vulnerable and prone to cyber-attack. In this paper, there has been a constant effort to analyse the different methods to solve the above problems by employing different strategies algorithms.
B) Dados derivados do objetivo:	
Vulnerabilidades	Access control-it is a security technique that can be used to provide physical and technical security. It is the process of limiting unauthorized or unwanted indulgence of any unauthorized access. Cryptography techniques for securing IOT aided SG. Cryptography is science art and study of hiding essential information from the perspective of keeping information safe.

A) Dados da publicação:	
Título:	A systemic and cognitive vision for IoT security: A case study of military live simulation and security challenges
Autor(es):	Sfar, A.R. and Chtourou, Z. and Challal, Y.
Fonte de Publicação:	International Conference on Smart, Monitored and Controlled Cities

Ano da Publicação:	2017
Resumo:	Securing data, objects, networks, systems and people in the Internet of Things (IoT) will have a prominent role in the research and standardization activities of the next years. The high connectivity of intelligent objects and their severe constraints lead to many security challenges, which are not included into the classical formulation of security problems and solutions. To help interested researchers to contribute to this research area, an IoT security roadmap overview is presented in this work based on a novel cognitive and systemic vision. The role of each component of the approach will be explained and relations with the other elements and their impact on the overall system will be detailed. According to the novel taxonomy of IoT vision, a case study of military live simulation will be presented to highlight components and interactions of the systemic and cognitive approach. Then, a discussion of security questions about privacy, trust, identification and access control will be provided, and different research challenges will be highlighted.
B) Dados derivados do objetivo:	
Vulnerabilidades	Their behavior depends on their personalities, skills, knowledge, motivations, expectations, visions, etc. To address security questions related to people in loT context, it is meaningful to handle them within a systemic approach by providing a global revision of rules and practices. For example, we consider different types of human profiles such as consumers, end users, service or technology providers, etc. All of them are necessary in controlling and improving security issues. Identification/Access Control: Used to identify and localize objects, systems and persons. Due to its specific features (size, ubiquity, heterogeneity, etc.), IoT architecture has to consider access and identification of any intelligent object by any remote system through a global identification and addressing system would be mandatory. Auto-Immunity: Concerns exclusively intelligent objects because they may be exposed to physical attacks in hostile areas (absence of communication channel, limitations of memory and calculation capacity, limited physical defense, etc.).

A) Dados da publicação:	
Título:	Autonomous Vehicle Security: A Taxonomy of Attacks and Defences
Autor(es):	Thing, V.L.L. and Wu, J.
Fonte de Publicação:	local de publicação
Ano da Publicação:	2017
Resumo:	texto contendo uma descrição do resumo
B) Dados derivados do objetivo:	
Vulnerabilidades	An attack vector is a path or means by which an adversary can gain unauthorized access to a target system. It is also an enabler for adversaries to carry out vulnerability exploitation on the target systems. Adversaries could gain unauthorized access to autonomous vehicles via either physical access (or close proximity access) or wireless remote access. - Side-channel attacks: A side-channel attack refers to attacks that result in revealing useful information regarding the transmitted data or the internal working of the system through alternative paths. - Code Modification: [...]Defences against such attacks is to ensure connections to the vehicle are password-protected so that only authorized personnel are granted access, and that only authorized and verified code modification can be carried out. - Code Injection Jamming attacks are availability attacks against the wireless medium or the external facing sensors. Consequently, the authorized communication is disrupted[...] Encryption is fundamental and crucial in protecting vehicular data transmission. Through encryption, the confidentiality of the data transmission can be assured. To ensure that the controllers of the AV can be trusted, certificates can be issued to support the authentication process

A) Dados da publicação:	
Título:	Security and Privacy of Smart Cities: A Survey, Research Issues and Challenges
Autor(es):	nome dos autores
Fonte de Publicação:	local de publicação
Ano da Publicação:	ano de publicação
Resumo:	texto contendo uma descrição do resumo
B) Dados derivados do objetivo:	

Vulnerabilidades	[...]One of the best ways to secure the smart cities communications is to develop lightweight cryptographic methods for encrypting and decrypting data and creating a shared secret key among various nodes.[...] Viruses, worms, and other malware have the capability to overwhelm the systems through the boot sectors where in the such viruses are located as an executable code and are able to be distributed to the other systems through the Internet connection or upon booting the other system using infected disks.[...] Indeed, secure boot is designed as an additional layer to protect the system against the pre-boot process. Secure booting is a technology for helping the system firmware to check the existence of a cryptographic signature for the system boot loader. Autenticação, Identificação e Controle de Acesso Secure Authentication and Access Control for IoT-Based Objects: The smart devices, like smart phones and sensing nodes, are responsible to collect data in the smart cities, suffer from resource limitation, e.g., energy resources and processing power. As a result, protecting the security of data in such devices requires proposing a lightweight cryptographic algorithm that incurs minimum computation cost on them

A) Dados da publicação:	
Título:	Internet of Things-Based Security Model and Solutions for Educational Systems
Autor(es):	Patnaik, R. and Raju, K.S. and Sivakrishna, K.
Fonte de Publicação:	Studies in Big Data
Ano da Publicação:	2021
Resumo:	Today the applications of Internet of things (IoT) are progressing rapidly in variety of domains. This encouraged to develop new applications (e.g., smart grid, smart home, smart cities, wearables, and vehicle networking) advancement as well. The emerging application of IoT is exposed toward security, privacy issues, and its challenges. The main objective of this work is to enhance security in the educational system (ES) using IoT devices. We propose several techniques to avail device identification, authenticate

	the user, and collect the data from various devices. As the IoT sensors are easily negotiable, it allows unauthorized users/devices that are able to steal and override the data from the cloud. This paper represents a brief summary of IoT security threats and challenges and their classification based on the application domain. The authors identified challenges in security issues in IoT-based educational systems and some probable solutions on security. In this research, the authors propose the incremental Gaussian mixture model (IGMM), blockchain, and EdgeSec as a probable solution for security and machine learning (ML) techniques. In this model, few solutions, like IGMM for authorizing the device, blockchain for the encryption of data during transfer in the information network, ML algorithms for identifying and authorizing devices, and EdgeSec, offer a security profile to collect a huge amount of data about each device in the connected IoT environment. The identified model is used for enhancing security in IoT-based educational systems.
B) Dados derivados do objetivo:	
Vulnerabilidades	Physical Level: Jamming Adversaries: This kind of attack is done by decreasing of network that sent frequency signal without following the any protocols. Insecure Initialization: To ensure a proper and secure network service in IoT, we must initialize and configure IoT devices in the physical layer without deviating secrecy and obstacle to the network. Insecure Physical Interface: Debugging exploits to negotiated nodes in the network by the poor physical security with the help of physical interface and tools Sleep Deprivation Attack: IoT devices are designed to consume low power so these are getting into sleep mode. The attackers are trying to not enter the device into sleep mode. It is known as sleep deprivation Middle Level Buffer Reservation Attack: Nodes are accessing the buffer to send or receive packets and reserving buffer for regathering of storing of packets, by sending broken packets it may be exploited by an attacker [...] It is ensured that the use of cryptographic mechanisms secure data communication over IoT devices

	Logical Level [...]Application layer is consisting of various types of applications for a different purpose, which is sometimes vulnerable. Insecure Interfaces: The IoT service interfaces used in cloud, Web, and mobile are responsible for susceptible to several attacks, which causes loss of privacy of the data Insecure of Software/Firmware: The software/firmware may cause several susceptibilities which make IoT insecure

