UNIVERSIDADE FEDERAL DO CEARÁ

CAMPUS DE ITAPAJÉ

CURSO DE GRADUAÇÃO EM SEGURANÇA DA INFORMAÇÃO

VITOR MANUEL GOMES VASCONCELOS

EXPLORANDO ABORDAGENS DE SEGURANÇA PARA DETECÇÃO DE INTRUSÃO UTILIZANDO APRENDIZADO DE MÁQUINA EM INTERNET DAS COISAS

ITAPAJÉ

2026

VITOR MANUEL GOMES VASCONCELOS

EXPLORANDO ABORDAGENS DE SEGURANÇA PARA DETECÇÃO DE INTRUSÃO UTILIZANDO APRENDIZADO DE MÁQUINA EM INTERNET DAS COISAS

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Segurança da Informação do da Universidade Federal do Ceará
Campus de Itapajé, como requisito parcial à obtenção do grau de técnico em Segurança da Informação.

Orientador: Prof. Dr. Artur de Oliveira da R. Franco

Coorientador: Prof. Dr. Julio César S. dos Anjos

ITAPAJÉ

2026

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

G618e Gomes Vasconcelos, Vitor Manuel.
EXPLORANDO ABORDAGENS DE SEGURANÇA PARA DETECÇÃO DE INTRUSÃO UTILIZANDO APRENDIZADO DE MÁQUINA EM INTERNET DAS COISAS / Vitor Manuel Gomes Vasconcelos. – 2026.
88 f. : il. color.

Trabalho de Conclusão de Curso (graduação) – Universidade Federal do Ceará, Campus de Itapajé, Curso de Segurança da Informação, Fortaleza, 2026.
Orientação: Prof. Dr. Artur de Oliveira da Rocha Franco.
Coorientação: Prof. Dr. Julio César Santos dos Anjos.

1. Inteligência Artificial. 2. Aprendizado de Máquina. 3. Internet das Coisas. 4. Detecção de Intrusão. 5. Segurança. I. Título.

CDD 005.8

VITOR MANUEL GOMES VASCONCELOS

EXPLORANDO ABORDAGENS DE SEGURANÇA PARA DETECÇÃO DE INTRUSÃO UTILIZANDO APRENDIZADO DE MÁQUINA EM INTERNET DAS COISAS

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Segurança da Informação do da Universidade Federal do Ceará
Campus de Itapajé, como requisito parcial à obtenção do grau de técnico em Segurança da Informação.

Aprovada em: 14 de Janeiro de 2026

BANCA EXAMINADORA

Prof. Dr. Artur de Oliveira da R. Franco (Orientador)
Universidade Federal do Ceará (UFC)

Prof. Dr. Julio César S. dos Anjos (Coorientador)
Universidade Federal do Ceará (UFC)

Prof. Dr. Windson Viana de Carvalho
Universidade Federal do Ceará (UFC)

Prof. Dr. Juan Sebastian Toquica Arenas
Universidade Federal do Ceará (UFC)

Primeiramente a Deus, a meu Pai, a minha Mãe, a minha família, pelo carinho e os incentivos para sempre progredir. Ao meus amigos pelo apoio e por acreditarem a todo momento nas minhas capacidades.

AGRADECIMENTOS

Ao Prof. Dr. Artur de Oliveira da Rocha Franco, por aceitar o papel de orientador e me acompanhar nessa longa jornada da graduação, enfrentando alguns desafios, aprendizados e muitas coquistas. Agradeço pela compreensão, paciência e o ímpeto de sempre buscar trazer o conhecimento e os conselhos necessários para meu desenvolvimento acadêmico. Reitero a agradecer a companhia até aqui e que me acompanhe para muitas futuras pesquisas.

Ao Prof. Dr. Julio César Santos dos Anjos, por me coorientar, me guiar e repassar diversos conhecimentos e ensinamentos durante essa trajetória da conclusão do curso, em principal o desenvolvimento da objetividade e como um pesquisador deve se portar diante um novo desafio.

Aos funcionários da Universidade Federal do Ceará, pela disponibilidade e comprometimento em realizar um trabalho de excelência ao longo dessa jornada, sendo extremamente solícitos e compreensivos durante este período da graduação.

Agradeço a todos os professores, em especial aos professores Dr. João Henrique Gonçalves Medeiros Corrêa e Dr. Tarek Sayjari, pela inspiração para o tema do trabalho e por me proporcionar o conhecimento não apenas racional, mas a manifestação do caráter e afetividade da educação no processo de formação profissional, por tanto que se dedicaram a mim, não somente por terem me ensinado, mas por terem me feito aprender.

Aos meus amigos, José Eric, Emanuel Ávila, Antônio Lucas, Nelson Felipe e João Batista, expresso minha sincera gratidão pela valiosa companhia, incentivo e diálogos enriquecedores ao longo desta jornada. A colaboração de vocês foi essencial para o desenvolvimento deste trabalho, pois suas opiniões e perspectivas diversificadas não apenas ampliaram minhas visões, mas também trouxeram novos caminhos a serem explorados. Que novas futuras colaborações surjam e que possamos juntos trabalhar em conjunto.

Aos meus pais e irmãos, expresso minha profunda gratidão pelo apoio incondicional e pela fé constante em minhas capacidades. Cada palavra de encorajamento e cada gesto de amor foram fundamentais na minha jornada. Agradeço por sempre acreditarem em mim, ajudando-me a enfrentar desafios e a perseverar em busca dos meus sonhos. Sem o seu suporte, muitas conquistas nesta trajetória não seriam possíveis. Que eu possa honrar esse apoio e continuar a avançar na realização dos meus objetivos e estudos.

"Grandes ideias podem vir de qualquer pessoa, em qualquer lugar. Trata-se de criar um ambiente onde essas ideias possam florescer."

(Jensen Huang)

RESUMO

O trabalho visa analisar a utilização de métodos apresentados no estado da arte que envolvem a utilização de Aprendizado de Máquina (ML) na defesa contra ataques de Intrusão em Redes de Internet das Coisas (IoT). O trabalho busca compreender como pesquisas nas quais se discutiam métodos de defesa contra ataques de intrusão, selecionando aquelas que se focavam na utilização de *ML* como modo de proteção, além dos principais ataques e suas motivações focados em adentrar redes *IoT*. Com os artigos obtidos, foi observado como as aplicações de defesa com técnicas de *ML* são utilizadas, realizados quatro métodos de Mineração de dados: análise da quantidade de termos específicos, método *Apriori*, para análise de frequência de itens; o método de clusterização, para a análise de grupos com características semelhantes; e a análise de Séries Temporais, para observar o comportamento dos artigos ao longo do período analisado, ao longo do tempo estabelecido da análise da pesquisa. Desta maneira, foi possível conceber três questionamentos relacionados a pesquisa, que indagaram sobre os desafios encontrados neste tema e como eles poderão ser resolvidos, através da *ML* em defesa da Intrusão em Redes de *IoT*.

Palavras-chave: inteligência artificial; aprendizado de máquina; internet das coisas; detecção de intrusão; segurança, survey.

ABSTRACT

The present work aims to analyze the use of state-of-the-art methods that involve Machine Learning (ML) techniques for defending against intrusion attacks in Internet of Things (IoT) networks. The study seeks to understand how research addressing defense mechanisms against intrusion attacks has evolved, selecting studies that focus on the use of ML as a protection approach, as well as identifying the main types of attacks and their motivations aimed at compromising IoT networks. Based on the selected articles, it was observed how defense applications employing ML techniques are applied, through the use of four data mining methods: analysis of the frequency of specific terms; the *Apriori* method for item frequency analysis; the clustering method for identifying groups with similar characteristics; and time series analysis to observe the behavior of the analyzed articles over the defined research period. In this way, it was possible to formulate three research questions addressing the challenges identified in this domain and how they may be mitigated through the use of ML in defending against intrusion attacks in IoT networks.

Keywords: artificial intelligence; machine learning; internet of things; intrusion detection; security; survey.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

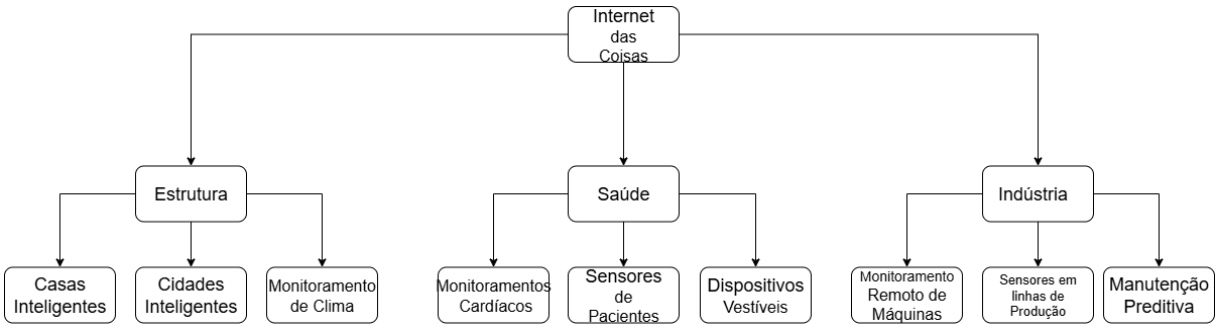
AI	*Artificial Intelligence*
ANN	*Artificial Neural Network*
CNN	*Convulutional Neural Networks*
DAE	*Denoising Autoencoder*
DDoS	*Distributed Denial of Service*
DL	*Deep Learning*
DNN	*Deep Neural Network*
DoS	*Denial of Service*
DT	*Decision Tree*
FL	*Federated Learning*
IDS	*Intrusion Detection System*
IIoT	*Intelligent Internet of Things*
IoT	*Internet of Things*
KNN	*K-Nearest Neighbors*
LLMs	*Large Language Models*
LSTM	*Long Short-Term Memory*
MIT	*Massachusetts Institute of Technology*
ML	*Machine Learning*
MLP	*Multilayer Perceptron*
NLP	*Natural Language Processing*
RF	*Random Forest*
RNN	*Recurrent Neural Network*
RQ	*Research Question*
SSA	*Salp Swarm Algorithm*
SVM	*Support Vector Machine*
XGBoost	*Extreme Gradient Boosting*

SUMÁRIO

1 INTRODUÇÃO

Desde sua conceituação por `Kevin Asthon`, pesquisador britânico do *Massachusetts Institute of Technology* (MIT), em 1999, a *Internet of Things* (IoT) tem impulsionado transformações tecnológicas significativas, possibilitando uma conectividade abrangente entre dispositivos e redes Tripathy e Anuradha (2017). Com aplicações que vão desde casas inteligentes até sistemas críticos em centros urbanos, a IoT emergiu como um alicerce para a sociedade moderna declarou Mohanty *et al.* (2021) e como exemplificado na Figura 1. Como reportado pela empresa multinacional americana de tecnologia Intel[1] que especulou que o valor de mercado da IoT poderia atingir 6,2 trilhões de dólares até 2025, e uma grande porcentagem disso está relacionada ao investimento na manufatura e na saúde Yalli *et al.* (2024).

Figura 1 – Esquema de Estrutura da Internet das Coisas.



Fonte: Elaborado pelo autor (2026).

No entanto, essa ampla adoção trouxe consigo desafios complexos de segurança, tornando a IoT um alvo atraente para atacantes que buscam explorar vulnerabilidades para obter dados sensíveis ou comprometer sistemas inteiros. Isso gera uma insegurança para os usuários recentes deste recurso de telecomunicação. Em 2022, foi estimado que mais de 50 bilhões de dispositivos estavam conectados à internet, e alguns deles foram invadidos por agentes mal-intencionados. Somente em 2016, houve aproximadamente 1 bilhão de violações de dados em todo o mundo, segundo a *Privacy Rights Clearinghouse* (PRC) Shafiq *et al.* (2022). Estima-se que o número de dispositivos IoT conectados cresça para 1 trilhão até 2025. De acordo com essa previsão, a IoT oferecerá uma receita econômica potencial de US$ 11 trilhões por ano até 2025 Manyika *et al.* (2015).

O cenário de segurança na IoT é agravado pela heterogeneidade dos dispositivos conectados e pela falta de padronização nas implementações. A arquitetura tradicional da camada

[1] <https://www.intel.com>

IoT consiste em três camadas: A camada de percepção, a camada de rede e a camada de aplicação. Essas três camadas são exploradas individualmente por agentes maliciosos, que buscam suas fraquezas para realizarem ataques diretos Alotaibi (2023). Ataques como *Denial of Service (DoS)*, injeção de *malwares* e exploração de credenciais fracas são comuns, colocando em risco tanto a privacidade dos usuários quanto a integridade das redes Shafiq *et al.* (2022).

Ambientes de aplicações de IoT, como a área da saúde, *Smart homes*, *smart cities* e a indústria, em específico a indústria 4.0, que depende diretamente da aplicação da IoT, para que o maquinário presente nas indústrias funcione adequadamente, podem sofrer grandes danos pela distribuição elevada de ataques de intrusão.

Nessa circunstância, o uso de *Intrusion Detection System* (IDS) é uma solução promissora para proteger as redes IoT contra múltiplos ataques, surgindo como uma ferramenta poderosa que auxilia uma rede com diversos dispositivos conectados Houda *et al.* (2022). Mas, ao mesmo tempo, ela não consegue segurar ataques que foquem em formas de aplicar força bruta; por isso, um reforço seria necessário para complementar sua defesa.

Nesse contexto, a *Machine Learning* (ML) surge como uma solução promissora, oferecendo abordagens proativas para a Detecção de Intrusões. Ao analisar padrões de tráfego em tempo real e identificar anomalias, algoritmos de ML podem atuar na prevenção e mitigação de ataques antes que causem danos significativos Rehman *et al.* (2022). Os IDS baseados em ML consistem em aprender a assinatura de cada ataque IoT, a fim de serem previstos/detectados de forma eficiente e oportuna pelo sistema. Uma vez que um ataque é detectado, medidas de precaução devem ser tomadas pela equipe (por exemplo, especialistas em segurança cibernética ou equipe executiva) para lidar com tal ataque Houda *et al.* (2022).

A utilização de algoritmos como *Random Forest* (RF), *Support Vector Machine* (SVM) e *Deep Neural Network* (DNN) tem mostrado resultados expressivos na identificação de tráfegos maliciosos em redes IoT Khan *et al.* (2022). Esses métodos não apenas aumentam a precisão na detecção de intrusões, como também adaptam-se continuamente a novos padrões de ataque. Por exemplo, ao analisar tráfego anômalo em dispositivos domésticos inteligentes, essas técnicas conseguem distinguir atividades legítimas de tentativas de comprometimento Khan *et al.* (2022).

Embora os avanços sejam promissores, ainda há barreiras a serem superadas. A limitação de recursos computacionais em dispositivos IoT, como sensores e atuadores, representa um desafio para a implementação de algoritmos de ML robustos Ravikumar *et al.* (2022).

Além disso, questões relacionadas à privacidade e à regulamentação da coleta de dados para treinamento de modelos precisam ser resolvidas para garantir um equilíbrio entre proteção e conformidade legal Abbas *et al.* (2022). Estudos contínuos são necessários para aprimorar as técnicas existentes, integrando-as a sistemas de segurança mais leves e eficientes, capazes de proteger uma tecnologia tão impactante para o futuro da sociedade conectada.

1.1 Objetivos

Como contextualizado anteriormente, os objetivos gerais deste trabalho tem como base o estudo do estado da arte atual, em como é abordado a segurança de redes IoT ao utilizarem de métodos de IDS com o complemento de ML. O trabalho busca compreender como as atuais pesquisas tratam sobre os métodos de defesa em ataques de intrusão, e formular uma análise exploratória, que poderá apontar demandas e soluções de segurança em IoT.