A) Dados da publicação:	
Título:	A comprehensive survey of security threats and their mitigation techniques for next-generation SDN controllers
Autor(es):	Han, T. and Jan, S.R.U. and Tan, Z. and Usman, M. and Jan, M.A. and Khan, R. and Xu, Y.
Fonte de Publicação:	Concurrency and Computation: Practice and Experience
Ano da Publicação:	2020
Resumo:	Software Defined Network (SDN) and Network Virtualization (NV) are emerged paradigms that simplified the control and management of the next generation networks, most importantly, Internet of Things (IoT), Cloud Computing, and Cyber-Physical Systems. The Internet of Things (IoT) includes a diverse range of a vast collection of heterogeneous devices that require interoperable communication, scalable platforms, and security provisioning. Security provisioning to an SDN-based IoT network poses a real security challenge leading to various serious security threats due to the connection of various heterogeneous devices having a wide range of access protocols. Furthermore, the logical centralized controlled intelligence of the SDN architecture represents a plethora of security challenges due to its single point of failure. It may throw the entire network into chaos and thus expose it to various known and unknown security threats and attacks. Security of SDN controlled IoT environment is still in infancy and thus remains the prime research agenda for both the industry and academia. This paper comprehensively reviews the current state-of-the-art security threats, vulnerabilities, and issues at the control plane. Moreover, this paper contributes by presenting a detailed classification of various security attacks on the control layer. A comprehensive state-of-the-art review of the latest mitigation

	techniques for various security breaches is also presented. Finally, this paper presents future research directions and challenges for further investigation down the line.
B) Dados derivados do objetivo:	
Vulnerabilidades	In SDN (Software Defined Network), all network-related functionalities are managed, controlled and secured from a centralized controller. The single-point dependency and programmable nature of an SDN controller make it a potential choice for the attackers. If security of the controller is compromised, the whole network is vulnerable to various attacks.[...] The southbound interface needs to be protected and secured against communication overhead. Therefore, unnecessary communication that results in congestion at this interface needs to be avoided for the smooth functioning of the network.[...] DoS/DDoS attacks: The denial-of-service (DoS) and distributed DoS (DDoS) are the most common attacks launched by cyber criminals, cyber extortionists, and hackers. Spoofing attacks on the SDN controller: The controller is the backbone of an SDN network as it manages and controls the whole network. Due to its centralized nature, it is vulnerable to many types of security attacks. One such attack is spoofing attack. In spoofing attacks, an adversary launches attacks on a legal entity (server/system) by mimicking a legitimate user. [...] The only thing that an attacker requires is the same privileges as a normal user. On the other hand, during SQL injection attacks, a perpetrator modifies the anticipated effect of an SQL query by injecting new SQL keywords or operators into the query. [...]

A) Dados da publicação:	
Título:	Study of the different security threats on the internet of things and their applications
Autor(es):	Sahmi, I. and Mazri, T. and Hmina, N.
Fonte de Publicação:	International Conference Proceeding Series
Ano da Publicação:	2019
Resumo:	The Internet of Things is one of the revolutions of the industry 4.0. It will change our lives mode. It will be present in every domain: healthcare, transportation, at home, agriculture generally in the city. Everyone will be connected

	to the Internet by the IoT. Furthermore, to realize this vision, the communication through IoT must be secure. So, it's one of the greatest challenges faced by the scientist's community today in their recent researches. This paper is a study of the different security threats on the Internet of Things by category in one hand: on data and network, on privacy and on system and IoT, and on the other hand we will details some threats on application's domain like smart home and smart city.
B) Dados derivados do objetivo:	
Vulnerabilidades	physical attacks : Node Tampering: The attacker can cause damage to a sensor node, by physically replacing the entire node or part of its hardware or even electronically interrogating the nodes to gain access and alter sensitive information [8]. RF Interference on RFIDs: The attacker by creating and sending noise signals over the Radio Frequency signals [9], the noise signals will interfere with the RFID signals hindering communication. Malicious Node Injection: The attacker deploy a new malicious node between two or more nodes of the IoT system, hence controlling all data flow; this is also known as Man in The Middle Attack [8]. Physical Damage: The attacker can physically damage devices of the IoT network with the purpose of impacting the availability of service [8]. Sleep Deprivation Attack: This attack, keeps the nodes awake which will result in a more power consumption, and will cause the nodes to shut down [8]. Malicious Code Injection: The attacker compromises a node by physically injecting it with malicious code that would give him access to the IoT system [8]. Social Engineering: The attacker manipulates users of an IoT system, to extract private information [8]. network's attacks: RFID Cloning: An attacker clones an RFID tag by copying data from the victim's RFID tag, onto another RFID tag [8]. RFID Unauthorized Access: The attacker can read, modify or even delete data on the RFID nodes, Because of the lack of proper authentication mechanisms in most RFID systems [11]. The attacker over the network manages to interfere between two sensor nodes, accessing restricted data, violating the privacy of the two nodes by monitoring, eavesdropping and controlling the communication between the two sensor nodes [12].

	Denial of Service: An attacker can bombard an IoT network with more traffic data that it can handle which can result in a successful Routing Information Attacks by spoofing, altering or replaying routing information can complicate the network and create routing loops [13]. IoT devices have limited resources so they are more vulnerable than the others, so it's necessary to study the different vectors of vulnerabilities: IoT Device Memory: Most of the IoT devices have a limited memory capacity and therefore external memory is needed to satisfy the demands. This will open threat points for the system in many ways [1]. IoT Web Interfaces: Most of the IoT devices may have a web interface which needs to be connected to database servers. One of the major security threats for such systems is SQL injection and cross-site scripting are some of the attacks that could impact the web interfaces IoT [17]. IoT device network services: Inability to execute high-level encryption algorithms on IoT devices make it vulnerable to information disclosure attacks. Due to the resource constraints such as computational power and data storage capacity, IoT devices are not expected to perform payload verification and integrity checking which make the system insecure [17]. IoT device software update: Software update is one process which should never fail or compromise in an IoT based system. Manually updating the patches for every IoT device may not be feasible. A cloud-based approach is one solution, but since the cloud also imposes security threats, updating the software patches for IoT devices is still under research [1]. IoT Data storage methods: Due to limited processing power and storage capacity, the data stored in IoT devices may be unencrypted. Most of IoT devices will support only symmetric encryption [1]. IoT AAA services: IoT Authentication, Authorization, and Accounting (AAA) services will be a challenging task. Because of the distributed nature of IoT systems, the device responsible for AAA will be under great challenge [1]. Phishing Attacks: The attacker gains access to confidential data by spoofing the authentication credentials of a user, usually through infected emails or phishing websites [14]. Malicious Scripts: The user that controls the gateway can be fooled into running executable active-x scripts which could result in a complete system shut down or data theft [18]. Denial of Service: An attacker can execute DoS or distributed denial of service DDoS attacks on the affected IoT

	network through the application layer, affecting all users in the network [18] From physical attack, malicious code injection attack has been the dangerous attack since it is not only stopping the services but also modify the data.

A) Dados da publicação:	
Título:	A survey on attacks in Internet of Things based networks
Autor(es):	Benzarti, S. and Triki, B. and Korbaa, O.
Fonte de Publicação:	International Conference on Engineering and MIS
Ano da Publicação:	2018
Resumo:	Nowadays, the study of the security of IoT has caught many attentions of researchers. Improving our world to be a better environment building a city of dreams which is called smart city is a trend field of research. In this context, objects will be connected to the Internet interacting with each other making the world more smarter. The variety of networks building makes the IoT vulnerable. Smart home, smart grid, Smart transport, WSN, UASN, UWASN, etc make our lives more easier by offering intelligent services that save time and effort. However, each network is exposed to some attacks that can disturb its performance. In this paper, we present a classification of attacks from various networks involved in IoT. This classification distinguish common and specific attacks from each network and use some criteria like the security attributes, congestion, disturbance. Also, some existing security solutions are presented in details in order to expose the security requirements to protect IoT.
B) Dados derivados do objetivo:	
Vulnerabilidades	COMMON ATTACKS IN IoT NETWORKS: Jamming: In physical layer, jamming is considered as the primary DOS attack [10]. It has the ability to disturb the communication of an appliance or a network by a powerful jamming source like diffusing radio signals [3]. Sinkhole attack: The attacker becomes attractive by offering optimal paths to reach the base station with powerful connections which pushes the transmitting nodes to change their routing tables to route data by the malicious node. Tampering : It is important to mention that an adversary can tamper with the device and use it to insert impostor to the system, use the device maliciously or out of its intended functionality [3] Denial of Service attack : It refers to the property of being inaccessible when requested by an authorized user.

	especifics smart home attacks: Malicious Code Injection: As indicated by his name, this attack injects a malicious code through the debugging interface of the device. ACK Attack: The wireless channel can be eavesdropped in order to send a fake ACK[3]. Phishing/Pharming: In this case, a malicious entity attempts to guide the user of the device to another server or for marketing purposes or to try to deceive to steal personal information Specific attacks in smart grid: Access through database links: As we know, the activities of a system are saved in databases. Whereas, if these databases are configured improperly, an attacker can access to them and may control the network system[5].

A) Dados da publicação:	
Título:	Analysing the resilience of the internet of things against physical and proximity attacks
Autor(es):	Xu, H. and Sgandurra, D. and Mayes, K. and Li, P. and Wang, R.
Fonte de Publicação:	Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)
Ano da Publicação:	2017
Resumo:	The Internet of Things (IoT) technology is being widely integrated in many areas like smart-homes, smart-cities, healthcare, and critical infrastructures. As shown by some recent incidents, like the Mirai and BrickerBot botnets, security is a key issue for current and future IoT systems. In this paper, we examine the security of different categories of IoT devices to understand their resilience under different security conditions for attackers. In particular, we analyse IoT robustness against attacks performed under two threat models, namely (i) physical access of the attacker, (ii) close proximity of the attacker (i.e., RFID and WiFi ranges). We discuss the results of the tests we performed on different categories of IoT devices, namely IP cameras, OFo bike locks, RFID-based smart-locks, and smart-home WiFi routers. The results show that most of IoT devices do not address basic vulnerabilities, which can be exploitable under different threat models.
B) Dados derivados do objetivo:	

Vulnerabilidades	Physical Attack. In this threat model, an attacker can physically interact with the IoT device without notification to Alice. For example, the attacker can access the hardware, and read and modify the default IoT device's settings, which may impact the privacy and authentication credentials of Alice. [...] , the user that will scan this QR Code with their mobiles phones will be redirected to a fake website that may request downloading a trojanized app that is similar to OFo app.[...] d when the user scans the code she will download a fake app update, which gives an attacker remote access to it.

A) Dados da publicação:	
Título:	Flying through the secure fog: A complete study on UAV-Fog in heterogeneous networks
Autor(es):	Gupta, A. and Gupta, S.K.
Fonte de Publicação:	International Journal of Communication Systems
Ano da Publicação:	2022
Resumo:	A drone or unmanned aerial vehicles (UAVs) is becoming a trending area for researchers worldwide. UAV's contribution is increasing in day-to-day life, whether it is in a military zone, disaster management, healthcare sector, smart cities, Internet of Things (IoT), urban air mobility, and many more. In contrast, UAV's limited computational capability and low-energy sources pose significant challenges for real-time data processing, storage, networking, and security that are critical in emergencies such as floods, earthquakes, and cyclones. UAVs are rapidly used to satisfy user requirements as well as services. As the demand for UAVs aided heterogeneous wireless networks increases in critical emergencies, fog computing serves several benefits to fulfill users' demands in terms of low latency, support, data storage, mobility, availability, scalability, and so on. This study aims to present a comprehensive study with their technical aspects for understanding fog computing, security issues, privacy concerns, and risks, along with its solutions. This paper suggests the collaboration of UAV-Fog architecture based on the four-tier network consisting of smart things, local UAVs, UAV-Fog, and cloud server, to control UAV's data and also described some of the security issues faced by this cloud infrastructure. Further, this research article also sheds new light on some scenarios of UAV-Fog for such deployments, applications, opportunities, challenges, and their major security threats and their countermeasures. Afterward, we design taxonomy of the collaboration of UAV-Fog with their respective approaches.

B) Dados derivados do objetivo:	
Vulnerabilidades	Authentication has become one of the security problems that are most concerned in this network since large services are delivered on a wide scale.[...] Cyber-attacks: Cryptography algorithms for smart devices to tackle device tampering Man-in-the-middle attack: It is a type of attack in which an attacker intervenes in an ongoing conversation or data transmission. After placing themselves in the “middle” of the conversation or transmission, the perpetrators pose as both legal parties. DoS and DDoS attack: DoS attacks are performed by flooding the target system with traffic requests or sending more data that causes the UAV's network to crash. The DDoS deals with more devices sending traffic requests to crash the whole system. Jamming: When RF noise is actively induced to disrupt aerial and ground services or restrict devices in a network from communicating with each other, this is known as jamming. The jamming attacks will degrade the quality of services. Phishing: It is a type of cyber-attack in which the attacker sends a fraud message to ground users in order to gain the credentials and sensitive information of the network users

A) Dados da publicação:	
Título:	Internet of Things (IoT) Security Challenges and Solutions: A Systematic Literature Review
Autor(es):	Ali, R.F. and Muneer, A. and Dominic, P.D.D. and Taib, S.M. and Ghaleb, E.A.A.
Fonte de Publicação:	Communications in Computer and Information Science
Ano da Publicação:	2021
Resumo:	The Internet of Things (IoT), often known as the Internet of Everything, is a new technological paradigm visualized as a worldwide network of interconnected machines. IoT brings another dimension into Information Technology (IT), where machines can communicate with various machines and humans. Researchers and IT industry produced various IoT devices, architectures. Different ways are introduced to implement and use IoT concepts. IoT is getting more intention in ideas like smart homes and smart cities, raising security concerns. This article aims to gather the reported

	security issues, the classification of those issues, and the solutions that were provided against those IoT security issues.
B) Dados derivados do objetivo:	
Vulnerabilidades	Every object in the IoT platform needs to be identified by the system and other objects. Every object needs to be authenticated before interacting with the system or other objects in the IoT platform [12][13]. Ensuring the data is available to authorized persons or objects is a critical task. Management of data is also vital to protect and manage that data so that the authorized objects will get their data [14]. A key management system needs to be enabled for ensuring confidentiality. They also gave the reason for these attacks; the devices either had unpatched vulnerabilities or used default passwords. The solution to these malware's is mainly related to energy consumption patterns and OpCode.[...] IoT, as we know, has small storage and processing power, so DNS security models cannot be implemented. It poses threats like DNS Cache Poisoning and Man-In-The-Middle attacks [18, 19]. Denial of Service (DOS), Denial of Sleep (also called sleep deprivation) attacks is flooding-type attacks where the device is flooded with requests until it stops responding and consumes all its energy (battery) to respond to these flooding requests. It is sometimes called an exhaustion attack as well.[...] IoT systems are vulnerable to many vulnerabilities, including encryption, decryption mechanisms, intruding into the network, and flooding requests. Whenever an attack happens, it exploits the vulnerabilities found in the system because every attack targets some specific vulnerabilities and then exploits them. The Authors proposed a fog-based distributed attack detection mechanism for IoT. [...]

A) Dados da publicação:	
Título:	On the security of the 5G-IoT architecture
Autor(es):	Rahimi, H. and Zibaeenejad, A. and Rajabzadeh, P. and Safavi, A.A.
Fonte de Publicação:	International Conference Proceeding Series
Ano da Publicação:	2018