Para a definição e para alcançar os objetivos gerais, foram definidos os seguintes objetivos específicos:

a) Mapear as principais vulnerabilidades e ataques direcionados às camadas de percepção, rede e aplicação em ecossistemas de IoT;
b) Identificar os algoritmos de ML mais utilizados na literatura acadêmica para a detecção de anomalias e intrusões;
c) Analisar quantitativamente as associações entre termos técnicos, como os algoritmos, ataques e resultados por meio da aplicação do algoritmo de mineração de dados *Apriori*;
d) Categorizar os focos de pesquisa da literatura atual mediante técnicas de clusterização (*K-Means*), identificando padrões de abordagens teóricas e práticas;
e) Avaliar as tendências temporais da área, observando a evolução dos desafios e a consolidação de algoritmos específicos ao longo dos últimos anos;
f) Discutir os desafios de implementação, como a restrição de recursos computacionais, propondo diretrizes para trabalhos futuros na área.

O restante deste trabalho está organizado da seguinte maneira: na Seção 2, é apresentada a revisão da literatura; na Seção 3, são resumidos os conceitos fundamentais para o entendimento da pesquisa; na Seção 4, é descrita a metodologia utilizada nesta monografia; na Seção 5, é feita a discussão das análises realizadas; por fim, na Seção 6, é oferecida uma conclusão que resume os principais achados e sugere direções para futuras pesquisas.

2 TRABALHOS RELACIONADOS

Na seção a seguir, são abordados os trabalhos que tangenciaram a base da pesquisa e que motivaram a criação e o desenvolvimento da mesma. Os trabalhos foram selecionados com base em sua contribuição, ao abordar situações de possíveis ataques de intrusão em cenários de atuação da IoT, como a área da saúde; indústria; lazer e como os autores contornaram essas adversidades através das propostas ou implementações de alguns algoritmo de ML.

A IoT se tornou um meio de acesso à tecnologia extremamente eficiente, Gad *et al.* (2022) relata sobre a eficiência do uso da mesma, como as redes IoT estão cada vez mais vulneráveis as violações de segurança à medida que a sua popularidade aumenta. Os ataques à cibersegurança, como *Denial of Service* (DoS), *Phishing*, estão entre os mais populares e perigosos para a segurança da IoT. Muitos acadêmicos estão cada vez mais interessados em melhorar a segurança dos sistemas IoT. Dessa forma, o uso de abordagens de ML para funcionar como sistemas de IoT para fornecer melhores capacidades de segurança.

Kumar *et al.* (2023) mostra em sua pesquisa que as ameaças à segurança de rede têm aumentado, levando a ataques de rede graves, de modo que um *firewall* simples não será suficiente para impedir ataques desafiadores e complicados. Dessa forma, a utilização de IDS (IoT) com outros dispositivos de segurança é imperativa para proteger as redes. A detecção de ataques empregando um único algoritmo de IoT não é eficaz, assim, o autor fez uso *Ensemble Learning* para combinar diferentes algoritmos.

Muitos aplicativos cruciais da IoT, como saúde e defesa, a detecção precoce de ataques de segurança desempenha um papel significativo na proteção de recursos enormes. Narayan *et al.* (2023) mostra que um sistema de Detecção de Intrusão é usado para resolver este problema. As abordagens baseadas em assinatura não detectam ataques de *Zero-Day*. Assim, a detecção baseada em anomalia, particularmente ferramentas de *Artificial Intelligence* (AI), está se tornando popular.

Alshathri *et al.* (2023) determina que recentemente a IoT tem sido utilizada em várias aplicações, como a indústria transformadora, os transportes, a agricultura e as aplicações voltadas a saúde, que podem melhorar a eficiência e a produtividade mediante uma aplicação de gestão inteligente à distância. Com o aumento da utilização de aplicações *Intelligent Internet of Things* (IIoT), o risco de ciberataques brutais também aumentou. Isto leva os pesquisadores a trabalhar no desenvolvimento de sistemas de Detecção de Intrusões eficazes com a utilização de ML para a infraestrutura IoT contra quaisquer atividades maliciosas.

A proteção contra intrusões indesejadas é crucial para preservar a integridade e a segurança dos dispositivos conectados no contexto das redes da IoT. Alrayes *et al.* (2024) mostra que o crescente número de dispositivos IoT tornou vários setores mais vulneráveis a ataques cibernéticos e violações de segurança, incluindo casas inteligentes, automação industrial e saúde. Em resposta a este dilema, o autor promove a ideia de criar um novo método para Detecção de Intrusão em sistemas de IoT utilizando modelos *Denoising Autoencoder* (DAE), com a abordagem sugerida, projeta-se criar um sistema que pode identificar e interromper as tentativas de intrusão em tempo real.

A IoT está se tornando uma parte inevitável da vida de todos. Dessa forma Thomas e Bhat (2024) mostra que a IoT está sendo amplamente utilizada para reduzir o fardo dos seres humanos. Embora a IoT facilite a vida humana, também coloque vários desafios em matéria de segurança. A segurança deve ser uma prioridade em toda a cadeia de valor, desde os fabricantes de dispositivos, aos fornecedores de serviços IoT, aos retalhistas e aos consumidores. Dessa forma, os IDS podem ser utilizados para a segurança dos dados e dos dispositivos através da *Internet*. Nos últimos anos, as técnicas de ML são aplicadas na detecção de ameaças em IDS.

Shirley e Priya (2023) fala que a IoT é considerada a próxima revolução da *Internet*, uma vez que proporcionou grandes melhorias nas atividades diárias dos seres humanos, incluindo a prestação de serviços de saúde eficientes e o desenvolvimento de cidades inteligentes e sistemas de transporte inteligentes. O IDS é uma resolução proposta pelos pesquisadores para monitorar e proteger a comunicação da IoT. Neste trabalho, uma análise meticulosa da segurança das redes de IoT com base em métricas de qualidade de serviço é realizada para implantar IDS, realizando experimentos em comunicação segura e medindo o desempenho da rede com base na comparação com as métricas de segurança existentes.

Alzubi *et al.* (2024) descreve que a IoT apresenta soluções para reduzir a necessidade de intervenção humana e enfatiza a automação de tarefas. No entanto, à medida que o número de dispositivos e usuários que utilizam essa tecnologia cresce, o potencial de violações de segurança e intrusões. Por exemplo, dispositivos IoT inseguros, como eletrodomésticos inteligentes ou sensores industriais, podem ser vulneráveis a tentativas de *hackers*. Para resolver e prevenir esse problema, o autor do trabalho propõe a integração de sistemas de detecção de intrusão (IDS) com uma rede neural artificial (*Artificial Neural Network* (ANN)) e um algoritmo de enxame de *Salp Swarm Algorithm* (SSA) para melhorar a detecção e compreensão de intrusão em um ambiente IoT.

Em síntese, os trabalhos relacionados apresentados nesta seção representam a base teórica que valida a relevância deste trabalho de conclusão de curso. Eles comprovam que a integração de ML em sistemas de IDS não é apenas uma tendência tecnológica, mas uma necessidade atual para garantir a integridade das redes de IoT. Em resumo, essas abordagens desta pesquisa se posiciona como uma continuidade necessária, utilizando métodos de mineração de dados, como os citados na seção de introdução: *Apriori*, Clusterização e Tendências Temporais, para extrair um conhecimento estruturado e direcionar o desenvolvimento de soluções de segurança mais eficientes e viáveis

3 FUNDAMENTAÇÃO TEÓRICA

A crescente conectividade promovida pela IoT tem revolucionado diversos setores, mas também ampliado a superfície de ataque das redes, exigindo soluções de segurança mais inteligentes e adaptativas. Nesse contexto, os Sistemas de IDS desempenham um papel essencial na identificação de atividades maliciosas. Combinando essas soluções com algoritmos de ML, é possível aprimorar a detecção de padrões anômalos em ambientes dinâmicos e heterogêneos, como os da IoT. A presente fundamentação teórica abordará os conceitos, desafios e inter-relações entre IDS, IoT e técnicas de ML evidenciaram como essa integração contribui para a construção de redes mais seguras e resilientes.

3.1 Internet das Coisas

A IoT refere-se à interconexão de uma vasta gama de microdispositivos em grande escala, que operam em uma ou várias redes, utilizando diversos protocolos de comunicação. Essa rede de dispositivos inteligentes é capaz de coletar, compartilhar e analisar dados em tempo real, permitindo que eles se comuniquem entre si de maneira eficiente e autônoma (DIAN, 2022). Na IoT, suas classificações podem ser agrupadas em aplicação, arquitetura e alcance, considerando os protocolos e tecnologias empregadas em cada cenário, como:

a) Cenários de Aplicação:
   - ***Consumer IoT (CIoT)***: refere-se a aplicações voltadas ao consumidor final, como casas inteligentes, automação residencial, dispositivos vestíveis (*wearables*) e assistentes virtuais, visando conforto, segurança e conveniência (GUBBI *et al.*, 2013);
   - ***Industrial IoT (IIoT)***: envolve sensores, atuadores e sistemas de controle aplicados à automação industrial, manutenção preditiva, manufatura inteligente e cadeias de suprimentos conectadas, aumentando eficiência e produtividade (SISINNI *et al.*, 2018));
   - ***Healthcare IoT (IoMT – Internet of Medical Things)***: focado em saúde digital, monitoramento remoto de pacientes, dispositivos médicos conectados e gestão hospitalar inteligente, promovendo prevenção, diagnóstico e tratamento mais ágeis (AMMOUN *et al.*, 2024));
   - ***Smart Cities IoT***: inclui sistemas integrados de transporte, iluminação pública inteligente, gerenciamento de resíduos, vigilância e monitoramento ambiental para

promover sustentabilidade e eficiência urbana (ZANELLA *et al.*, 2014);

- ***Smart Farming*** (Agricultura Inteligente): aplicações voltadas à agricultura de precisão, envolvendo sensores de solo, clima e irrigação automatizada, otimizando produção e recursos naturais (WOLFERT *et al.*, 2017).

b) Cenários de Arquitetura:

- ***Cloud-based IoT***: utiliza infraestrutura em nuvem para armazenamento, processamento e análise de dados, favorecendo escalabilidade e integração global, mas podendo apresentar latência para aplicações críticas (BOTTA *et al.*, 2016);
- **Arquitetura Distribuída (*Edge/Fog Computing*)**: realiza processamento próximo à fonte de dados (*edge devices*), reduzindo latência e carga de tráfego na nuvem, adequada para aplicações em tempo real (SHI *et al.*, 2016);
- **Arquitetura Híbrida**: combina nuvem e *edge/fog computing*, aproveitando os benefícios de ambas para balancear processamento local e centralizado, melhorando eficiência e resposta do sistema (CHIANG; ZHANG, 2016).

c) Cenários de Alcance

- ***Personal Area IoT (PIoT)***: redes de curto alcance como *Bluetooth*, *ZigBee* e NFC, geralmente utilizadas em dispositivos vestíveis, automação pessoal e comunicação entre sensores próximos (MIORANDI *et al.*, 2012);
- ***Local Area IoT (LIoT)***: abrange redes locais como *Wi-Fi* e *Ethernet*, usadas em ambientes residenciais, comerciais e industriais para conectar múltiplos dispositivos em uma área restrita (ATZORI *et al.*, 2010);
- ***Wide Area IoT (WIoT)***: inclui tecnologias como *LoRaWAN* e *Sigfox*, que possibilitam comunicação de longo alcance com baixo consumo energético, aplicadas em rastreamento, agricultura inteligente e cidades inteligentes (CENTENARO *et al.*, 2016);
- ***Cellular IoT (CIoT)***: baseia-se em redes celulares como *NB-IoT* e *LTE-M*, oferecendo conectividade confiável, ampla cobertura e suporte para abundância de dispositivos com baixo consumo energético, aplicável em infraestrutura urbana e monitoramento industrial (HASSAN *et al.*, 2020).

3.2 Principais ataques a IoT

Com base na estrutura da IoT, que se forma em três pilares: aplicação, rede e percepção, se abordará nesse tópico, os principais ataques que segundo o estado da arte, são os mais utilizados por invasores, ao se aproveitarem de brechas nos três pilares da IoT (ALOTAIBI, 2023):

a) **Percepção:**
   - **Node Capture**: o atacante obtém controle físico de um nó da rede, acessando dados e credenciais sensíveis;
   - **Jamming**: o sinal de comunicação é intencionalmente interferido para interromper a transmissão de dados entre dispositivos;
   - **Sleep Deprivation**: o nó é impedido de entrar em modo de economia de energia, esgotando rapidamente sua bateria;
   - **Replay**: pacotes legítimos são interceptados e retransmitidos pelo invasor para enganar o sistema e obter acesso indevido.

b) **Rede**
   - **Selective-Forwarding**: o nó comprometido descarta seletivamente pacotes, afetando a integridade dos dados na rede;
   - **Eavesdropping**: o invasor intercepta comunicações para coletar informações confidenciais sem ser detectado;
   - **Sybil and ID Cloning**: um único nó assume múltiplas identidades falsas para manipular o funcionamento da rede;
   - **Wormhole**: dois nós maliciosos criam um túnel entre si para desviar e retransmitir pacotes, enganando o roteamento;
   - **Denial of Service (DoS)**: recursos da rede são sobrecarregados por tráfego malicioso, tornando-a indisponível para usuários legítimos;
   - **Man in the Middle**: o atacante intercepta e altera possivelmente a comunicação entre dois nós sem que eles percebam;
   - **Sinkhole**: um nó falso atrai o tráfego da rede prometendo o melhor caminho, mas pode manipulá-lo ou descartá-lo;
   - **Black hole**: um nó malicioso aceita pacotes e os descarta silenciosamente, interrompendo a comunicação da rede.

c) **Aplicação**

- **Malicious Code Injection**: o invasor insere código malicioso em sistemas para alterar seu comportamento ou obter acesso não autorizado;
- **Cross-site or Malicious Scripts**: scripts maliciosos são injetados em páginas web, afetando usuários ao interagir com o conteúdo;
- **Malware Injection**: software malicioso é inserido em sistemas ou redes com o objetivo de espionagem, sabotagem ou controle;
- **Data Distortion**: dados são intencionalmente corrompidos ou manipulados para comprometer decisões baseadas em informações falsas;
- **SQL Injection**: comandos SQL maliciosos são inseridos em entradas de dados para manipular bancos de dados e obter acesso a informações;
- **Ransomware**: arquivos e sistemas são criptografados por atacantes que exigem pagamento para restaurar o acesso;
- **Side-channel**: informações sensíveis são extraídas observando canais colaterais como tempo de execução ou consumo de energia;
- **Authorization and Authentication**: ataques visam burlar ou explorar falhas na verificação de identidade e permissões de acesso.

3.3 Sistema de Detecção de Intrusão

IDS é uma ferramenta de segurança cibernética projetada para monitorar e analisar atividades em uma rede ou em sistemas computacionais em busca de comportamentos suspeitos, ou maliciosos. O principal objetivo de um IDS é identificar tentativas de acesso não autorizado, ataques cibernéticos e outras atividades que possam comprometer a integridade, confidencialidade ou disponibilidade dos dados (MANGLIK *et al.*, 2024). Ele é capaz de detectar uma variedade de ataques, incluindo varreduras de porta, acessos não autorizados, negação de serviço, exploração de vulnerabilidades de *softwares*, tráfego malicioso ou desvio de políticas internas.

Existem dois principais mecanismos de detecção, a detecção baseada em assinatura, que identifica padrões de ataques previamente catalogados em bancos de dados, como *malwares*. E detecção baseada em anomalia, que constrói um perfil do comportamento normal da rede e sinaliza os desvios significativos como possíveis intrusões (SPADACCINO; CUOMO, 2020).

Durante sua operação, o IDS examina pacotes de dados, requisições, respostas, e comandos executados, correlacionando essas informações com suas regras e modelos de detecção. Quando o IDS identifica um padrão que corresponde a uma ameaça conhecida ou observa uma anomalia fora do comportamento esperado, ele gera um alerta para o administrador de segurança, registrando informações detalhadas do evento para análise posterior (DAVIES *et al.*, 2025). Por padrão, um IDS não toma ações diretas contra os ataques, pois é um sistema de detecção passiva, apenas notificando sobre atividades suspeitas.

Por exemplo, um IDS pode detectar um ataque de *SQL Injection*, em que comandos maliciosos são inseridos em campos de entrada de formulários *web* para manipular ou acessar dados do banco de dados de maneira não autorizada, comprometendo a integridade e confidencialidade das informações da organização.