Resumo:	In this paper, we study the security aspects of the new 5G-IoT architecture, which is recently developed by this research team. We classify potential security attacks at each layer of the 5G-IoT architecture. As the main contribution of this work, we propose a security taxonomy for the 5G-IoT architecture in the context of smart city applications. This taxonomy consists of five layers to confront the studied attacks and to protect the privacy of clients. The number of layers is selected according to the types of attacks where each attack type affects a particular layer of the 5G-IoT architecture.
B) Dados derivados do objetivo:	
Vulnerabilidades	Physical Device Layer: Unauthorized Access to the Tags. The lack of effective authentication techniques for RFID systems allows attackers to easily access tags. In WSNs, if an attacker has access to the network, he can easily use the whole network. Tag Cloning. Cloning RFID tags is an effective attack in the physical layer. By this attack, the important information could be captured by reverse engineering or directly from its deployment environment. RF Jamming. In this attack, RF signals are sent to the network to disturb communication between the tags and readers. Attackers could employ RF jamming to prevent readers from communicating with all tags by interfering with all the signals within its range. Communication Layer: DoS Attack. A Denial of Service (DoS) network attacker engages the victim with flooding of requests by making a large mass of network traffic. Sybil Attack. A node in the system shows multiple pseudonymous identities to a victim node. This action is able to deceive the victim node to perform an action multiple time. Eavesdropping. Eavesdropping includes a blocking of data flow between two connected devices. In the IoT systems, it occurs on the network layer to takes the form of information sniffing. During data communication, we use privacy as a technique to provide security with efficient access control corresponding eavesdropping. Application Layer: Code Injection. In this attack, attackers for a variety of purposes such as stealing data, getting system control, and propagating worms inject malicious codes into the system to exploit program errors. Buffer Overflow. In this threat, attackers use program vulnerabilities to involve the violation of the bounds of code

	or data buffer. In fact, attackers put a long series of data to a specified area, to make the system overflow. Phishing Attack. In this threat, attackers act like a real user or authorized institution to receive sensitive information from users such as passwords and credit card details. Perception Layer Access Control. IoT devices largely preserve the information in the RFID tags cannot be caught at insistence, instead to block privacy leak users. In addition, it consists of label failure, processor certainty, analysis of antenna energy, etc. Data Encryption. Data security of RFID system necessitates encryption of the RFID signal, using the appropriate algorithm. According to [13], a nonlinear key algorithm based on the displacement calculation realizes RFID system data encryption Physical Security Design. This contains both node and antenna design. The node design means hardware composition design and security processor selection, processor link, radio frequency circuit design, data acquiring unit design; whereas antenna design has to have high communication range, high flexibility, stability, etc

A) Dados da publicação:	
Título:	IoT Powered Agricultural Cyber-Physical System: Security Issue Assessment
Autor(es):	Kariri, E.
Fonte de Publicação:	IETE Journal of Research
Ano da Publicação:	2022
Resumo:	Smart farming or development in agriculture Cyber-Physical Systems has led to the development of various IOT based innovative platforms to aid automated systems for precision agriculture. There are smart devices (IoT devices, smart vehicles, UAVs, ROVs, and drones) and sensors (magnetic, electrochemical, and mechanical sensors)constantly connected at the edge and procure data that is uploaded to cloud-based interfaces for further processing. The sensors can be maneuvered using an insecure, intelligent farming system to create choreographed cybersecurity attacks on a particular farm. End-to-end system is achieved by putting together smart devices, communication media, uploading data to the cloud, intermediate nodes, and processing this data at a central unit like the cloud or intermediate processing at other nodes. Cyber-physical systems are a combination of many technologies, resulting in a large number of security

	threats. This chapter is to delineate the attack vectors and categories of threats that can be performed on these innovative IOT based agricultural products; if not appropriately secured, can lead to more strategized and sophisticated security attacks that can hinder production for a region under effect and thus bringing down the economy and food stocks of Nations who implemented smart agriculture.
B) Dados derivados do objetivo:	
Vulnerabilidades	Node Tampering/Jamming: Equipment such as actuators, sensors are generally embedded in nature, having a single task to perform. Therefore, these nodes cannot have more security forefront. Attacks like node tampering, jamming are more prevalent. Interferences/Insider Attacks: The perception layer in IoT is more susceptible to insider attacks wherein eavesdropping; interferences can be introduced by injecting an external agent in disguise. Physical Damage: Physical damage to equipment can be natural as a result of calamity or otherwise. It can lead to null values at receiving end or missed values, which can cause an imbalance in the real-time processing of data. Unauthorized Access: To provide for crops through smart IOT based agriculture deployments, it is highly important to properly monitor conditions in real-time. Denial of Service: According to [5], in precision agricultural systems, the denial of service is more frequent towards users using smart services; the threats can be due to poorly managed systems, disruption to PNT(positioning, navigation, and timing) systems that use GPS to collect information for processing. Encryption: Encryption of contents is extremely important when the data is transmitted or stored; the practice helps to secure the parameter to a vast extent Social Engineering: A naive user is often the most insecure point in the complete network; Phishing is another social engineering attack strategy that is generally used to lure the users into clicking on synonymous links to gain access;

A) Dados da publicação:	
Título:	Future Directions of Cybersecurity in Industrial Internet of Things Through Edge Computing
Autor(es):	T. Zhukabayeva, L. Zholshiyeva and N. Karabayev
Fonte de Publicação:	9th International Conference on Computer Science and Engineering (UBMK)

Ano da Publicação:	2024
Resumo:	As Industrial Internet of Things (IIoT) technologies and edge computing continue to evolve, the volume of data processed in real-time to optimize manufacturing processes has increased. However, this increase in connected devices also amplifies the risks associated with cyber threats. This paper examines the use of edge computing in cyber-physical systems (CPSs) to ensure security in IIoT environments. The focus is on analyzing existing security issues by comparing research related to vulnerability protection in industrial networks and proposing solutions to enhance data protection. The study includes a comparative analysis of traditional IoT and IIoT systems, as well as a proposed taxonomy of solutions with future strategies aimed at improving security within industrial networks.
B) Dados derivados do objetivo:	
Vulnerabilidades	- In wireless communication, data exchange in IIoT interactions is vulnerable to numerous security and privacy issues, especially in IIoT group communication environments with many devices. - Security challenges in edge computing, such as unauthorized access and breaches of confidentiality, remain inadequately addressed in urban architecture and require furthe r research. - The implementation of IIoT faces several key challenges. Heterogeneity is a significant issue, as the variety of devices and protocols complicates compatibility and integration. - Additionally, IIoT devices often have limited resources, such as constrained power and memory, which restrict their functionality.

A) Dados da publicação:	
Título:	Radon transform based malware classification in cyber-physical system using deep learning
Autor(es):	Rasim Alguliyev, Ramiz Aliguliyev, Lyudmila Sukhostat
Fonte de Publicação:	Results in Control and Optimization
Ano da Publicação:	2024
Resumo:	The development of cyber-physical systems entails the growth and diversity of malware, which increases the scale of cybersecurity threats. Attackers use malicious software to compromise various components of cyber-physical systems. Existing technologies make it possible to reduce the risk of malware infection using vulnerability and intrusion scanners,

	network analyzers, and other tools. However, there is no perfect protection against the increasingly sophisticated types of malware. The goal of this research is to solve this problem by combining different visual representations of malware and detection models based on transfer learning. This method considers two pre-trained deep neural network models (AlexNet and MobileNet) that are capable of differentiating various malware families using grayscale images. Radon transform is applied to the resulting grayscale malware images to improve the classification accuracy of the new malware binaries. The proposed model is evaluated using three datasets (Microsoft Malware Classification, IoT_Malware and MalNet-Image datasets). The results show the superiority of the proposed model based on transfer learning over other methods in terms of the efficiency of classifying malware families aimed at infecting cyber-physical systems.
B) Dados derivados do objetivo:	
Vulnerabilidades	- CPSs consist of a large number of connected devices (e.g., sensors, smart meters, etc.) that are targeted by many malware families, such as Tsunami, Bashlite, and Mirai [7]. They take advantage of weak authentication, outdated firmware, and scanners designed to find open ports and compromise system devices - The weakest link in the CPS security chain is the human factor. Cybercriminals use this factor to gain unauthorized access, steal personal data, and infect systems with malware