Para realizar a defesa de possíveis invasores, se é utilizado de estratégias para realizar tal ação. Essas estratégias podem ser dividas com ou sem o uso de ML. Sem a utilização de ML, pode-se citar as principais estratégias como:

a) ***Signature-based Detection* (Detecção por Assinatura)**: detecta intrusões comparando padrões de tráfego com assinaturas conhecidas de ataques. Efetivo para ataques já catalogados, mas incapaz de detectar ataques novos (*zero-day*);
b) ***Anomaly-based Detection* (Detecção por Anomalia Clássica)**: define um perfil normal de tráfego e sinaliza desvios como possíveis intrusões. Baseia-se em estatísticas, limites pré-definidos ou regras heurísticas;
c) ***Stateful Protocol Analysis***: examina protocolos para identificar desvios de seus padrões normais de funcionamento. Útil para detectar explorações de vulnerabilidades específicas de protocolos.

Agora com a utilização de ML, pode-se citar as principais estratégias como:

a) ***Supervised Learning IDS***: usa classificadores treinados com dados rotulados (ataque/não ataque), como: *Decision Trees* (Árvores de Decisão) *Support Vector Machines* (SVM) *k-Nearest Neighbors* (k-NN);
b) ***Unsupervised Learning IDS***: utiliza algoritmos sem dados rotulados, detectando clusters anômalos, como: *K-Means, Clustering DBSCAN e Autoencoders*;
c) ***Semi-supervised Learning IDS***: treina o modelo com poucos dados rotulados e muitos não rotulados, combinando aprendizado supervisionado e não supervisionado;
d) ***Reinforcement Learning IDS***: aprende ações ótimas para detectar intrusões ao interagir

com o ambiente e receber recompensas ou penalidades;

e) ***Deep Learning-based IDS***: redes neurais profundas para detectar padrões complexos em tráfego de rede, como: *Convolutional Neural Networks (CNN) Recurrent Neural Networks (RNN/LSTM)*

3.4 Aprendizado de Máquina

ML é um ramo da inteligência artificial que se concentra no desenvolvimento de algoritmos e modelos que permitem que os computadores aprendam a partir de dados. Em vez de serem programados explicitamente para realizar uma tarefa específica, os sistemas de ML utilizam padrões e informações contidas nos dados para melhorar seu desempenho ao longo do tempo (ZHOU; LIU, 2021).

Segundo o *review* de (JANIESCH *et al.*, 2021), ML e *Deep Learning* (DL) são usados para construir modelos preditivos de forma automatizada, substituindo técnicas estatísticas manuais em tarefas com alta dimensionalidade e complexidade. Um estudo de (SUBASI *et al.*, 2023) destaca que ML moderno engloba também estratégias como *Federated Learning* (FL) e aprendizado distribuído, refletindo a escalabilidade e evolução constante da área.

A ML está presente em diversas áreas da sociedade, como a Indústria 4.0, com aplicações em controle de qualidade automatizado usando visão computacional e aprendizado supervisionado; manutenção preditiva para detectar falhas antes que ocorram; otimização de processos de produção por meio da análise de dados em tempo real (JOHANESA *et al.*, 2024). A ML tem sido empregado em análises financeiras para saúde pública, auditando gastos e prevendo custos futuros de forma automatizada, mais eficiente e transparente, especialmente em ambientes de *finite resources* e múltiplos *stakeholders* (RAMEZANI *et al.*, 2023).

Modelos de ML são usados para avaliar riscos climáticos e estressar cenários financeiros, lidando com não-linearidades e incertezas que modelos tradicionais não capturam bem (NIMMALA, 2023). Estudos recentes empregam ML para prever acidentes no ambiente de trabalho, recomendando estratégias de retorno ao trabalho e mapeando desigualdades demográficas, com uso de técnicas como *gradient boosting*, *isolated forests* e *Large Language Models* (LLMs) para dados não estruturados (VIVIAN *et al.*, 2025)

A seguir, um pequeno resumo das tecnologias derivadas da ML, apresentando o seu intuito de estudo/desenvolvimento e sua importância na aplicação com o tema pesquisado:

SVM é um algoritmo de aprendizado supervisionado que busca encontrar o hiper-

plano ótimo que melhor separa as classes em um espaço de características, utilizado principalmente em classificação de padrões e detecção de anomalias. RF é um método de aprendizado ensemble baseado em múltiplas árvores de decisão, no qual cada árvore é treinada com subconjuntos aleatórios dos dados, sendo amplamente empregado em tarefas de classificação e regressão devido à sua alta acurácia e robustez contra *overfitting*.

DNN são redes neurais profundas compostas por múltiplas camadas ocultas capazes de aprender representações hierárquicas dos dados, sendo aplicadas em reconhecimento de imagens, processamento de linguagem natural e detecção de intrusões complexas. *Decision Tree* (DT) é uma técnica de aprendizado supervisionado que constrói um modelo em formato de árvore baseado em regras de decisão simples, útil em classificação, interpretação de dados e análise de atributos relevantes. Já *Naive Bayes* é um classificador probabilístico baseado no Teorema de *Bayes* e na suposição de independência entre as variáveis, sendo utilizado em filtragem de spam, análise de sentimentos e classificação de texto pela sua eficiência em problemas com grandes volumes de dados e baixa complexidade computacional.

ANN são modelos inspirados no funcionamento do cérebro humano, compostos por camadas de neurônios artificiais interconectadas. Elas aprendem ajustando os pesos das conexões com base em dados de entrada e saída, sendo usadas em regressão, classificação e controle adaptativo (MUKHAMEDIEV *et al.*, 2022). *Multilayer Perceptron* (MLP) é um tipo de ANN *feed-forward*, com múltiplas camadas ocultas e conexões totalmente conectadas entre neurônios. O MLP é amplamente utilizado em tarefas de classificação e regressão e apresenta bom desempenho com dados numéricos tabulares e estrutura simples (WOODMAN; MANGONI, 2023).

Recurrent Neural Network (RNN) são projetadas para lidar com dados sequenciais ou de séries temporais, mantendo um estado interno (memória) que permite capturar dependências temporais. Aplicações típicas incluem *Natural Language Processing* (NLP), reconhecimento de fala e previsão de séries temporais (MUKHAMEDIEV *et al.*, 2022). *Convulutional Neural Networks* (CNN) processam entradas estruturadas espacialmente, como o uso de imagens, usando filtros convolucionais, *pooling* e camadas totalmente conectadas. São altamente eficazes em visão computacional, mas também aplicadas em NLP e séries temporais 1D devido à capacidade de extração automática de características das imagens analisadas (MUKHAMEDIEV *et al.*, 2022).

O ML supervisionado, implica em modelos que aprendem a partir de dados de entrada

e saída rotulados. É utilizado para tarefas como classificação e regressão (MUKHAMEDIEV *et al.*, 2022). O ML Não supervisionado, se aplica a um modelo que explora padrões ou estruturas ocultas em dados sem rótulos, como *clustering* e redução de dimensionalidade. Muito usado para agrupamentos e detecção de anomalias (MUKHAMEDIEV *et al.*, 2022). *K-Nearest Neighbors* (KNN) são utilizados para classificar um novo ponto, considera os k vizinhos mais próximos no espaço de características. Não exige treinamento explícito (*lazy learning*), não faz suposições sobre a distribuição dos dados e é eficaz quando há poucas dimensões e muitos dados (GUPTA *et al.*, 2022).

3.5 Apriori

O método Apriori, proposto por (AGRAWAL RAKESH; SRIKANT, 1996), é um algoritmo clássico para a descoberta de conjuntos de itens frequentes e regras de associação em bases de dados transacionais. O Apriori aborda regras de associação para a explorarão das relações entre Itens em conjuntos de dados:

a) **Support (Suporte):** a relação entre o número de vezes que um item ocorre nas transações e o número total de transações;
b) **Confidence (Confiança):** identifica a probabilidade de itens ou conjuntos de itens ocorrerem juntos nos conjuntos de itens;
c) **Lift (Levantamento):** fator que indica o quanto a probabilidade de o item A levar ao item B é maior do que a probabilidade isolada de A ocorrer. Um valor de *Lift* maior que 1 sugere uma associação positiva, enquanto um valor menor que 1 indica uma associação negativa, e um valor igual a 1, independência.

3.6 Clusterização

A clusterização é uma técnica de ML não supervisionado, geralmente utilizando *K-Means*, cujo objetivo consiste em agrupar dados com características semelhantes em subconjuntos denominados *clusters*, de forma que os elementos pertencentes a um mesmo grupo apresentem alta similaridade entre si e baixa similaridade em relação aos elementos de outros grupos. Diferentemente dos métodos supervisionados, a clusterização não depende de dados previamente rotulados, o que a torna particularmente relevante em cenários onde a obtenção de rótulos é custosa, limitada ou inviável.

Para agregar à análise de clusterização, foi aplicado o *One-Hot Encoding* que é amplamente utilizado como técnica de pré-processamento, pois transforma variáveis categóricas em vetores binários, preservando a informação sem introduzir relações ordinais artificiais entre categorias. Adicionalmente, a determinação do número de *clusters (K)* constitui um desafio fundamental em algoritmos como o *K-Means*, uma vez que a escolha inadequada desse parâmetro pode resultar em agrupamentos pouco representativos ou excessivamente fragmentados. Métodos como o *Elbow Method*, o *Silhouette Score* e a análise da variância *intra-cluster* são comumente empregados na literatura para estimar um valor ótimo de *K*, equilibrando a coesão interna dos *clusters* e a separação entre eles.

3.7 Séries Temporais

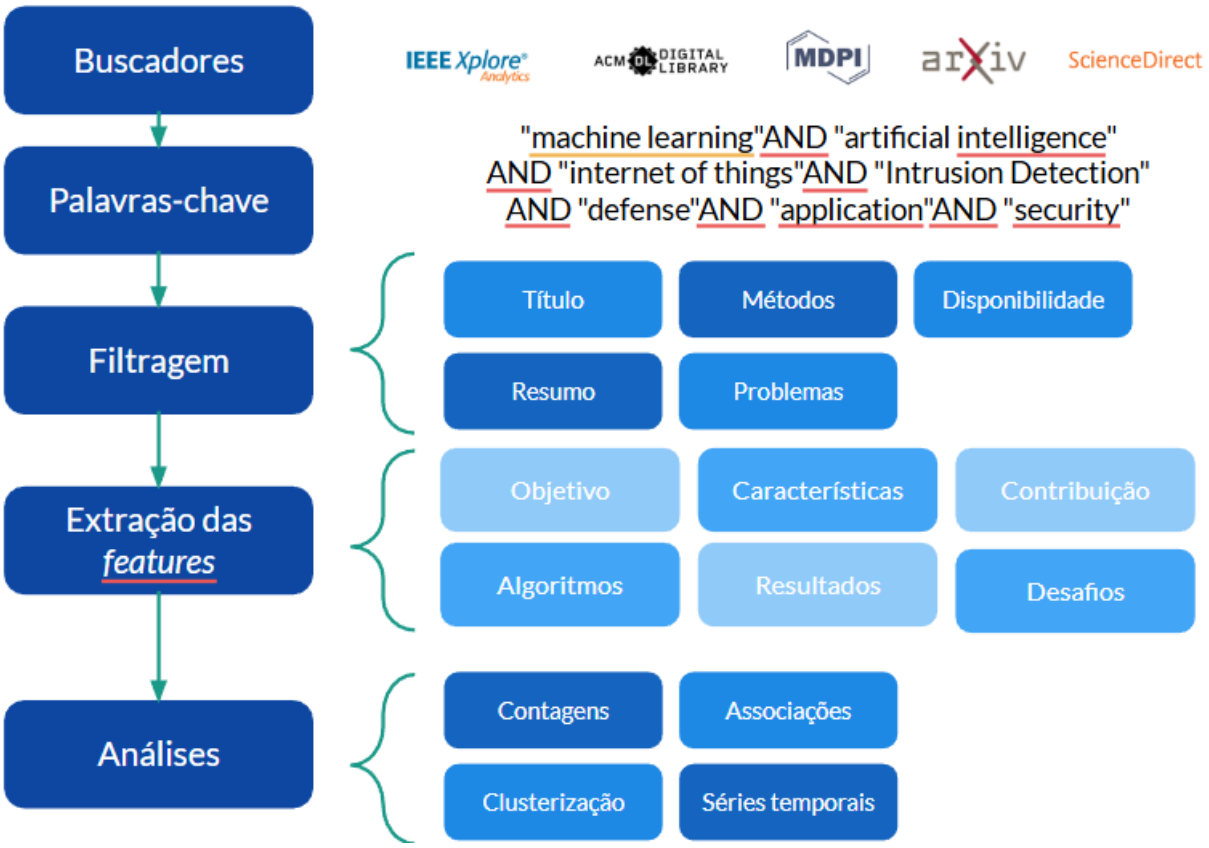
Séries Temporais referem-se à análise da evolução de padrões, abordagens e tecnologias ao longo do tempo, permitindo identificar como determinado campo de pesquisa se desenvolve em diferentes períodos (MORETTIN; TOLOI, 2018). Além da evolução dos algoritmos, as tendências temporais também evidenciam mudanças nas estratégias de validação e avaliação dos modelos. Métricas simples, como acurácia, deram lugar a indicadores mais robustos, incluindo *F1-score*, taxa de falsos positivos e curvas *ROC*.

De forma geral, a Fundamentação Teórica ao fornecer as definições de ataques e as capacidades dos algoritmos, a Seção 3 permite que o leitor compreenda a lógica por trás dos cenários abordados neste trabalho, situando sobre as definições de ML, IDS, IoT e das análises de *Apriori*, Clusterização e Tendências Temporais apresentadas posteriormente, validando a escolha do ML como a resposta técnica aos desafios de segurança da IoT.

4 METODOLOGIA

Nesta seção será abordado os métodos de ordenação utilizadas no trabalho, assim como os materiais e artifícios que também foram aplicados, para engrandecer a decorrência do trabalho. A metodologia do trabalho foi estruturada em algumas etapas, como pode ser observado no fluxograma presente na Figura 2, baseada no estudo de Franco *et al.* (2024), que delineia um processo sistemático para a investigação. O fluxograma serve como uma representação visual clara do fluxo de atividades, facilitando a compreensão das interações entre as diferentes fases do estudo e assegurando que todas as variáveis relevantes sejam consideradas na execução da metodologia.

Figura 2 – Etapas da Metodologia



Fonte: Elaborado pelo autor (2026)

Como apresentado no fluxograma, inicialmente realizou-se uma busca na literatura, englobando diversas fontes e publicações relevantes por meio de pesquisa em artigos acadêmicos que conversassem com o tema do trabalho, utilizando os buscadores e plataformas de trabalhos acadêmicos: *IEEE*, *MDPI*[1] e *ACM*, *arXiv*, *ScienceDirect* vide Tabela 1.

[1] Os trabalhos obtidos foram analisados manualmente. Mas o autor assume o risco, caso algum artigo possua resultados errôneos, já que a comunidade acadêmica considera o *MDPI* predatório.

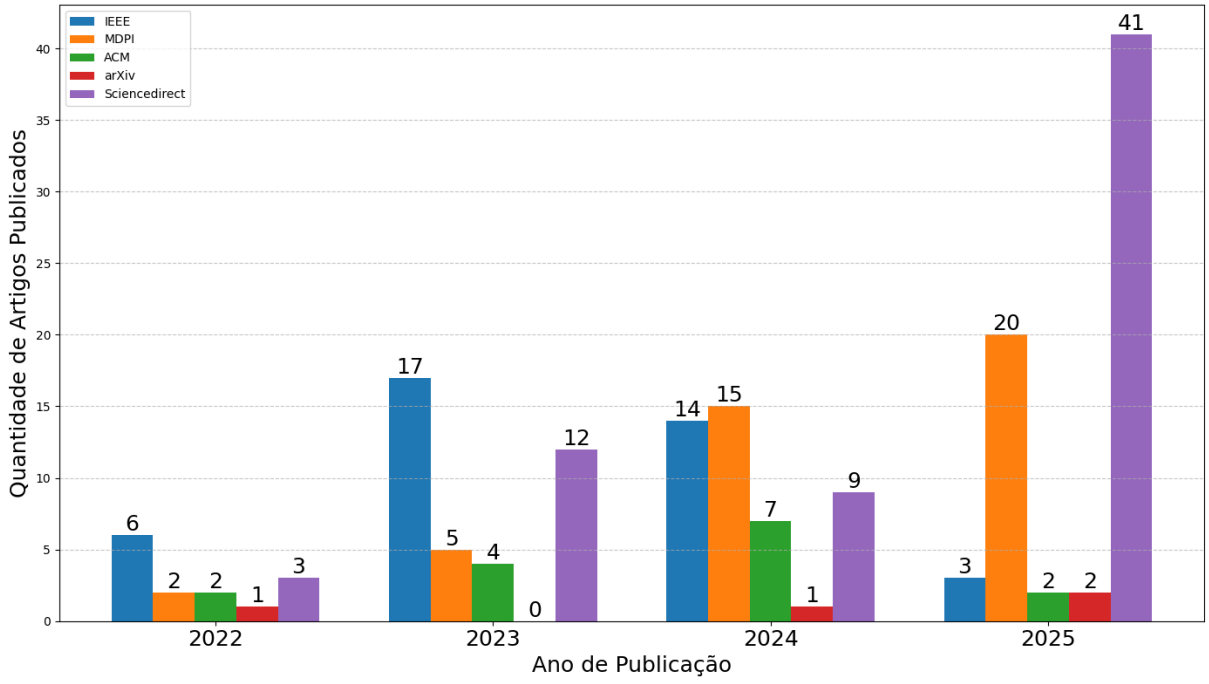
Tabela 1 – Palavras-chave para escolha dos Artigos

Consulta	Periodo	Plataforma	N° de Artigos
"machine learning"AND "artificial intelligence" AND "internet of things"AND "Intrusion Detection" AND "defense"AND "application"AND "security"	2022-2025	IEEE	41
"machine learning"AND "artificial intelligence" AND "internet of things"AND "Intrusion Detection" AND"Protection"AND "Systems"AND "defense" AND "application"AND "security"AND "Cybersecurity" AND "Cyber Defense"AND "framework"	2022-2025	MDPI	42
"machine learning"AND "artificial intelligence" AND "internet of things"AND "Intrusion Detection" AND"Protection"AND "defense"AND "application" AND "securityCyber Defense"AND "countermeasure" AND "network"AND "framework"AND "Anomaly Detection"AND "Prevention"	2022-2025	ACM	15
“machine learning” AND “internet of things” AND “intrusion detection”	2022-2025	arXiv	4
"internet of things"AND "Intrusion Detection" AND "IDS"AND "approach"AND "defense" AND "Security"AND "application"	2022-2025	Science Direct	65

Fonte: Elaborado pelo autor (2026)

As buscas focaram em conteúdos sobre cibersegurança que utilizam técnicas de ML. A seleção dos trabalhos seguiu critérios como afinidade com o tema e relevância, avaliando o período abordado e a coerência com a pesquisa, especialmente em relação a Ataques de Intrusão em Redes IoT. Com base nos trabalhos realizados, foi feita uma organização para quantificar os artigos publicados anualmente, conforme a Figura 3.

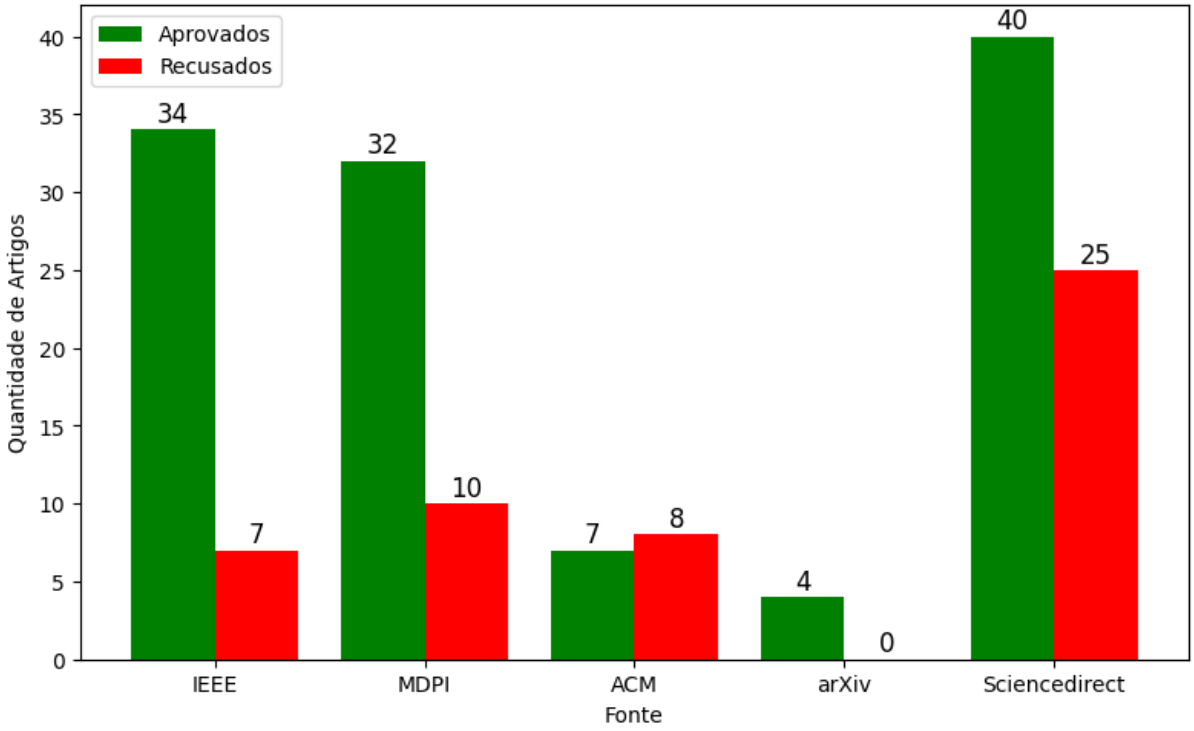
Figura 3 – Quantidade de artigos coletados por ano



Fonte: Elaborado pelo autor (2026)

Com base nos artigos coletados, foi realizada uma filtragem, conforme ilustrado na Figura 4. Este processo visou identificar aqueles artigos que apresentavam maior afinidade com o tema proposto, permitindo, assim, a obtenção de resultados mais coerentes e concisos. A seleção dos materiais foi fundamental para assegurar a relevância e a qualidade das informações, garantindo que os dados analisados estivessem alinhados com os objetivos da pesquisa.

Figura 4 – Filtragem dos artigos com base no tema



Fonte: Elaborado pelo autor (2026)

Após a obtenção dos artigos selecionados, iniciou-se a montagem de uma tabela com as informações de cada trabalho analisado e como suas pesquisas podem contribuir para o material necessário para a análise, segundo as colunas de análises de informações que podem ser observadas no Apêndice A.

As colunas referenciadas são:

a) **Objetivo**: do que se trata o artigo. O conteúdo que será explorado durante a leitura;
b) **Algoritmos**: programas ou AI que foram exploradas/utilizadas, para chegar ao objetivo do artigo;
c) **Características de IoT analisada**: as características que os autores buscaram abordar em cada trabalho, seja como foco principal ou como ponte de conteúdo;
d) **Resultados**: as consequências de todas as pesquisas realizadas e as informações geradas

no final do artigo;

e) **Contribuição**: ao final do trabalho, o que a proposta do autor auxiliou/obteve que possa ser divulgado para outros pesquisadores;

f) **Desafios**: as adversidades encontradas durante a pesquisa e como elas foram contornadas/-resolvidas.

Para a extração de informações, foi selecionada a sequência de alguns termos que se correlacionasse com os trabalhos, a fim de computar a quantidade de artigos para cada termo apresentado. Essa etapa foi baseada em estudos como Silva (2025), que busca avaliar a viabilidade de agentes de LLMs no auxílio à pesquisa científica e Franco (2025), que a aborda a geração de textos com LLMs e como esses textos conversam com o conteúdo esperado.

Dessa forma, foi introduzida as tabelas presentes no Apêndice A na LLMs *Qwen3-Max* e construído um *prompt* para gerar termos de acordo o conteúdo presente nos textos de cada colunas das tabelas, com exceção da coluna de Algoritmos.

As colunas que necessitam da obtenção dos termos, foram as colunas 3, 4, 5, 6 e 7. Colunas de Objetivos; Características de IoT analisada; Resultados; Contribuição e Desafios, respectivamente. A tabela de associação com cada artigo pode ser visualizada no Apêndice B.

Os termos para a coluna Objetivos selecionados são os seguintes:

a) **Avaliar métodos de comunicação**: este termo refere-se à análise e comparação de diferentes formas e protocolos de comunicação em sistemas, especialmente no contexto de IoT, para determinar sua eficiência, segurança e adequação a aplicações específicas;

b) **Aprimorar segurança de redes**: este termo descreve o objetivo de fortalecer as defesas de redes de computadores contra ameaças e ataques cibernéticos, através da implementação de novas tecnologias, algoritmos ou arquiteturas;

c) **Investigar abordagens de segurança**: refere-se ao estudo e exploração de diferentes estratégias e métodos para proteger sistemas e dados. Isso pode incluir a análise de abordagens tradicionais, baseadas em AI, ou outras técnicas inovadoras;

d) **Analisar técnicas de detecção**: este termo foca na avaliação de diferentes métodos e algoritmos para identificar atividades maliciosas ou anômalas em sistemas e redes, buscando entender sua precisão, eficiência e limitações;

e) **Revisar técnica de IDS**: este termo descreve a análise crítica e comparativa de IDS, que são ferramentas projetadas para monitorar e alertar sobre atividades suspeitas em uma rede ou sistema;

f) **Propor metodologia de segurança**: refere-se à criação e apresentação de um novo método ou conjunto de procedimentos para proteger sistemas contra ameaças. Geralmente, envolve uma abordagem estruturada e sistemática para a segurança;

g) **Desenvolver *framework* de segurança**: este termo descreve a construção de uma estrutura ou plataforma que serve como base para o desenvolvimento de soluções de segurança. Um *framework* geralmente inclui um conjunto de ferramentas, bibliotecas e diretrizes para facilitar a implementação de medidas de segurança;

h) **Explorar eficácia AI**: refere-se à investigação do quão bem a AI funciona na prática para resolver um problema específico, como a detecção de ameaças cibernéticas. O foco é medir o desempenho e o impacto da AI em um determinado contexto.

Os termos para a coluna Características de IoT analisada selecionados são os seguintes:

a) **Sistemas de IoT**: este termo refere-se ao conjunto de dispositivos interconectados, sensores, software e outras tecnologias que coletam e trocam dados pela internet, permitindo a automação e o controle de ambientes físicos;

b) **Conectividade e Integração**: este termo descreve a capacidade dos dispositivos de IoT de se conectarem entre si e com outras redes ou sistemas, bem como esses diferentes componentes são combinados para funcionar todo coeso;

c) **Detecção de Anomalias**: refere-se ao processo de identificar padrões ou eventos incomuns que se desviam do comportamento normal em dados de IoT, o que pode indicar falhas, ataques cibernéticos ou outras situações críticas;

d) **Comportamento de Dispositivos**: este termo foca na análise das ações, interações e padrões de uso dos dispositivos de IoT, o que é crucial para entender seu funcionamento, otimizar seu desempenho e identificar atividades suspeitas;

e) **Segurança e Dados**: Este termo abrange as medidas e estratégias implementadas para proteger os dispositivos de IoT, as redes e os dados transmitidos e armazenados contra acessos não autorizados, ataques e violações de privacidade;

f) **Comunicação de Dados**: Refere-se aos métodos e protocolos utilizados pelos dispositivos de IoT para trocar informações entre si e com a nuvem ou outros sistemas, garantindo a transmissão eficiente e confiável dos dados;

g) **Restrições de Recursos**: Este termo destaca as limitações inerentes aos dispositivos de IoT, como capacidade de processamento, memória, energia e largura de banda, que

influenciam o design e a implementação de soluções de segurança e outras funcionalidades;

h) **Tráfego de Rede**: Refere-se ao volume e tipo de dados que fluem através das redes de IoT. A análise do tráfego é fundamental para monitorar o desempenho da rede, detectar anomalias e identificar possíveis ameaças;

i) **Vulnerabilidade e Ameaças**: Este termo descreve as fraquezas em sistemas de IoT que podem ser exploradas por atacantes (vulnerabilidades) e os perigos potenciais que podem comprometer a segurança, a privacidade ou a funcionalidade desses sistemas (ameaças).

Os termos para a coluna Resultado analisada selecionados são os seguintes:

a) **Detecção eficaz**: este termo indica que o método ou sistema em questão é capaz de identificar com sucesso e de forma eficiente os eventos, padrões ou ameaças para os quais foi projetado, minimizando falhas ou omissões;

b) **Redução de custos**: Refere-se à capacidade de uma solução, técnica ou abordagem de diminuir as despesas operacionais, de manutenção ou de implementação em um determinado contexto, gerando economia financeira;

c) **Eficácia comprovada**: este termo significa que a solução ou método foi testado e demonstrou, por meio de evidências ou resultados práticos, ser capaz de atingir os objetivos propostos e produzir os efeitos desejados;

d) **Alta precisão**: indica que os resultados obtidos por um sistema, modelo ou algoritmo são muito próximos dos valores reais, ou esperados, com um baixo índice de erros ou desvios. É um indicador de confiabilidade e exatidão;

e) **Melhoria de desempenho**: este termo descreve o aprimoramento na performance de um sistema, processo ou algoritmos, que pode se manifestar em maior velocidade, eficiência, capacidade de processamento ou qualidade dos resultados.

Os termos para a coluna Contribuição analisada selecionados são os seguintes:

a) **Visão equilibrada**: este termo indica que a contribuição oferece uma perspectiva justa e imparcial sobre um tópico, considerando múltiplos pontos de vista, benefícios e riscos, sem pender excessivamente para um lado;

b) **Melhorar segurança**: refere-se a uma contribuição que visa aprimorar as medidas de proteção e defesa de sistemas, redes ou dados, tornando-os mais resilientes contra ataques e vulnerabilidades;

c) **Desenvolvimento de *framework***: este termo descreve a criação de uma estrutura ou conjunto de ferramentas e diretrizes que servem como base para o desenvolvimento de

soluções, facilitando e padronizando o processo de implementação;

d) **Taxonomia abrangente**: indica uma contribuição que organiza e classifica de forma completa e detalhada um conjunto de conceitos, ataques, técnicas ou elementos num domínio específico, proporcionando uma visão estruturada;
e) **Abordagem inovadora**: refere-se a uma contribuição que introduz uma nova maneira de pensar, um método original ou uma solução criativa para um problema, que se destaca das práticas existentes e pode abrir novos caminhos de pesquisa ou aplicação;
f) **Análise abrangente**: este termo descreve uma contribuição que realiza um exame completo e detalhado de um tópico, considerando todos os seus aspectos relevantes, dados e perspectivas, a fim de fornecer um entendimento aprofundado.

Os termos para a coluna Desafios analisada selecionados são os seguintes:

a) **Desafios de Segurança**: este termo refere-se aos obstáculos e problemas enfrentados na proteção de sistemas, redes e dados contra acessos não autorizados, ataques cibernéticos e outras ameaças. Inclui a complexidade de manter a confidencialidade, integridade e disponibilidade das informações;
b) **Ameaças Emergentes**: este termo descreve os novos tipos de ataques, vulnerabilidades ou riscos que surgem devido ao avanço tecnológico, novas técnicas de ataque ou mudanças no cenário de segurança, exigindo constante adaptação e novas estratégias defensivas;
c) **Complexidade e Dificuldade**: refere-se à natureza intrincada e desafiadora de um problema ou sistema, que pode envolver múltiplos componentes, interações complexas, grande volume de dados ou a necessidade de lidar com incertezas e variáveis difíceis de controlar;
d) **Necessidade de Melhoria**: este termo indica que há um reconhecimento de que o desempenho, a eficiência, a segurança ou a funcionalidade atual de um sistema, processo ou método não são ideais e que há espaço para aprimoramento e otimização;
e) **Limitações e Restrições**: refere-se aos fatores que impõem barreiras ou impedimentos ao desenvolvimento, implementação ou operação de uma solução. Isso pode incluir restrições de recursos, limitações tecnológicas ou desafios inerentes ao ambiente da pesquisa.