A) Dados da publicação:	
Título:	Vulnerability Detection in Cyber-Physical System Using Machine Learning
Autor(es):	Bharathi V, Vinoth Kumar C N S
Fonte de Publicação:	Scalable Computing: Practice and Experience
Ano da Publicação:	2024
Resumo:	The cyber-physical system is a specific type of IoT communication environment that deals with communication through innovative healthcare (medical) devices. The traditional medical system has been partially replaced by this application, improving healthcare through efficiency, accessibility, and personalization. The intelligent healthcare industry utilizes wireless medical sensors to gather patient health information and send it to a distant server for diagnosis or treatment. The healthcare industry must increase electronic device accuracy, reliability, and productivity. Artificial intelligence (AI) has been applied in various industries, but

	cybersecurity for cyber-physical systems (CPS) is still a recent topic. This work presents a method for intelligent threat recognition based on machine learning (ML) that enables run-time risk assessment for better situational awareness in CPS security monitoring. Several machine learning techniques, including Nave Bayes (65.4\%), Support Vector Machine (64.1%), Decision Tree (89.6%), Random Forest (92.5%), and Ensemble crossover (EC) XG boost classifier (99.64), were used to classify the malicious activities on real-world testbeds. The outcomes demonstrate that the Ensemble crossover XG boost enabled the best classification accuracy. When used in industrial reference applications, the model creates a safe environment where the patient is only made aware of risks when categorization optimism exceeds a specific limit, minimizing security managers' pressure and efficiently assisting their choices.
B) Dados derivados do objetivo:	
Vulnerabilidades	- Cyberattacks can compromise the accuracy and reliability of patient data, making it difficult for healthcare providers to make informed decisions - The availability of sensitive health data can be exploited, leading to unauthorized access and potential data breaches - Cyber threats can directly affect the integrity of medical devices, which may lead to malfunction or incorrect operation, posing risks to patient safety - Vulnerabilities in environmental monitoring systems (like temperature and humidity controls in ICUs) can affect the conditions necessary for patient care

A) Dados da publicação:	
Título:	Preamble-based RF-DNA Fingerprinting Under Varying Temperatures
Autor(es):	Cinque S. Peggs; Tanner S. Jackson; Ashley N. Tittlebaugh; Taylor G. Olp; Joshua H. Tyler; Donald R. Reising
Fonte de Publicação:	12th Mediterranean Conference on Embedded Computing (MECO)
Ano da Publicação:	2023
Resumo:	A total of 30.9 billion Internet of Things (loT) deployments are expected by 2025 with most employing weak or no encryption at all, which raises concerns about loT security. This concern is exacerbated by loT-connected critical infrastructure and the successful exploitation of this security vulnerability. This led researchers to propose a physical layer-based loT security solution coined Specific Emitter

	Identification (SEI). However, SEI has been shown to be sensitive to temperature changes. This sensitivity is important when considering loT deployments in highly variable temperature environments. The presented approach shows the temperature sensitivity of SEI is mitigated when the classifier is trained using RF-DNA fingerprints drawn from waveforms collected at two temperatures. In fact, SEI performance improves the most when the two temperatures are at or near the extremes of the operating temperature range. Specifically, our work shows that training SEI classifiers using the extremes of the collected temperatures improves overall classification performance across temperature ranges. The work in this paper also shows that emitters operating in a sub-ambient, exothermic state have a more consistent fingerprint than those operating in a high-temperature, endothermic state.
B) Dados derivados do objetivo:	
Vulnerabilidades	- A total of 30.9 billion Internet of Things (loT) deployments are expected by 2025 with most employing weak or no encryption at all, which raises concerns about loT security. This concern is exacerbated by loT-connected critical infrastructure and the successful exploitation of this security vulnerability. - In light of this information, loT security remains a pressing concern because most loT devices employ weak or no encryption at all due to (i) onboard resource limitations such as power and memory, (ii) prohibitive manufacturing costs, and (iii) encryption implementation and management challenges.

A) Dados da publicação:	
Título:	Blockchain Integration with Machine Learning for Securing Fog Computing Vulnerability in Smart City Sustainability
Autor(es):	L. A. Ajao and S. T. Apeh
Fonte de Publicação:	1st International Conference on Advanced Innovations in Smart Cities (ICAISC)
Ano da Publicação:	2023
Resumo:	The advent of a smart city-based industrial Internet of Things (IIoT) is confidently built on the combined protocols of a virtual IPv6 addressing scheme and the fifth generation (5G) mobile network. For better network service and to achieve Quality of Experience (QoE) in the architecture. But this intelligent city architecture is vulnerable to several cyber-attack and malicious actors at the different layers which make it exposed to the same attacks as in the conventional IPv4

	wireless sensor networks. However, this work aims to develop a blockchain-based machine learning (BML) security framework that secures the fog computing layer vulnerability in the smart city's sustainability. The machine learning approach is firstly implemented between the edge layer and fog server nodes of the city architecture for the variants of intrusion detection using different ML algorithms for the attack's discovery and classification. While the augmented blockchain technology is implemented between the fog layer and cloud computing to enhance the privacy and confidentiality of packet traffic broadcast to the public. The results obtained from ML-IDS show high-performance detection accuracy and low processing time. While the blockchain framework is also evaluated based on the certmcate generation, and retrieval size in bytes and time in milliseconds.
B) Dados derivados do objetivo:	
Vulnerabilidades	- This research proposed an enhanced security framework for the fog computing layer's vulnerability to attacks in intelligent city architecture. Using augmentation of a blockchain-based machine learning algorithm for intrusion detection system (BML-IDS) as illustrated in "Fig. 2". These techniques help to secure the big data transmitted from the edge computing layer through the fog server nodes to the cloud computing without information tampering or alteration. - The transmission of collected big data traffic from the edge computing layer through the fog server node is secured using Machine Learning (ML) algorithms. This ML algorithm helps to detect infiltration of abnormal activity that intends to eavesdrop on the packet traffic in the city's network. By classifying the city's traffic into normal and abnormal through the features extraction processes of a collected packet captured (PCAP).

Apêndice B - Descrição das Vulnerabilidades

Link para o catálogo: https://github.com/Clintonhud/Vulnerabilidades/wiki

DISPOSITIVO

Nome	Descrição
Canal de Voz	Associados à segurança e à privacidade quando os dispositivos IoT incorporam capacidades de voz, como assistentes pessoais ativados por voz, sistemas de controle de casa inteligente ou dispositivos de comunicação por voz. Em casas inteligentes, essas informações podem agora ser facilmente captadas ao explorar dispositivos IoT mal protegidos com sistemas de microfone integrados, como serviços de assistente pessoal (por exemplo, Google Home, Amazon Echo), brinquedos infantis e outros eletrodomésticos controlados por voz. Esses sistemas são vulneráveis a ataques como voz intrusa e mascaramento de voz.
Configuração Padrão	Muitas vezes, as configurações padrão atribuídas pelos fabricantes de dispositivos beneficiam a empresa em vez de seus usuários. Os fabricantes frequentemente adicionam ou habilitam recursos que não são essenciais para a operação do dispositivo, o que ajuda os atacantes a lançar seus ataques. Essas configurações devem ser verificadas e alteradas imediatamente após a compra e configuração do dispositivo. As configurações de login padrão dos dispositivos IoT podem ser usadas pelos atacantes para acessar o dispositivo ilicitamente ou para redefinir a senha.
Falsificação de Dispositivo	A falsificação (*spoofing*) de dispositivo refere-se a uma técnica na qual um atacante disfarça seu dispositivo para parecer como um dispositivo legítimo ou confiável em uma rede ou sistema. O objetivo é enganar administradores de rede, sistemas de segurança ou outros dispositivos para conceder acesso ou privilégios não autorizados ao atacante. O atacante geralmente manipula ou falsifica informações de identificação, como endereços MAC, endereços IP ou identificadores de dispositivo, para mascarar seu dispositivo como outro dispositivo confiável.
Vazamento de Emanações Eletromagnéticas	Emanação Eletromagnética resultante do processamento de informações dentro de dispositivos. A coleta de informações é baseada na observação dos campos eletromagnéticos dos dispositivos IoT. Aqui, um exemplo seria as emanações eletromagnéticas vazando de linhas de energia não filtradas.