Ainda se tratando de manipulação e também mineração de dados, foi realizada a aplicação dos métodos Apriori, Clusterização e Séries Temporais como ferramentas de análises para identificar padrões e correlações significativas entre os dados coletados nos artigos, como demonstrado na aplicação no código. A aplicação destes métodos possibilita a extração de padrões frequentes entre atributos relacionados a ataques, comportamentos anômalos e métricas

de desempenho dos modelos de detecção. Assim, a análise dos resultados gerados pelo Apriori, Clusterização e Séries Temporais contribui para identificar correlações entre variáveis relevantes, como tipos de ataque, respostas do IDS e eficácia das abordagens de ML aplicadas.

Com as informações obtidas, foram montadas três *Research Question* (RQ) com base a pesquisa, como mostra a Tabela 2. Este estudo busca definir o foco da investigação, ajudando a esclarecer o que o pesquisador pretende descobrir ou entender, orientando a metodologia e a análise dos dados.

Tabela 2 – Questões de Pesquisa

	Questão	Justificativa
RQ1	Como algoritmos de *ML* detectam intrusões em redes de *IoT*?	Por meio da modelagem do comportamento normal e anômalo do tráfego de rede e dos dispositivos conectados
RQ2	Quais algoritmos, métricas e validações são utilizadas, para a detecção de intrusões em *IoT*?	Em sua grande maioria, algorítimos clássicos supervisionados, com maior foco em *Random Forest*, *Decison Tree* e *Support Vector Machine*.
RQ3	Quais desafios a detecção de intrusões em dispositivos *IoT* enfrenta e como a *ML* pode superá-los?	Devido a recursos limitados e à heterogeneidade de *IoT*, a *ML* pode oferecer soluções de segurança otimizadas e adaptáveis que garantem alta detecção com baixo impacto nos recursos.

Fonte: Elaborado pelo autor (2026)

5 RESULTADOS

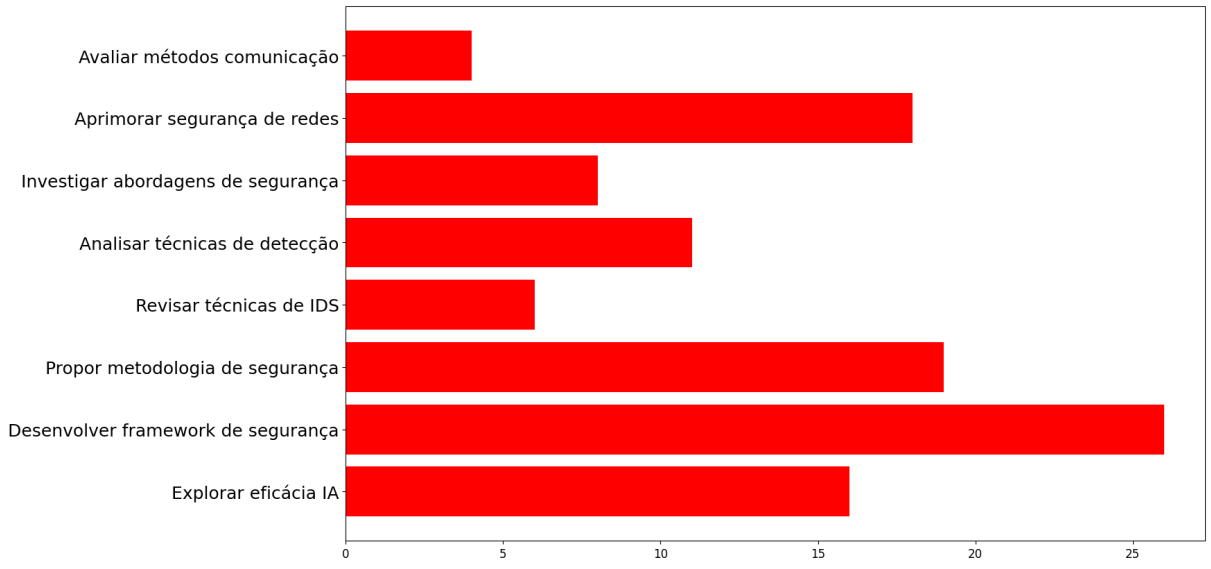
Neste tópico irá ser abordado os resultados obtidos, por meios das análises e experimentos descritos na seção 4, abordando as informações geradas e como elas se correlacionam com o objetivo do trabalho, demostrando com praticidade a correlação das informações obtidas. Além das conclusões das RQ.

5.1 Análise da Tabela de Artigos

Para as análises, foram acoplados os artigos selecionados na Figura 4 e montado uma tabela com as informações referentes ao: Objetivo; os algoritmos de *Machine Learning* usados; as características de *IoT* analisadas em cada artigo; os resultados encontrados; a contribuição do artigo ao final; e por fim os Desafios que foram descobertos ou solucionados. O conteúdo referenciado, que se trata da tabela completa, está presente no Apêndice A e a tabela com os termos já associados aos artigos que está presente no Apêndice B.

Com base nas informações extraídas com a montagem das tabelas, buscou-se observar como as informações se comportam, sendo elas correlacionadas a um mesmo tema ou abordando novos métodos. Em relação às tabelas, foram extraídas as informações da Coluna Objetivo e analisou-se a repetição de palavras referente a finalidade de cada trabalho e como eles se comportam, conforme a Figura 5:

Figura 5 – Número de Repetições de Palavras na Coluna Objetivo



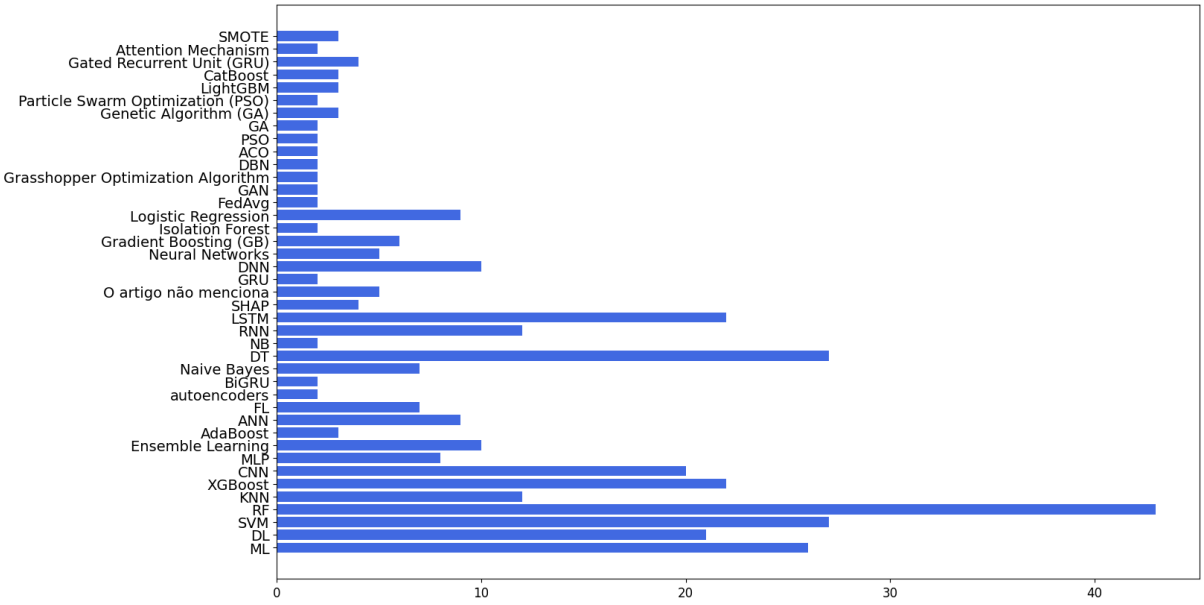
Fonte: Elaborado pelo autor (2026).

Na Figura 5 percebe-se que as palavras com maior reincidência são: Desenvolver *framework* de Segurança (Com 26 repetições); Propor metodologia de segurança (Com 19 repetições) e Aprimorar segurança de redes (Com 18 repetições). O maior número de ocorrências nos pontos citados anteriormente, em especial o termo “Desenvolver *framework* de segurança” indicam que grande parte dos trabalhos analisados tem foco em propostas práticas ou arquiteturas para reforçar segurança, bem como na aplicação de AI para avaliar a eficácia dessas soluções. Categorias como “Explorar eficácia de AI” e “Analisar técnicas de detecção” aparecem com frequência similares, o que sugere que a pesquisa científica busca tanto novas metodologias com a utilização de AI quanto o refinamento das técnicas existentes de detecção de intrusão.

“Revisar técnicas de IDS” e, principalmente, “Avaliar métodos de comunicação” têm menor número de ocorrências, o que pode indicar que, na literatura recente, a segurança no contexto de redes IoT com IDS via ML é mais explorada pelo viés da detecção e resposta do que pela infraestrutura de comunicação em si. Os dados reforçam que o campo está majoritariamente voltado para desenvolver e testar *frameworks* e metodologias baseadas em ML para IDS, dentro do ecossistema de IoT, priorizando eficiência, eficácia e inovação nos mecanismos de detecção de ataques.

Na coluna de Algoritmos, foi realizada a extração de informações e buscou-se analisar as repetições de palavras para cada programa ou método de AI que foi utilizado pelos autores ao decorrer do trabalho, conforme a Figura 6:

Figura 6 – Número de Repetições de Palavras na Coluna Algoritmos



Fonte: Elaborado pelo autor (2026)

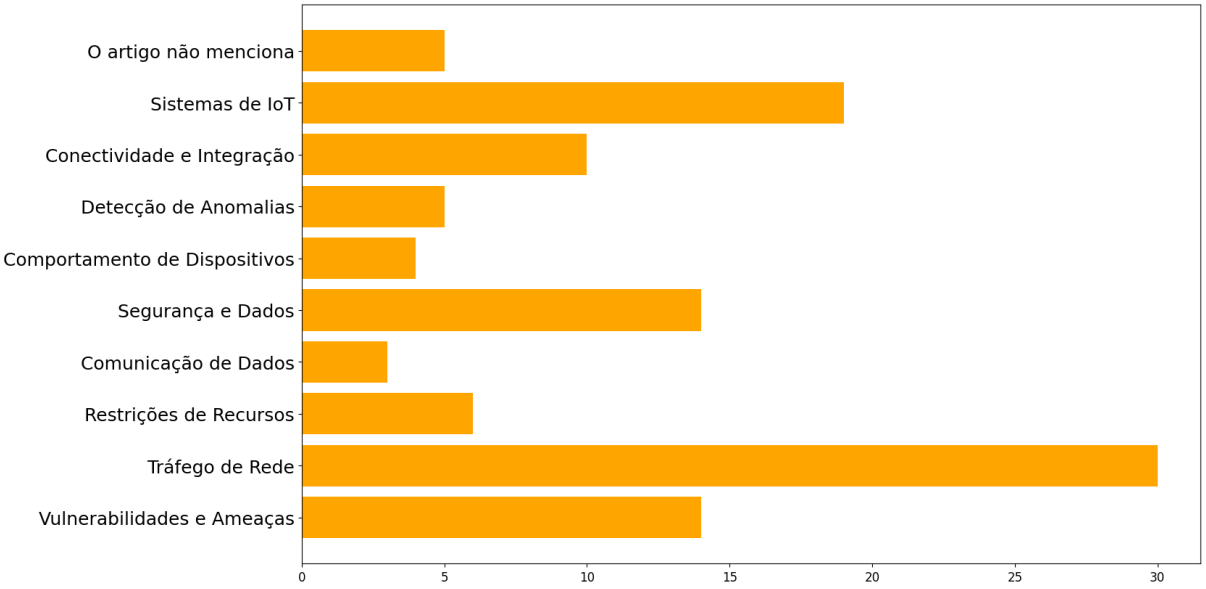
Na Figura 6 observa-se que as palavras com mais repetições se concentram nas palavras: RF (Random Forest) (Com 43 repetições), SVM (Support Vector Machine) (Com 27 repetições) e DT (Decision Tree) (Com 27 repetições). O algoritmo RF é disparadamente o mais citado, indicando que a maioria dos trabalhos faz referência ao conceito, utilizando-se de sua capacidade de aprendizagem de conjunto para classificação e regressão. Isso demonstra a preferência por métodos ensemble e baseados em distância devido à simplicidade, eficiência computacional e bom desempenho na detecção de intrusões em IoT, onde recursos são limitados. SVM e DT aparecem com números expressivos, sugerindo que essas técnicas são amplamente exploradas na detecção de intrusões em redes IoT, possivelmente devido à sua capacidade de lidar com grandes volumes de dados e identificar padrões complexos de ataques. Algoritmos como RF, SVM e DT são ideais para IDS em IoT devido a baixo consumo de energia (dado o cenário de uso em IoT) e processamento *edge*, contrastando com o uso de DL, que exige mais hardware, mas oferece maior precisão em ameaças avançadas.

Algoritmos como *Extreme Gradient Boosting* (XGBoost), *Long Short-Term Memory* (LSTM) e CNN aparecem entre 20 e 22 artigos, mostrando adoção de *boosting* e redes neurais para otimização, mas métodos de otimização evolutiva, como PSO e GA, e isolados como o *Isolation Forest*, são subutilizados, com menos de 10 aparições, revelando oportunidades para explorar abordagens híbridas em cenários IoT restritos. O termo “O artigo não menciona” é mínimo, confirmando que a maioria dos estudos, dos 117 trabalhos explorados, foca explicitamente em algoritmos ML, reforçando a maturidade do campo.

O gráfico demonstra que o campo de estudo está migrando de técnicas de ML clássico para algoritmos da esfera de DL e *ensemble*, o que demonstra uma prudência em ter uma detecção altamente precisa sem esgotar os recursos físicos de um dispositivo de IoT. A dominância desses algoritmos, como o RF ou SVM, valida o uso de métodos eficazes contra Ataques Multi-alvo, como *Distributed Denial of Service* (DDoS) e *Botnets*, excelentes em distinguir não apenas entre o uso “normal” e um ataque propriamente dito, mas em identificar qual tipo de ataque está ocorrendo. Algoritmos como o KNN, por exemplo, exigem métodos matemáticos com custos elevados para lidar com várias classes de uma vez, o que sobrecarregaria um dispositivo que tenta detectar um ataque de intrusão. O gráfico confirma que há um ecossistema diversificado de técnicas de ML utilizadas em IDS para IoT, mas com maior concentração em métodos de alto desempenho, como RF, SVM e DT, alinhando-se ao propósito do estudo de explorar abordagens relevantes e eficazes para esse contexto.

A Coluna Características de IoT foi analisada, também foi realizada a extração de informações e buscou-se analisar a repetição de palavras e a correlação das características, com a ideia de se projetar uma defesa para sistemas IoT, conforme a Figura 7:

Figura 7 – Número de Repetições de Palavras na Coluna Características de IoT

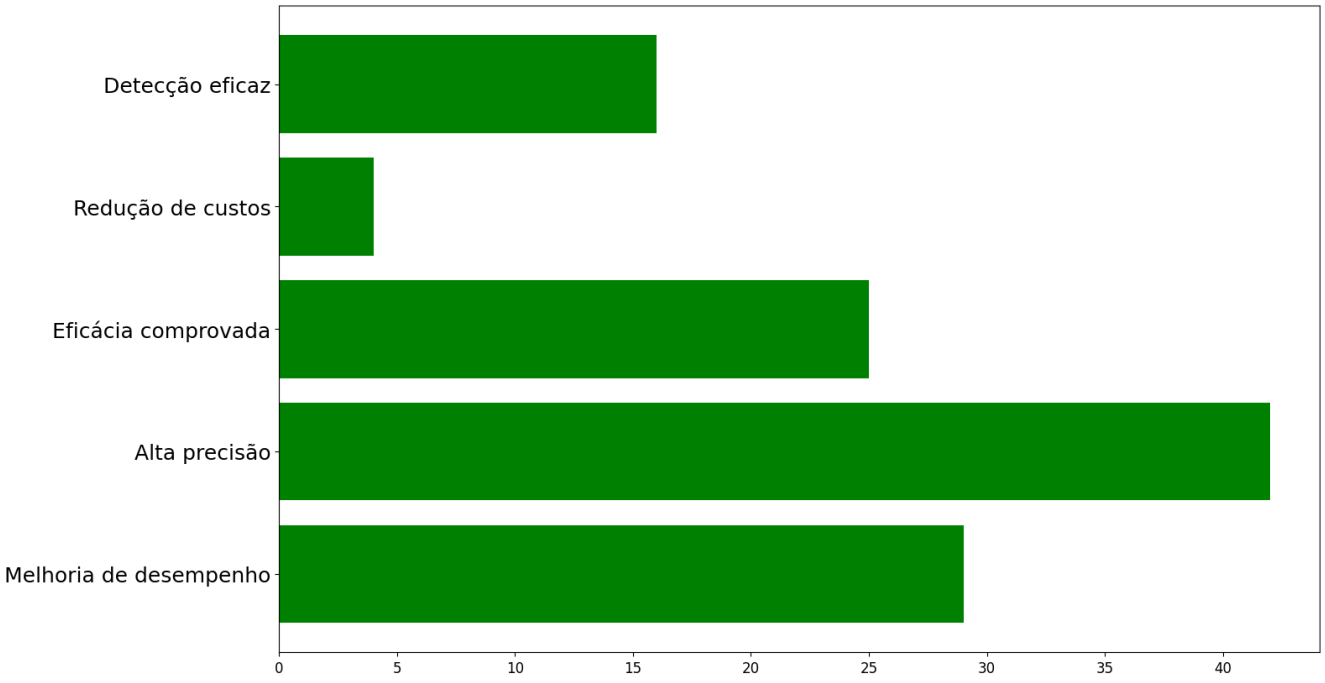


Fonte: Elaborado pelo autor (2026)

Na Figura 7 verifica-se a recorrência das seguintes palavras: Tráfego de Rede (Com 30 repetições); Sistemas de IoT (Com 19 repetições); Segurança e Dados, Vulnerabilidades e Ameaças (Com 14 repetições cada). "Tráfego de Redes" se apresenta como o termo mais citado, indicando que muitos trabalhos analisados dão prioridade à movimentação de dados entre redes de computadores, destaque para o volume de dados ou sessões e além de serem essenciais a segurança e desempenho de sistemas IoT. A alta incidência do termo "Sistemas de IoT" sugere que os autores abordam frequentemente o estudo de como funciona o agrupamento de dispositivos IoT e como nestes sistemas podem possuir falhas que comprometam a segurança. O termo "Vulnerabilidades e Ameaças", implica que os autores realizaram correlações de possíveis ameaças que poderiam ser utilizadas em determinadas vulnerabilidades existentes nas redes IoT e como a aplicação de IDS com ML poderia ser utilizada para contorná-la. O termo "Segurança e Dados" incita que a proteção da integridade e da confidencialidade das informações transmitidas é abordada com relevância, mostrando a preocupação em garantir a confiabilidade de redes IoT, dado o iminente desafio de combater ataques de intrusão. Em sua maioria, os trabalhos apresentam uma abordagem mais voltada à segurança das informações e como o resguardo dessas informações pode ser afetado ou não através da rede de conexão, ou através do sistema.

A coluna de Resultados, com a extração de informações e as análises das repetições de palavras, buscou informar como cada artigo apresentava as resoluções das pesquisas, conforme a Figura 8:

Figura 8 – Número de Repetições de Palavras na Coluna Resultado



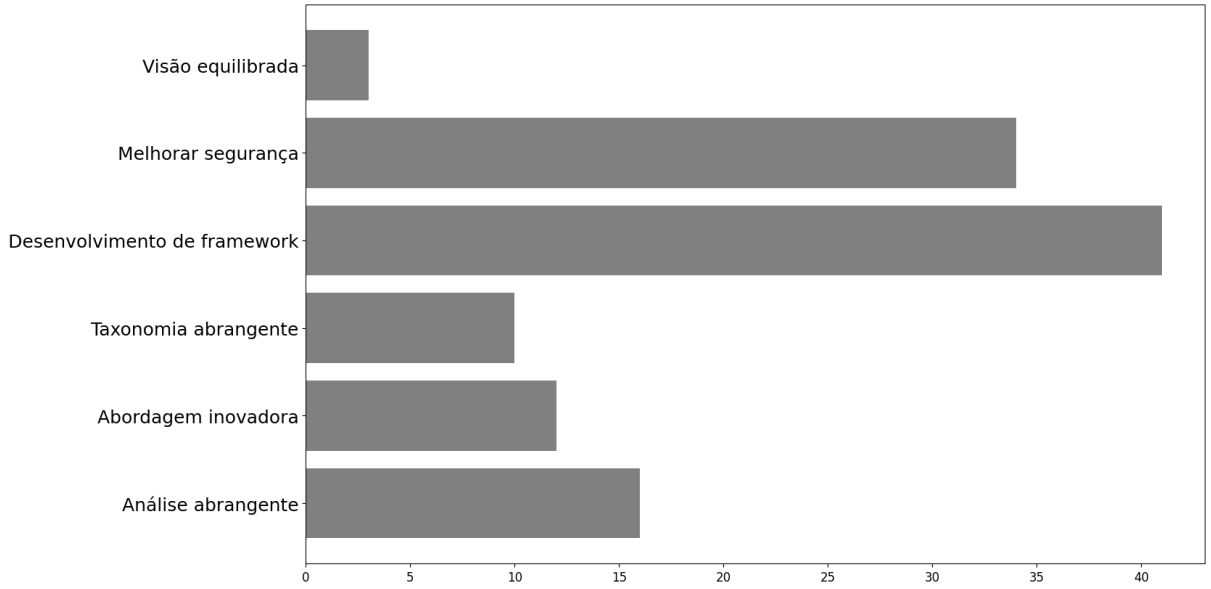
Fonte: Elaborado pelo autor (2026)

Na Figura 8 verifica-se a recorrência das seguintes palavras: Alta precisão (Com 42 repetições); Melhoria de desempenho (Com 29 repetições); Eficácia comprovada (Com 25 repetições). O termo “Alta precisão” ter uma ocorrência tão expressiva demostra que a grande maioria das propostas dos trabalhos atingiram um patamar de exatidão em seus resultados, sejam estas propostas, um modelo ou testes em cenários simulados de redes IoT. Além disso, “Melhoria de desempenho” também aparece com relevância, evidenciando que muitos autores buscam otimizar o tempo de processamento ou reduzir o impacto da solução nos dispositivos IoT, conciliando segurança e eficiência operacional.

Abordando o termo de “Eficácia comprovada”, nota-se em sua maioria, os trabalhos abordaram métodos ou desenvolveram novos tipos de sistemas e pesquisas que necessitavam de testes prévios em ambientes ataques. Assim, a comprovação de que esses métodos fossem eficazes necessitaria de realizar os testes necessários, o que se mostrou efetivo. Por outro lado, “Redução de custos” e “Detecção eficaz” aparecem com menor frequência, sugerindo que há espaço para pesquisas que explorem a redução de serviços utilizados e simplicidade de implementação, tornando essas soluções mais acessíveis para aplicações práticas.

A coluna de Contribuição, na extração de informações e as análises das repetições de palavras, buscou informar como cada artigo apresentava sua colaboração com as pesquisas acadêmicas, conforme a Figura 9:

Figura 9 – Número de Repetições de Palavras na Coluna Contribuição



Fonte: Elaborado pelo autor (2026)

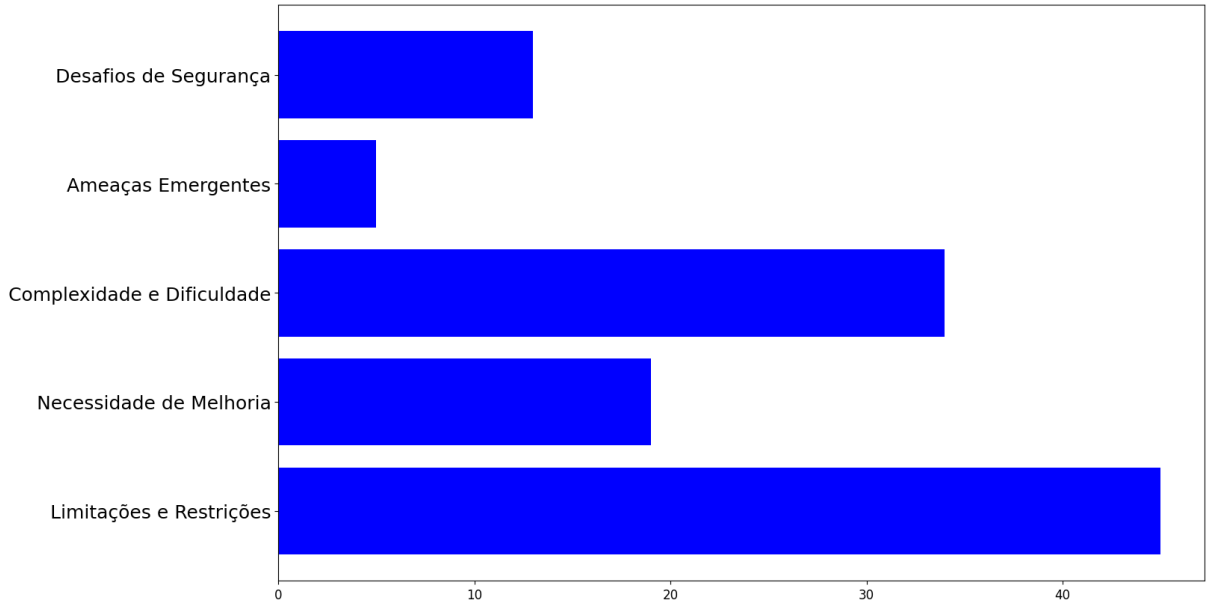
Na Figura 9 verifica que a recorrência das seguintes palavras: “Desenvolvimento” (Com 41 repetições); “Melhorar segurança” (Com 34 repetições). Os termos “Desenvolvimento de *framework*” e “Melhorar segurança” são os mais frequentes, indicando que a maioria dos estudos prioriza soluções aplicáveis, como criação de estruturas integradas de ML para IDS em IoT, em vez de análises teóricas. Isso se aplica a um cenário atual de grande abundância de dispositivos, gera o aumento de ataques, e soluções para esses ataques são cada vez mais requisitados; o foco em criar meios de defesas se tornam um meio importante de pesquisa.

Os termos “Análise abrangente” e “Abordagem inovadora” sugerem ênfase em avaliações mais detalhadas e propostas criativas, mas com menor admissão comparada ao desenvolvimento de *frameworks*, revelando uma tendência para implementações concretas em cenários IoT vulneráveis, que contribuem para o estudo, ao trazer pontos de vista diferentes, ao abordarem estilos de métodos diferentes.

“Taxonomia abrangente” e “Visão equilibrada” são os termos com menor frequência, apontando para deficiências na classificação sistemática de ameaças ou perspectivas equilibradas entre prós e contras de ML em IDS para redes de IoT, o que gera trabalhos com pouca extração de tópicos relevantes para o estudo.

A coluna de Desafios, com a extração de informações e as análises das repetições de palavras, buscou informar como cada artigo apresentava as adversidades enfrentadas no decorrer das pesquisas, conforme a Figura 10:

Figura 10 – Número de Repetições de Palavras na Coluna Desafios



Fonte: Elaborado pelo autor (2026)

Na Figura 10 verifica-se que a recorrência das seguintes palavras: Limitações e Restrições (Com 45 repetições); Complexidade e Dificuldade (Com 34 repetições); Necessidade de Melhoria (Com 19 repetições). O termo de maior regularidade é “Limitações e Restrições”, que necessariamente se traduzem as insuficiências sobre os *hardware* e *software*, que enfrentaram muitos autores ao decorrer de seus trabalhos, como as restrições de utilizam de determinados programas, ou as limitações de potencial com peças físicas.

“Complexidade e Dificuldade”, se compreende como a forma de realizar testes necessários para as pesquisas serem comprovadas, sejam essas complexidades a análise de muitos algoritmos, a divisão de multi-tarefas para a detecção de múltiplos ataques, e as dificuldades relacionadas a limitações de *hardwares*, que limitaram muitas aplicações. “Necessidade de melhoria” se expressa como a forma de alcançar os objetivos propostos pelos autores, seja ele *frameworks* em desenvolvimentos, pesquisas sistemáticas que pesquisam sobre meios de defesas atuais.

5.2 Aplicação do Apriori

Visando identificar padrões recorrentes e associações significativas entre abordagens de segurança, algoritmos de ML e estratégias adotadas em IDS para redes de IoT, foi aplicado o algoritmo *Apriori* sobre o conjunto dos 117 trabalhos presentes no Apêndice A. Cada artigo foi modelado como uma transação, enquanto suas características metodológicas, assim como os algoritmos utilizados, tipos de abordagem, contribuições e desafios reportados, foram tratados como itens categóricos.

A aplicação do *Apriori* seguiu parâmetros adequados ao contexto de uma revisão sistemática exploratória, considerando um suporte mínimo de 5%, uma confiança mínima de 70% e a métrica de *lift* superior a 1.2, de modo a garantir a relevância estatística e evitar associações triviais. Esses valores estabelecidos colaboram para uma melhor tiragem de resultados, dado o contexto do número de trabalhos explorados. A tabela com os principais resultados, seguindo as métricas estabelecidas, pode ser observada na Tabela 3.

Tabela 3 – Principais regras de associação obtidas pelo algoritmo Apriori

Antecedente	**Consequente**	**Support (%)**	**Confidence (%)**	**Lift**
KNN	Random Forest	8.55	83.3	2.27
MLP	Random Forest	6.84	100.0	2.72
Decision Tree	Random Forest	16.24	70.4	1.91
Logistic Regression	Random Forest	5.98	77.8	2.12
Naive Bayes	SVM	4.27	71.4	3.10
Naive Bayes	Random Forest	4.27	71.4	1.94
Gradient Boosting	Random Forest	5.13	100.0	2.72
Federated Learning	Limitações e Restrições	4.27	71.4	1.86

Fonte: Elaborado pelo autor (2026)

Os resultados da aplicação do *Apriori*, revelam uma forte centralidade de algoritmos baseados em *ensemble learning*, especialmente o RF, que aparece de forma consistente associado a diversos outros métodos de ML. Observa-se que os trabalhos que utilizam KNN apresentam elevada probabilidade de também empregar RF, com uma confiança superior a 80% e *lift* significativamente acima de 1, indicando uma associação positiva robusta. Observação que se pode identificar para algoritmos como MLP, *Gradient Boosting*, DT e Regressão Logística, os quais demonstram elevada correlação com RF.

Esses resultados sugerem que o RF é amplamente utilizado como algoritmo de referência na avaliação de IDS baseados em ML, frequentemente empregado em estudos de desenvolvimento de *frameworks* ou como parte de abordagens de melhora da segurança de

sistemas. Esta predominância pode ser associada a sua robustez frente a dados desbalanceados, capacidade de lidar com alta dimensionalidade e bom desempenho em cenários heterogêneos, características comuns em ambientes de IoT.

Do mesmo modo, foram identificadas associações relevantes entre algoritmos probabilísticos e métodos de margem máxima, como *Naive Bayes* e SVM. A conexão desses algoritmos indica uma tendência da literatura em explorar abordagens complementares, comparando modelos estatísticos simples com classificadores mais sofisticados, a fim de avaliar desempenho e generalização em diferentes cenários de ataque. Outro resultado relevante refere-se às abordagens emergentes, como o FL. As regras de associação indicam que trabalhos que adotam essa técnica apresentam forte correlação com a menção explícita de limitações e desafios, tais como restrições computacionais, comunicação entre nós e problemas de convergência.