	Existem demonstrações da viabilidade de medir a atividade da linha de energia de uma casa com tanta precisão que poderiam identificar o que os ocupantes estavam assistindo na televisão.
Restrições de Energia	Os dispositivos inteligentes, como sensores IoT, em um ambiente de big data baseado em IoT na nuvem podem falhar devido a problemas de energia. Dispositivos IoT são limitados em sua capacidade de consumo de energia, o que pode afetar negativamente seu desempenho, funcionalidade ou disponibilidade.
Interação Heterogênea	A vulnerabilidade baseada na heterogeneidade de dispositivos IoT conectados e em interação refere-se à exploração de falhas de segurança que surgem devido à diversidade de dispositivos IoT presentes em um ambiente conectado. Essa heterogeneidade abrange diferenças em termos de hardware, software, protocolos de comunicação e configurações entre os dispositivos IoT.
Transferência e Armazenamento Inseguros de Dados	Refere-se à exposição indevida ou ao comprometimento das informações durante a transmissão ou armazenamento. Os dados gerados no hardware quando modificados podem causar uma diferença absoluta nos dados, que são posteriormente enviados para camadas superiores para processamento. Essa abertura ocorre porque os dispositivos IoT, que são responsáveis por coletar e transferir dados, são vulneráveis a várias formas de ataque. Por exemplo, a injeção de dados falsos no sensor são formas de ataques nos sistemas IoT, que podem direcionar as decisões do sistema automatizado a se comportar da maneira desejada pelo atacante.
Firmware Inseguro	Falhas de segurança presentes no firmware dos dispositivos, que podem ser exploradas por adversários para comprometer a integridade, confidencialidade ou disponibilidade do dispositivo ou das informações que ele manipula. O firmware é o software de baixo nível que controla o funcionamento dos dispositivos IoT. Devido à natureza heterogênea desses dispositivos, o firmware não é atualizado frequentemente, o que causa uma variedade de ameaças de segurança.
Inicialização Insegura	Falhas de segurança no processo de inicialização do dispositivo, que podem ser exploradas por adversários para comprometer a integridade, autenticidade ou confidencialidade do sistema durante o processo de inicialização e configuração dos dispositivos. Esta fase crítica é quando o dispositivo é ligado e os componentes básicos de software e hardware são inicializados para preparar o

	dispositivo para operação.
Senha Insegura	Uma vulnerabilidade de segurança ocorre quando as senhas são fracas, fáceis de adivinhar, padrão, compartilhadas ou armazenadas incorretamente. Senhas são um mecanismo padrão para autenticação e proteção em sistemas e aplicativos de computador. No entanto, quando escolhidas ou gerenciadas inadequadamente, podem permitir acesso não autorizado a contas, dispositivos ou informações sensíveis.
Interface Física Insegura	Falhas de segurança relacionadas à interação física com o dispositivo, seja por meio de portas físicas de conexão, interfaces de usuário ou outros pontos de acesso físico. Essas vulnerabilidades podem permitir que adversários tenham acesso não autorizado ao dispositivo, manipulem sua funcionalidade ou comprometam sua segurança.
Testes Insuficientes	A maioria dos dispositivos IoT é produzida rapidamente para atender às crescentes demandas do mercado e, portanto, não passa por testes adequados ou segue quaisquer padrões de segurança aceitáveis ou estruturas de avaliação. Esses dispositivos podem não ter sido testados tão robustamente quanto os sistemas operacionais de desktop/servidor.
Falta de Proteção de Canais Laterais	Um ataque de canal lateral refere-se a ataques que resultam na revelação de informações úteis sobre os dados transmitidos ou o funcionamento interno do sistema por meio de caminhos alternativos. Esses canais laterais podem ser explorados por adversários para obter informações confidenciais que podem ser obtidas através de canais como, análise de padrões de consumo de energia, emissões eletromagnéticas, tempo de resposta, entre outros, mesmo sem acesso direto aos dados transmitidos pela rede.
Falta de Autenticação Forte	Um protocolo de autenticação deve ser desenvolvido para confirmar a confiança mútua entre diferentes objetos, usuários ou sistemas, verificando suas identidades. Isso impede que um atacante acesse o dispositivo sem fornecer as credenciais corretas, burlando os mecanismos de autenticação e ganhando controle sobre o dispositivo.
Baixo Poder Computacional	Dispositivos IoT geralmente têm recursos limitados, o que significa que eles teriam que depender de sistemas operacionais e protocolos de rede menos robustos e, portanto, podem ser mais fáceis de comprometer. Por outro lado, eles coletam informações sensíveis, o que agravaria o risco. A capacidade de processamento limitada faz com que os métodos de segurança tradicionais sofram vários

	contratempos e muitas vezes não detectem as ameaças físicas na rede.
Baixo Alcance de Transmissão de Dados	Dispositivos com baixo alcance de transmissão de dados são suscetíveis a ataques porque exigem proximidade com outros dispositivos para trocar dados. Isso significa que um atacante pode facilmente se infiltrar na área de alcance desses dispositivos para realizar ataques de proximidade.
Injeção de Código Malicioso	O atacante injeta código malicioso em um dispositivo físico comprometido, o que pode ajudá-lo a lançar outros ataques também. O atacante compromete um nó injetando fisicamente nele um código malicioso que lhe daria acesso ao sistema IoT. Um dos objetivos dessas injeções é instalar uma versão comprometida do software/firmware durante as atualizações sem fio do dispositivo IoT, o que poderia dar ao adversário controle remoto total sobre o dispositivo comprometido.
Obtenção de Acesso ao Console	Ao conectar-se a uma interface serial, é possível obter acesso completo ao console de um dispositivo. O atacante pode acessar o hardware e ler/modificar as configurações padrão do dispositivo IoT, o que pode afetar a privacidade e as credenciais de autenticação com a modificação intencional da configuração do circuito do sistema.
Dano Físico	O dano físico ao equipamento pode ser natural, como resultado de uma calamidade ou mesmo resultante de um ataque físico direto de alguém. Isso pode levar a valores nulos no destino ou valores perdidos, o que pode causar um desequilíbrio no processamento em tempo real dos dados.
Violação Física	Refere-se ao ato de modificar fisicamente um dispositivo (por exemplo, RFID) ou um link de comunicação. É importante mencionar que um adversário pode adulterar o dispositivo e usá-lo para inserir um impostor no sistema, usar o dispositivo maliciosamente ou fora de sua funcionalidade pretendida. Esse tipo de ataque é lançado quando o atacante está muito mais próximo do dispositivo de rede e é forçado a quebrar o hardware sem permissão.
Privação do Sono	Muitos dispositivos IoT usam baterias como fontes de energia, portanto, eles apenas detectam e transmitem periodicamente e entram em um estado de suspensão entre eles. Esse ataque tem como objetivo de alguma forma impedir que os dispositivos entrem em modo de suspensão ou minimizar o período de suspensão, esgotando assim a bateria muito mais rapidamente do que em um uso normal.
Sistemas de Baixo	Há em muitos dispositivos IoT os riscos de segurança

Custo	associados à produção e implementação com ênfase excessiva na redução de custos, muitas vezes às custas da segurança. Esses dispositivos podem apresentar várias fraquezas que os tornam mais suscetíveis a ataques cibernéticos.
Clonagem de Etiqueta	Atividade maliciosa na qual um atacante duplica ou replica a etiqueta de identificação única de um dispositivo IoT para enganar ou comprometer o sistema. Etiquetas são componentes usados em tecnologias como RFID (Identificação por Radiofrequência) para identificar e rastrear dispositivos ou objetos. A clonagem de etiquetas na camada física envolve a obtenção das informações de identificação únicas de uma etiqueta legítima e reproduzindo-as em uma etiqueta falsificada.
Acesso Físico Não Protegido	Refere-se à captura física de um dispositivo IoT. Essa ameaça pode ser séria se os dispositivos IoT precisarem ser implantados em áreas sem proteção de segurança física.
Controle de Acesso Fraco	Falha de segurança que permite que usuários não autorizados ou mal-intencionados obtenham acesso não autorizado aos recursos, funcionalidades ou dados do dispositivo IoT. Esta vulnerabilidade pode resultar de uma implementação inadequada de políticas de controle de acesso, autenticação fraca ou ausência de mecanismos de autorização robustos.
Fraca/Falta de Criptografia nos Dispositivos	A fraqueza ou falta de criptografia em dispositivos IoT refere-se a uma vulnerabilidade em que os mecanismos de criptografia em vigor para proteger os dados em trânsito ou em repouso dentro dos dispositivos são insuficientes ou completamente ausentes.

REDE

Nome	Descrição
Arquitetura Centralizada	Desing de arquitetura que concentra o controle e a tomada de decisões em um único ponto central. Isso significa que todas as informações dos dispositivos IoT são enviadas para esse ponto central, onde são processadas e as ações são tomadas. Os dispositivos conectados à IoT transmitem solicitações de processamento e informações de dados de seus sensores diretamente de volta ao centro de dados, onde o processamento de informações e o armazenamento são realizados por servidores executando aplicativos específicos por meio de switches.