Em resumo, a utilização do *Apriori* evidencia que a literatura sobre IDS utilizando ML em redes de IoT é marcada pela predominância de estratégias comparativas e pelo uso recorrente de algoritmos consagrados, especialmente *ensembles*. Ao mesmo tempo, observa-se um movimento gradual em direção a abordagens mais distribuídas e colaborativas, ainda acompanhadas de desafios significativos.

5.3 Análise de Clusterização (K-Means)

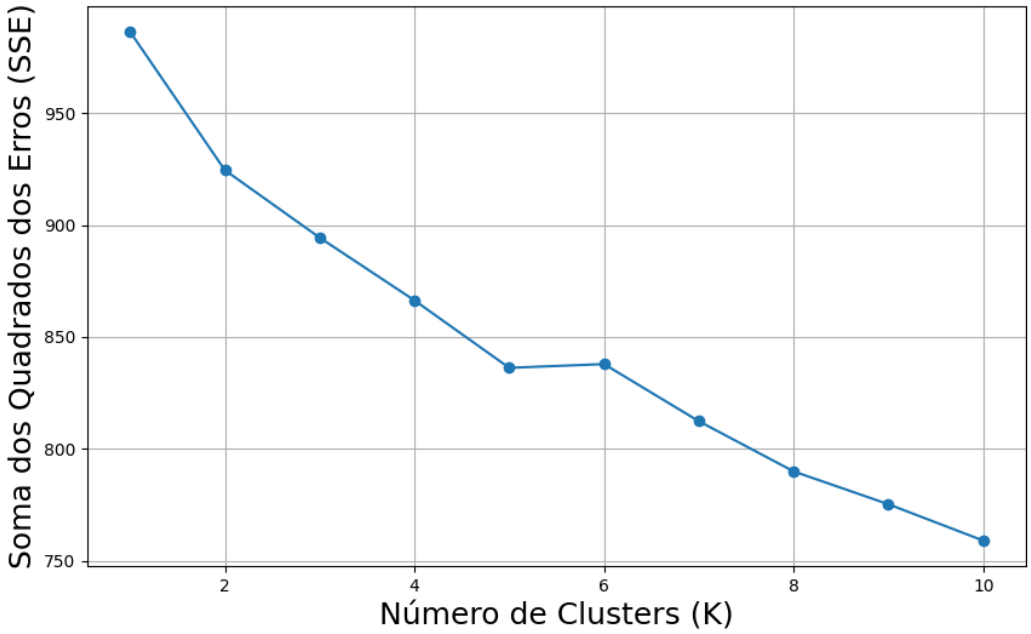
Nesta seção, será abordado o processo de Clusterização, realizada com o intuito de identificar padrões ocultos sobre os trabalhos analisados e organizar os dados obtidos sobre eles em grupos baseados em semelhança, assim, buscando trazer a tendência de correlação das colunas indicadas no Apêndice A.

Para identificar padrões e agrupar artigos com características temáticas semelhantes, aplicou-se a técnica de Análise de Clusterização utilizando o algoritmo *K-Means*. Foi realizada a seleção de *features*, que utilizando as colunas categóricas que descrevem o conteúdo técnico dos artigos: Objetivo, Algoritmos, Características de IoT Analisadas, Resultado, Contribuição e Desafios.

Como o algoritmo *K-Means* exige dados numéricos e as colunas continham múltiplos termos textuais, como RF e SVM, foi aplicado o *MultiLabelBinarizer*, uma forma de *One-Hot Encoding*. Este processo transformou cada termo único, como “Algoritmos_RF”, “Desafior_Limitações”, em uma nova coluna binária (1 para presente, 0 para ausente), resultando em uma matriz de *features* com 117 artigos e 319 colunas.

O número ideal de *clusters* (*K*) foi determinado pelo Método do Cotovelo (*Elbow Method*). O princípio do Método do Cotovelo é identificar o ponto de inflexão na curva, onde o ganho marginal na redução da Soma dos Quadrados dos Erros (SSE) começa a diminuir drasticamente. Este ponto, visualmente semelhante a um cotovelo, sugere o número de clusters que melhor equilibra a minimização da variância intra-cluster com a complexidade do modelo.

Figura 11 – Evolução Temporal dos Termos Mais Frequentes (em %)



Fonte: Elaborado pelo autor (2026)

Conforme observado na Figura 11, a redução da *SSE* é acentuada até *K=3*. A partir deste ponto, a curva começa a se estabilizar, indicando que a adição de mais *clusters* oferece um retorno decrescente na explicação da variância dos dados.

A análise do gráfico da *SSE* em função de *K* indicou que o ponto de inflexão mais significativo (o "cotovelo") ocorreu em *K=3* e *K=4*. Optou-se por *K=4* para permitir uma granularidade maior na identificação dos focos de pesquisa. A escolha de *K=4* foi justificada pela necessidade de uma maior granularidade na identificação dos focos de pesquisa. Esta escolha permitiu separar as linhas de pesquisa em quatro grupos temáticos distintos.

A aplicação do *K-Means* com K=4 resultou na divisão dos 117 artigos em quatro grupos distintos. O *Silhouette Score* de 0.0300, embora baixo, é esperado em dados textuais de alta dimensionalidade e serve para confirmar a separação mínima dos grupos, como pode ser observado no quadro de composição na Tabela 4.

Tabela 4 – Composição e Foco dos Clusters de Pesquisa

Cluster	Contagem	Foco Principal (Interpretação)	Termos Dominantes (>50% de Ocorrência)
Cluster 0	29	Revisão e Análise Abrangente	Algoritimos_ML (55.2%), Contribuição_Análise abrangente (44.8% - próximo de 50%).
Cluster 1	21	Desenvolvimento de Frameworks com Alta Precisão	Resultado_Alta precisão (90.5%), Contribuição_Desenvolvimento de framework (76.2%).
Cluster 2	29	Melhoria de Desempenho e Complexidade	Contribuição_Desenvolvimento de framework (75.9%), Resultado_Melhoria de desempenho (58.6%), Objetivo_Desenvolver framework de segurança (55.2%), Desafios_Complexidade e Dificuldade (51.7%).
Cluster 3	38	Algoritmos Clássicos (RF/SVM) e Segurança	Algoritimos_RF (73.7%), Contribuição_Melhorar segurança (73.7%), Resultado_Alta precisão (52.6%), Algoritimos_SVM (50.0%).

Fonte: Elaborado pelo autor (2026)

A análise dos quatro *clusters* na tabela, revela a diversidade de abordagens na literatura, permitindo a pesquisa a categorizar os artigos em linhas de pesquisa bem definidas e destrinchar os resultados de cada *clusters*:

a) **Cluster 0: Revisão e Mapeamento de Desafios**: Este cluster é caracterizado pela presença do termo genérico “Algoritimos_ML” e pela ausência de termos de algoritmos específicos de DL. Os artigos neste grupo tendem a ser trabalhos de revisão (*surveys*) ou estudos que se concentram em mapear o estado da arte e os desafios gerais da área, sem propor uma solução algorítmica específica;

b) **Cluster 1: Desenvolvimento de Frameworks de Alta Precisão**: Este grupo é dominado pelo foco em resultados de Alta Precisão e pela “Contribuição de Desenvolvimento de *Frameworks*”. Os artigos aqui se concentram em soluções que buscam resultados de detecção robustos, muitas vezes utilizando uma combinação de algoritmos para maximizar a acurácia. A alta frequência de “Desafios_Limitações” e “Restrições” sugere que, embora o foco seja na precisão, os autores reconhecem as dificuldades de implementação em ambientes reais de IoT;

c) **Cluster 2: Otimização de Desempenho e Complexidade**: Este *cluster* é o mais associado à "Complexidade e Dificuldade", mas também à "Melhoria de Desempenho". Isso indica que os artigos neste grupo tendem a propor soluções mais sofisticadas, provavelmente envolvendo DL ou arquiteturas complexas, para otimizar métricas de desempenho, como latência ou taxa de falsos positivos. O alto índice de "Objetivo_Desenvolver *framework*" de segurança reforça a ideia de que são trabalhos que buscam soluções completas e de alto nível;

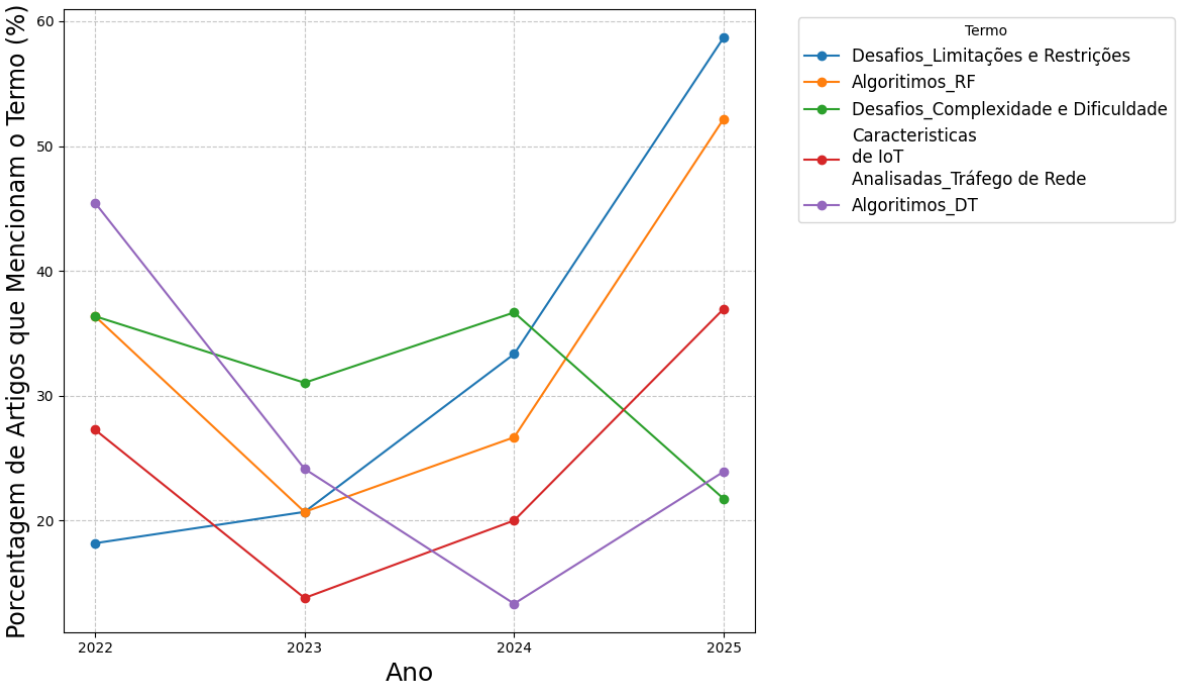
d) **Cluster 3: Viabilidade Prática com Algoritmos Clássicos**: Sendo o maior *cluster*, ele representa a linha de pesquisa mais pragmática. É dominado por algoritmos leves e eficientes como RF e SVM. O foco principal é "Melhorar a Segurança" e alcançar "Alta Precisão" com modelos que são mais facilmente implementáveis em dispositivos de borda com recursos limitados. Este *cluster* sugere que a comunidade de pesquisa valoriza a viabilidade e a simplicidade em ambientes de IoT, onde a complexidade de modelos mais pesados pode ser inviável.

5.4 Análise de Séries Temporais da Pesquisa

Para complementar a análise de clusterização e mapear a evolução da pesquisa ao longo do tempo, realizou-se uma Análise de Séries Temporais. O objetivo foi identificar como a popularidade de algoritmos, características de IoT e desafios abordados mudou anualmente na literatura. Assim como na clusterização, as colunas categóricas, Algoritmos, Características de IoT Analisadas e Desafios, foram transformadas em colunas binárias utilizando o *MultiLabel-Binarizer*. Cada termo único, como o "Algoritmos_RF", tornou-se uma coluna, onde o valor 1 indicava a presença do termo no artigo e 0 a ausência.

Os dados binários foram agrupados pelo campo Ano. Para cada ano, a soma das ocorrências de cada termo foi calculada. Em seguida, esta soma foi normalizada, dividindo-se pelo número total de artigos publicados naquele ano. O resultado é a porcentagem de artigos que mencionam o termo (%) para cada ano, permitindo uma comparação justa entre períodos com diferentes volumes de publicação. A Figura 12 ilustra a evolução temporal dos cinco termos mais frequentes identificados na análise, abrangendo o período de 2022 a 2025. A análise do gráfico revela tendências claras que refletem a maturidade e as prioridades da pesquisa em IDS para IoT, que podem ser observadas na análise a seguir:

Figura 12 – Evolução Temporal dos Termos Mais Frequentes (em %)



Fonte: Elaborado pelo autor (2026)

a) **Crescimento do Foco em Limitações e Restrições:** O termo "Desafios_Limitações e Restrições" (linha azul) demonstra uma tendência de crescimento constante e acelerada, atingindo o seu pico em 2025. Isso demostra que pesquisadores estão se tornando cada vez mais conscientes sobre as dificuldades de implementação prática de IDS em ambientes de IoT. O foco está deslocando da detecção de ataques, para a viabilidade da solução em dispositivos com restrições de *hardware*, memória e energia;

b) **Consolidação de Algoritmos Leves RF:** O termo "Algoritimos_RF" (linha laranja) apresenta uma forte tendência de crescimento, especialmente a partir de 2023, consolidando-se como um dos algoritmos mais citados. Esta informação se interliga com a conclusão do *Cluster 3*, da análise anterior, mas com uma mudança de um algorítimo, onde o RF e outros algoritmos leves, como o DT, em vez do SVM, são preferidos por oferecerem um excelente equilíbrio entre precisão e baixo custo computacional, tornando-os ideais para a implantação em dispositivos de borda de IoT;

c) **Estabilidade do Foco em Tráfego de Rede:** A "Características de IoT Analisadas_Tráfego de Rede" (linha vermelha) mostra um crescimento constante, indicando que a análise do fluxo de dados da rede permanece a principal fonte de informação para a detecção de intrusão, independentemente do algoritmo utilizado;

d) **Volatilidade da Complexidade:** O termo “Desafios_Complexidade e Dificuldade” (linha verde) iniciou-se em alta em 2022, obteve uma queda, mas retornou em seu pico em 2024, mas mostrou uma queda imediata. Esta volatilidade sugere que, embora a complexidade tenha sido um desafio inicial, a pesquisa mais recente está focando em problemas mais tangíveis, as “Limitações e Restrições de *hardware*”, ou está encontrando formas de mitigar a complexidade algorítmica.

5.5 Questões de Pesquisa

Neste tópico será abordada as Questões de Pesquisas (RQ), que inicialmente foram apresentadas na Seção 4. As Questões foram respondidas, se fundamentando a partir dos resultados obtidos pelas análises anteriores e trazendo respostas concisas com a abordagem do trabalho.

Como algoritmos de Machine Learning detectam intrusões em redes de IoT?

As redes de IoT possuem grande diversidade de dispositivos, que geram volumes massivos de dados em tempo real. Isso torna os métodos tradicionais de detecção de intrusão, baseados em assinaturas ou regras, muitas vezes inadequados devido à sua limitação em identificar novos padrões de ataque. Algoritmos de ML oferecem a capacidade de analisar abundância de dados, identificar comportamentos anômalos e detectar ameaças desconhecidas, possibilitando um nível superior de eficiência e precisão na segurança dessas redes.

Ao se utilizar de algoritmos de ML, consegue-se selecionar as variáveis relevantes, como número de conexões por IP, taxa de pacotes, tempo de sessão, entre outros. Isso reduz a dimensionalidade e melhora o desempenho do algoritmo. Os algoritmos mais utilizados na atualidade como RF, SVM, DT, ou DNN aprendem os padrões típicos de comportamento a partir de dados de treinamento. Durante esse processo, o modelo ajusta seus parâmetros para minimizar erros de classificação. Após os treinamentos, os modelos são capazes de identificar, em tempo real, desvios no padrão esperado, ou seja, comportamentos que diferem do que foi aprendido como normal são classificados como possíveis ataques (como DoS, *spoofing*, MitM, etc.). Como exemplificação, um modelo baseado em RF pode aprender que, normalmente, um sensor de temperatura envia dados a cada 30 segundos com tamanho médio de 100 bytes. Se esse mesmo sensor começar a enviar pacotes de 1.000 bytes a cada segundo, o modelo reconhece isso como comportamento anômalo, indicando uma possível intrusão ou comprometimento do dispositivo.