Interferência de Canal	Suscetibilidade dos dispositivos IoT a interferências eletromagnéticas ou de sinais em seus canais de comunicação. Essas interferências podem ocorrer de várias formas e podem comprometer a integridade e a confiabilidade das comunicações entre os dispositivos IoT. Ataques de *Jamming* são ataques de disponibilidade contra o meio sem fio ou os sensores voltados para o exterior, onde um dispositivo de interferência pode ser usado para bloquear os sensores do dispositivo de receber sinais.
Sobrecarga de Comunicação	Situação em que a quantidade de pacotes de dados transmitidos entre os dispositivos IoT e os sistemas de processamento ou armazenamento excede a capacidade da rede ou dos servidores, resultando em degradação do desempenho, latência aumentada ou até mesmo indisponibilidade do sistema.
Configurar a Rede Repetidamente	A vulnerabilidade de segurança que surge quando as configurações de rede são frequentemente aplicadas ou modificadas, potencialmente deixando a rede exposta a acessos não autorizados, configurações incorretas ou outros riscos de segurança.
Vazamento ou Violação de Dados	Refere-se ao vazamento ou violação de dados em redes IoT por meio de brechas de segurança que permitem acesso não autorizado, divulgação ou perda de dados confidenciais transmitidos ou armazenados em redes IoT.
Escuta Clandestina	Interceptação e monitoramento de comunicações entre dispositivos IoT e sistemas de gerenciamento, sem o conhecimento ou consentimento dos usuários legítimos. Isso pode ocorrer em vários pontos da comunicação entre dispositivos, incluindo principalmente a transmissões de dados sem fio. Como os dispositivos IoT transmitem informações sem fio, é mais fácil interceptar os sinais transmitidos, mesmo que os dispositivos IoT estejam protegidos com segurança física.
Nó Falso/Malicioso	O atacante insere um nó falso entre dois nós legítimos da rede para controlar o fluxo de dados entre eles. Um nó malicioso poderia estar conectado ao sistema IoT para coletar e trocar dados de outros dispositivos.
Comunicação Heterogênea	Refere-se à troca de dados e informações entre dispositivos e sistemas que utilizam diferentes protocolos de comunicação, padrões ou tecnologias dentro da rede.
Servidor Inseguro	Refere-se a um servidor ou infraestrutura de *backend* que é vulnerável a ameaças de segurança e carece de salvaguardas

	adequadas para proteger os dados e dispositivos conectados à rede. Em redes IoT, os servidores desempenham um papel crítico no processamento de dados, armazenamento e comunicação entre dispositivos e aplicativos.
Controle de Tráfego Inseguro	Falhas de segurança que permitem a interceptação, manipulação ou comprometimento do tráfego de dados entre dispositivos IoT e outros elementos da rede, como gateways, servidores, serviços em nuvem ou falhas no próprio firewall de segurança de rede.
Mecanismos de Atualização Inseguros	Falhas em atualizações de firmware, software ou outras partes dos dispositivos IoT e da infraestrutura de rede. Esses mecanismos de atualização são cruciais para corrigir falhas de segurança, adicionar novos recursos e garantir o desempenho adequado dos dispositivos. Os recursos conectados ao IoT têm ainda uma demanda maior por atualizações, e a frequência das mensagens causa latência, o que resulta em vulnerabilidades de rede.
Falta de Mecanismos de Autenticação Adequados	Ausência ou inadequação de mecanismos que verificam a identidade e as permissões de entidades, como dispositivos, usuários ou serviços, que tentam acessar ou interagir com a rede. A autenticação é um mecanismo de segurança fundamental que garante que apenas entidades autorizadas tenham acesso à rede e aos seus recursos.
Falta de Senha Forte	A ausência ou uso inadequado de senhas robustas e seguras para fins de autenticação e controle de acesso dentro da rede. As senhas servem como um meio primário de verificar a identidade de usuários, dispositivos ou serviços que tentam acessar a rede IoT ou seus recursos.
Falta de Protocolos de Comunicação Seguros	Falta ou uso inadequado de protocolos que garantam a confidencialidade, integridade e autenticidade dos dados transmitidos entre dispositivos IoT, serviços e sistemas de back-end. Se os protocolos de comunicação seguros não estiverem em vigor, isso introduz riscos significativos de segurança.
Propriedades Físicas do Sistema de Energia	Refere-se a vulnerabilidades de segurança que surgem da infraestrutura física e características do sistema de fornecimento de energia elétrica usado para suportar dispositivos e redes IoT. Os sistemas de energia são essenciais para fornecer a energia elétrica necessária para operar os dispositivos e garantir sua funcionalidade contínua.
Falsificação de Sinal	Um atacante se passa ou falsifica um sinal para enganar dispositivos, serviços ou redes IoT a aceitar comandos não

	autorizados ou fornecer informações sensíveis. O *spoofing* de sinais envolve a manipulação ou imitação dos sinais transmitidos entre dispositivos ou serviços para obter acesso não autorizado ou manipular a rede.
Acesso Não Autorizado	O controle de acesso é necessário para evitar que entidades não autorizadas tenham acesso aos recursos do sistema e para garantir que entidades autorizadas só possam acessar os recursos aos quais têm permissão. Portanto, políticas de controle de acesso confiáveis desempenham um papel importante na prevenção de atividades que levam a uma violação de segurança no IoT.
Rede Insegura	Manter os dispositivos IoT em uma rede privada separada também elimina a possibilidade de um atacante infectar outros dispositivos e espalhar o malware na rede quando o dispositivo está conectado a redes Wi-Fi públicas não seguras.
Portas Não Utilizadas Habilitadas	Portas de rede desnecessárias ou não utilizadas em dispositivos IoT ou infraestrutura de rede são deixadas habilitadas, potencialmente fornecendo pontos de acesso não autorizados para atacantes. Portas não utilizadas são aquelas que não são ativamente utilizadas para os fins previstos na rede IoT.
Fraca/Falta de Criptografia na Comunicação	Refere-se a uma vulnerabilidade de segurança que surge quando os dados transmitidos entre os dispositivos e a rede não são adequadamente protegidos com mecanismos de criptografia forte.
Desautenticação de Wi-i	A desautenticação de Wi-Fi não é de forma alguma nova, mas no contexto da casa inteligente, a perda de Wi-Fi significa perda de conectividade com a Internet na residência, na qual as plataformas IoT estão cada vez mais dependentes para funcionar. Quando um atacante desautentica ou desconecta maliciosamente dispositivos IoT de suas redes Wi-Fi, isso pode levar a interrupções de serviço, perda de conectividade ou acesso não autorizado aos dispositivos ou à rede. Os ataques de desautenticação de Wi-Fi exploram o protocolo de comunicação usado pelas redes Wi-Fi para forçar dispositivos a se desconectarem de sua rede atual.

APLICAÇÃO

Nome	Descrição
Bloqueio de Conta	Permitir que sejam enviadas tentativas de autenticação após 3 - 5 tentativas de login mesmo após sequencias de tentativas fracassadas.
Quebra de Autenticação	O processo de confirmar a identidade ou veracidade de um objeto é conhecido como autenticação. Com muitos dispositivos IoT em ambientes inteligentes carentes de mecanismos de autenticação forte ou controle de acesso, torna-se fácil para os atacantes se passarem por um usuário legítimo e usarem as credenciais ou qualquer outra informação que lhes dê acesso para explorar e descobrir falhas de segurança em aplicativos da web.
Estouro de Buffer	O estouro de buffer ocorre quando um programa ou processo tenta escrever mais dados em um bloco de memória de comprimento fixo, ou buffer, do que o buffer foi projetado para conter.
Inconsistência de Dados	Em IoT, ataques à integridade dos dados coletados, processados e armazenados sujeitam os sistemas de gerenciamento associados aos dispositivos a erros ou discrepâncias, resultando em informações imprecisas, incompletas ou contraditórias.
Gerenciamento de Acesso Inseguro	O controle de acesso é necessário para impedir que entidades não autorizadas obtenham acesso aos recursos do sistema e para garantir que entidades autorizadas só possam acessar os recursos aos quais têm permissão. Portanto, políticas de controle de acesso confiáveis desempenham um papel importante na prevenção de atividades que levam a violações de segurança no IoT.
Componentes inseguros de terceiros	Associados ao uso de software, bibliotecas, dispositivos ou serviços fornecidos por terceiros que contenham falhas de segurança ou vulnerabilidades conhecidas. Isso pode acontecer quando os fabricantes de dispositivos IoT utilizam componentes de terceiros em seus produtos sem avaliar adequadamente a segurança desses componentes ou sem manter esses componentes atualizados com as correções de segurança mais recentes.
Configuração de Interface Insegura	As interfaces da web são comumente usadas para interagir com dispositivos IoT, permitindo que os usuários acessem e controlem seus recursos e configurações por meio de um

	navegador. No entanto, se essas interfaces não forem adequadamente seguras, podem representar um risco significativo à segurança. A falta de segurança em uma interface da web IoT pode levar a várias vulnerabilidades, incluindo senhas fracas ou padrões previsíveis, problemas de criptografia, falhas de autenticação, software desatualizado e falta de controle de acesso.
Gestão Insegura de Dados	Falta de gestão e proteção adequada dos dados coletados, processados e armazenados por sistemas e dispositivos IoT. Isso pode incluir uma série de questões relacionadas à maneira como os dados são tratados ao longo de seu ciclo de vida, desde a coleta até o armazenamento e o compartilhamento. A depender dos mecanismos de segurança utilizados, as informações pessoais podem ser facilmente vazadas, resultando em violações de segurança.
Software Inseguro	A atualização de software é um processo que nunca deve falhar ou ser comprometido em um sistema baseado em IoT. Deve-se prestar atenção aos processos de atualização inseguros que correm o risco de instalar software malicioso ou não autorizado, com atualizações corrompidas que podem comprometer dispositivos IoT. Deve-se evitar o uso de componentes inseguros ou desatualizados, como software de código aberto ou de terceiros. No entanto, atualizar manualmente patches para cada dispositivo IoT pode não ser viável.
Falta de Monitoramento Ativo de Dispositivos	Ausência de um sistema robusto para monitorar continuamente o status, o comportamento e as atividades dos dispositivos IoT na rede. Monitorar dispositivos IoT pode ser desafiador. Isso ocorre porque a maioria das ferramentas e práticas de monitoramento existentes, especialmente aquelas com foco em nuvem, tradicionalmente foram projetadas para monitorar dados métricos de séries temporais sem foco nos dispositivos IoT modernos ou seus processos. A falta de ferramentas de monitoramento ativo de dispositivos IoT dificulta alcançar uma visibilidade completa da rede em ambientes inteligentes baseados em IoT.
Código de Baixa Qualidade	O nível de código de baixa qualidade em aplicações de ambiente IoT refere-se à presença de práticas de desenvolvimento de software que resultam em código-fonte mal estruturado com possíveis problemas de segurança e confiabilidade, devido ao uso inadequado de recursos que resultam em falhas de segurança, como falta de validação de entrada, manipulação inadequada de senhas ou criptografia

	fraca, o que pode facilitar ataques.
Código Malicioso no Aplicativo	Código malicioso em aplicações de sistemas IoT refere-se a programas de software ou trechos de código que foram desenvolvidos com intenções maliciosas e são projetados para comprometer a segurança, privacidade ou funcionamento adequado de dispositivos IoT e sistemas relacionados.
Não Repúdio	Em um contexto geral de segurança da informação, a não repudiação garante que o remetente da informação seja fornecido com uma prova de entrega, e o destinatário seja fornecido com uma prova da identidade do remetente, para que nenhum dos dois possa negar posteriormente ter processado a informação.
Superfície de Ataque Excessivamente Grande	Cada conexão que pode ser feita com um sistema oferece um novo conjunto de oportunidades para um atacante descobrir e explorar vulnerabilidades. Quanto mais serviços um dispositivo oferece, mais serviços ele pode atacar. Sistemas de software IoT frequentemente envolvem uma complexa interação entre dispositivos, servidores, serviços em nuvem e outros componentes. Quanto mais complexo for o software, maior será a superfície de ataque, devido à maior chance de introdução de vulnerabilidades.
Injeção em Banco de Dados	Este é um dos pontos de vulnerabilidade mais conhecidos para servidores que aceitam consultas e atualizações de banco de dados, onde comandos adicionais podem ser injetados para roubar informações ou alterar/excluir registros. Muitos invasores usam instruções SQL para realizar operações de gravação, exclusão e leitura quando a aplicação web está sendo comprometida por injeção de SQL.
Enumeração de Nomes de Usuário	Capacidade de coletar um conjunto de nomes de usuário válidos interagindo com o mecanismo de autenticação através de tentativas repetidas de login ou consultas de API. Esta vulnerabilidade pode ser explorada por meio de técnicas de força bruta ou por meio de métodos mais sofisticados, como análise de mensagens de erro ou comportamento do sistema.
Fraca/Falta de Criptografia na Aplicação	Criptografia fraca ou ausente em aplicativos de sistemas IoT refere-se à falta de implementação adequada de algoritmos de criptografia ou ao uso de algoritmos de criptografia considerados fracos e facilmente quebráveis. A criptografia é uma medida essencial para proteger a confidencialidade,

	integridade e autenticidade dos dados transmitidos e armazenados em sistemas IoT.

PEOPLEWARE

Nome	Descrição
Acesso a Links Maliciosos	Os usuários podem clicar ou interagir com links projetados para enganar ou explorá-los. Links maliciosos podem ser entregues por vários canais, incluindo e-mail, redes sociais, plataformas de mensagens ou sites comprometidos.
Identificação do Fornecedor do Produto	Identificação e exposição de informações sobre o fabricante ou fornecedor dos dispositivos IoT, que podem ser exploradas por adversários para fins maliciosos.
Conhecimento do Sistema	Para a vulnerabilidade do conhecimento do sistema, temos dois pontos de referência: a perspectiva do atacante, pois eles estão cientes dos pontos fracos do sistema e empregam malware ou técnicas apropriadas para intrusão, e a perspectiva do usuário, considerando a crescente inovação das tecnologias IoT, onde muitos usuários ainda precisam entender como os dispositivos IoT modernos são projetados e funcionam para se protegerem melhor.
Falta de Suporte Técnico	A ausência ou disponibilidade insuficiente de recursos, expertise e assistência para lidar com problemas técnicos ou fornecer orientação para dispositivos e redes IoT. Quando há falta de suporte técnico, os usuários de sistemas IoT podem encontrar dificuldades na configuração, solução de problemas ou manutenção de seus dispositivos e redes.
Circunstâncias Pessoais e Sociais	As falhas de segurança que surgem devido a fatores pessoais e sociais relacionados aos usuários, como comportamentos inadequados, falta de conscientização ou treinamento, negligência ou uso indevido de dispositivos IoT.
Phishing	*Phishing* é usado para enganar as pessoas a fornecerem suas informações pessoais ou baixar software malicioso capaz de espalhar malware. Uma entidade maliciosa tenta guiar o usuário do dispositivo para outro servidor com fins de marketing ou para tentar enganar e roubar informações pessoais.
Engenharia Social	O atacante manipula os usuários de um sistema para extrair

	informações privadas. Isso torna fácil para os atacantes usar a engenharia social para enganar os usuários de dispositivos IoT a fornecer dados ou informações sensíveis que podem ser usados para acessar as redes de ambientes inteligentes.
Aquisição de Dispositivo Não Confiável	Usuários ou organizações adquirem e integram dispositivos IoT em suas redes sem garantir a confiabilidade ou segurança desses dispositivos.
Postura de Segurança do Fornecedor	Quando vulnerabilidades de segurança são descobertas, a resposta do fornecedor determina significativamente o impacto. O fornecedor tem um papel em receber informações sobre vulnerabilidades potenciais, desenvolver medidas de mitigação e atualizar dispositivos em campo.