Quais algoritmos, métricas e validações são utilizadas, para a detecção de intrusões em IoT?

Após os resultados das análises, na parte de mineração dos dados dos artigos investigados, se pode definir os algorítimos analisados em 4 categorias: Algoritmos clássicos supervisionados; Algoritmos baseados em *Ensemble Learning*; Algoritmos de DL; Formas de Abordagens Emergentes.

a) Algoritmos clássicos supervisionados: Neste tópico se destaca os algoritmos mais utilizados no estado da arte atual, conforme comprovado pelas análises anteriores. Sendo estes os algoritmos: RF, DT e SVM. Estes algoritmos se destacaram como os métodos mais utilizados pelos autores, muito por sua robustez frente a quantidade de dados desbalanceados e a capacidade de lidar com a alta dimensionalidade e desempenhos adversos em cenários heterogêneos, que são tipicamente encontrados em redes IoT;
b) Algoritmos baseados em *Ensemble Learning*: Os algoritmos de *ensemble learning* são em sua particularidade, considerados poderosos para a aplicações em redes de IoT, já que estes cenários, enfrentam desafios que apenas um modelo, não teria capacidade de resolver desfavorecido, frente a ataques de intrusões. Os algoritmos que tiveram mais destaque foram: *Gradient Boosting*; XGBoost; *AdaBoost*. Estes algoritmos, em grande maioria dos casos, foram utilizados para aumentar a taxa de detecção de falsos positivos, gerados nos sistemas de IDS;
c) Algoritmos de DL: Algoritmos de DL, se provaram como métodos, frequentemente aplicados em arquiteturas centralizadas ou em ambientes com maior capacidade computacional. Os mais citados durante o trabalho foram: MLP; CNN; LSTM;
d) Formas de Abordagens Emergentes: Já alguns trabalhos, optaram por outros tipos de abordagens, como a aplicação de FL, visando preservar privacidade e reduzir tráfego de dados; a aplicação de *Reinforcement Learning*, para adaptação dinâmica e resposta a ataques; e a aplicação de Modelos híbridos, realizando uma combinação de ML clássico e DL.

   As métricas mais abordadas pelos autores, se concentraram em meios como o *Accuracy*; *Precision*; *Recall (Detection Rate)*; *F1-score*; *False Positive Rate (FPR)*. Se observa ao longo dos trabalhos, que métricas como o *Accuracy*, isoladamente não é considerada suficiente, especialmente devido ao desbalanceamento típico entre tráfego normal e ataques em *datasets* de IoT. Dessa maneira, métricas como *Recall*, *F1-score* e *FPR* são ampla-

mente empregadas para fornecer uma avaliação mais realista, equiparada aos cenários de intrusões.

As validações utilizadas, segundo o analisado nos artigos, evidencia o uso recorrente de técnicas de validação cruzada *(k-fold cross-validation*), amplamente empregada para mitigar vieses decorrentes da divisão dos dados e para avaliar o desempenho dos modelos em diferentes subconjuntos do conjunto de dados. Em cenários com forte desbalanceamento entre tráfego normal e malicioso, também são observadas abordagens baseadas em *stratified k-fold*, assegurando a preservação da distribuição das classes em cada partição. Também a utilização de múltiplos *datasets* públicos e sintéticos como forma de validação externa, visando comprovar a generalização das soluções propostas.

Quais desafios a detecção de intrusões em dispositivos IoT enfrenta e como a ML pode superá-los?

Dispositivos de IoT operam frequentemente com recursos computacionais limitados, como baixa capacidade de processamento e energia, o que dificulta a aplicação de técnicas complexas de segurança. Além disso, a heterogeneidade dos dispositivos e a falta de padronização agravam os desafios de integração e proteção. O ML pode ajudar a superar essas barreiras por meio de modelos otimizados e adaptáveis, que analisam dados de maneira distribuída e eficiente, minimizando o impacto nos recursos dos dispositivos enquanto mantêm altos níveis de detecção.

Em redes de sistema IoT de alta complexidade e tamanho, como, por exemplo, o uso em cidades inteligentes, a gama de dispositivos conectados simultaneamente não apresenta uma precisão segura para a defesa e distribuição de dados entre estes dispositivos e em muitos casos, por limitações de *hardware*, acabam se limitando na forma de assegurar esta distribuição e se limitando nas informações repassadas, com o perigo iminente de um ataque a qualquer aparelho. Dessa forma, ao se utilizar de um algoritmo, que seja um auxiliador na segurança de todos os dispositivos simultâneos, se abre um precedente de melhora na distribuição dessa rede, podendo contornar um problema que limita na expansão de mais dispositivos ativos ao mesmo tempo.

5.6 Síntese dos Resultados Obtidos

Os algoritmos mais proeminentes identificados incluem RF, SVM e DT, que demonstraram alta precisão na detecção de intrusões, frequentemente superando 95% em conjuntos

de dados como NSL-KDD e UNSW-NB15. Mas demostrando que apenas o uso da métrica de acurácia, não ser o suficiente, reforçando a utilização de outras métricas como *Recall*, *F1-score* e *False Positive Rate*. Essas técnicas se destacam pela capacidade de lidar com volumes massivos de dados gerados por dispositivos IoT, identificando padrões anômalos associados a ataques comuns, como DoS, DDoS e injeções maliciosas.

As características das redes IoT analisadas, tais como baixa latência, escalabilidade e consciência de localização, foram cruciais para o sucesso dessas aplicações, destacando a necessidade de soluções leves que minimizem o consumo de energia em dispositivos restritos.

As análises realizadas por meio dos métodos de mineração de dados, demostrou resultados como as análises de repetição de palavras nas colunas de contribuições e desafios reforçam que, embora o ML contribua significativamente para a automação da detecção e resposta a incidentes, persistem barreiras como a dependência de conjuntos de dados rotulados de alta qualidade e a vulnerabilidade a ataques adversariais.

A análise de regras de associação confirmou a forte correlação entre o antecedente como o RF, e algoritmos baseados em *ensemble learning*, sublinhando a preferência da comunidade de pesquisa por soluções que equilibram eficácia e viabilidade em ambientes de recursos limitados.

A Análise de Clusterização (K-Means), revelou que a linha de pesquisa mais proeminente, referida no Cluster 3, é dominada por algoritmos leves e eficientes, como RF e SVM. Esta observação se complementa pela Análise de Tendências Temporais, que mostrou o crescimento contínuo do termo “Algoritimos_RF”, confirma que a comunidade de pesquisa prioriza a viabilidade prática e a simplicidade em detrimento da complexidade de modelos de DL, devido às restrições de recursos dos dispositivos IoT.

Além disso, a Análise de Tendências Temporais demonstrou uma clara evolução no foco dos desafios. Houve uma migração da preocupação com a “Complexidade e Dificuldade”, que obteve um pico em 2022, para um foco crescente e sustentado em “Limitações e Restrições”, termo este que obteve ascensão até 2025.

6 CONCLUSÕES E TRABALHOS FUTUROS

Este trabalho explorou o estado da arte em abordagens de segurança para IDS em redes de IoT, com ênfase no emprego de técnicas de ML como mecanismo de defesa. Por meio de uma análise de 117 artigos selecionados, se identificou padrões recorrentes nos objetivos, algoritmos utilizados, características específicas das redes IoT, resultados obtidos, contribuições e desafios enfrentados. Os achados revelam que a ML representa uma solução robusta e adaptável para mitigar ameaças cibernéticas em ambientes IoT, onde a heterogeneidade de dispositivos, a limitação de recursos computacionais e a necessidade de processamento em tempo real impõem restrições significativas aos métodos tradicionais de segurança.

Em termos de contribuições, esta revisão sistemática oferece um panorama consolidado que pode guiar pesquisadores e profissionais na implementação de IDS mais eficazes, promovendo uma maior resiliência contra ameaças evolutivas. O trabalho tem entendimento que, embora tenha sido utilizadas bases de dados abrangentes, dado a quantidade de artigos obtidos, a exclusão de literatura cinzenta como, relatórios técnicos industriais, white papers, e a restrição a termos de busca específicos podem ter omitido abordagens proprietárias ou tecnologias emergentes que ainda não foram amplamente documentadas em periódicos acadêmicos.

Os resultados do trabalho também refletem o que está sendo publicado e não necessariamente o que está sendo implementado na indústria de IoT em larga escala. O trabalho compreende que existe frequentemente um hiato entre a pesquisa acadêmica e a adoção industrial, o que significa que as tendências identificadas podem levar tempo para se materializarem em produtos comerciais.

Mas apesar destes contrapontos mencionados, o trabalho se valida pela utilização de formas como a utilização combinada de três técnicas distintas de análise de dados, *Apriori*, Clusterização e Análise de Tendências Temporais, que permitiu que as conclusões fossem validadas por diferentes perspectivas. A convergência de resultados, como o RF aparecendo como tendência temporal e como núcleo de um cluster de viabilidade, reforça a precisão das descobertas. Além da aplicação de critérios de inclusão e exclusão bem definidos, utilizando bases de dados científicas renomadas, garantiu que a amostra de 117 artigos fosse representativa do estado da arte atual, minimizando a inclusão de trabalhos sem relevância técnica.

Para trabalhos futuros, sugere-se a investigações em modelos de ML leves, como *TinyML*, poderiam endereçar as restrições computacionais de dispositivos de baixa potência, permitindo detecções em tempo real sem comprometer a autonomia energética. Outra direção

promissora envolve o desenvolvimento de *frameworks* de *XAI* adaptados a IoT, visando melhorar a interpretabilidade dos modelos e facilitar sua adoção em ambientes regulados, como saúde e infraestrutura crítica. Também se propõe uma investigação sistemática sobre as abordagens de privacidade preservada no contexto de IDS para IoT. Dado que o treinamento de modelos de ML exige o acesso a grandes volumes de dados sensíveis, torna-se imperativo analisar como as soluções propostas na literatura lidam com a confidencialidade das informações.

Por fim, a sugestão de avaliação da portabilidade e do desempenho dos métodos de ML em diferentes ecossistemas de IoT. Embora muitos modelos apresentem alta acurácia em *datasets* específicos, o comportamento do tráfego varia drasticamente entre ambientes de *Smart Homes*, *Smart Offices* e a IIoT.

REFERÊNCIAS

ABBAS, G.; MEHMOOD, A.; CARSTEN, M.; EPIPHANIOU, G.; LLORET, J. Safety, security and privacy in machine learning based internet of things. **Journal of Sensor and Actuator Networks**, MDPI, v. 11, n. 3, p. 38, 2022. Disponível em: <https://www.mdpi.com/2224-2708/11/3/38>. Acesso em: 21 jan. 2025.

ABDI, A. H.; AUDAH, L.; SALH, A.; ALHARTOMI, M. A.; RASHEED, H.; AHMED, S.; TAHIR, A. Security control and data planes of sdn: A comprehensive review of traditional, ai, and mtd approaches to security solutions. **IEEE Access**, v. 12, p. 69941–69980, 2024. Disponível em: <https://ieeexplore.ieee.org/document/10508380>. Acesso em: 16 jan. 2025.

ADEWOLE, K. S.; JACOBSSON, A.; DAVIDSSON, P. Intrusion detection framework for internet of things with rule induction for model explanation. **Sensors**, MDPI, v. 25, n. 6, p. 1845, 2025. Disponível em: <https://www.mdpi.com/1424-8220/25/6/1845>. Acesso em: 10 dez. 2025.

ADIL, M.; SONG, H.; JAN, M. A.; KHAN, M. K.; HE, X.; FAROUK, A.; JIN, Z. Uav-assisted iot applications, qos requirements and challenges with future research directions. **ACM Computing Surveys**, ACM New York, NY, v. 56, n. 10, p. 1–35, 2024. Disponível em: <https://dl.acm.org/doi/10.1145/3657287>. Acesso em: 18 jan. 2025.

AFROZ, M.; NYAKWENDE, E.; GOSWAMI, B. Intrusion detection in smart home environments: A machine learning approach. **Transportation Research Procedia**, Elsevier, v. 84, p. 243–250, 2025. Disponível em: <https://www.sciencedirect.com/science/article/pii/S2352146525001176>. Acesso em: 15 dez. 2025.

AGRAWAL RAKESH; SRIKANT, R. **Fast algorithms for mining association rules and sequential patterns**. The University of Wisconsin-Madison, 1996. Disponível em: <https://search.proquest.com/openview/f7039a6fc721d9fd7a677aa548b01e9a/1?pq-origsite=gscholar&cbl=18750&diss=y>. Acesso em: 21 jan. 2025.

AHMAD, J.; SHAH, S. A.; LATIF, S.; AHMED, F.; ZOU, Z.; PITROPAKIS, N. Drann_pso: A deep random neural network with particle swarm optimization for intrusion detection in the industrial internet of things. **Journal of King Saud University-Computer and Information Sciences**, Elsevier, v. 34, n. 10, p. 8112–8121, 2022. Disponível em: <https://www.sciencedirect.com/science/article/pii/S1319157822002701>. Acesso em: 15 dez. 2025.

AHMED, U.; LIN, J. C.-W.; SRIVASTAVA, G. Exploring the potential of cyber manufacturing system in the digital age. **ACM Transactions on Internet Technology**, ACM New York, NY, v. 23, n. 4, p. 1–38, 2023. Disponível em: <https://dl.acm.org/doi/10.1145/3596602>. Acesso em: 18 jan. 2025.

AKSHAYA, V.; MANDALA, V.; ANILKUMAR, C.; VISHNURAJA, P.; AARTHI, R. *et al.* Security enhancement and attack detection using optimized hybrid deep learning and improved encryption algorithm over internet of things. **Measurement: Sensors**, Elsevier, v. 30, p. 100917, 2023. Disponível em: <https://www.sciencedirect.com/science/article/pii/S2665917423002532>. Acesso em: 15 dez. 2025.

ALAHMARI, S.; ALKHARASHI, A. Privacy-aware federated learning framework for iot security using chameleon swarm optimization and self-attentive variational autoencoder.

Computer Modeling in Engineering & Sciences, Tech Science Press, v. 143, n. 1, p. 849, 2025. Disponível em: <https://www.sciencedirect.com/org/science/article/pii/S1526149225000827>. Acesso em: 15 dez. 2025.

ALHARBI, S.; ALGHAZZAWI, D.; HAKEEM, A.; MOHAISEN, L.; CHENG, L.; ATTIAH, A. A blockchain-based collaborative intrusion detection systems framework. **IEEE Internet of Things Journal**, v. 11, n. 15, p. 25481–25493, 2024. Disponível em: <https://ieeexplore.ieee.org/document/10374188>. Acesso em: 16 jan. 2025.

ALMALAWI, A. Claire: A four-layer active learning framework for enhanced iot intrusion detection. **Electronics**, MDPI, v. 14, n. 22, p. 4547, 2025. Disponível em: <https://www.mdpi.com/2079-9292/14/22/4547>. Acesso em: 10 dez. 2025.

ALMOHAIMEED, M.; ALBALWY, F. Enhancing iot network security using feature selection for intrusion detection systems. **Applied Sciences (2076-3417)**, v. 14, n. 24, 2024. Disponível em: <https://www.mdpi.com/2076-3417/14/24/11966>. Acesso em: 10 dez. 2025.

ALNASSER, O.; MUHTADI, J. A.; SALEEM, K.; SHRESTHA, S. Signature and anomaly based intrusion detection system for secure iots and v2g communication. **ALEXANDRIA ENGINEERING JOURNAL**, ELSEVIER RADARWEG 29, 1043 NX AMSTERDAM, NETHERLANDS, v. 125, p. 424–440, 2025. Disponível em: <https://www.sciencedirect.com/science/article/pii/S1110016825003771>. Acesso em: 15 dez. 2025.

ALOTAIBI, A.; BARNAWI, A. Idsoft: A federated and softwarized intrusion detection framework for massive internet of things in 6g network. **Journal of King Saud University-Computer and Information Sciences**, Elsevier, v. 35, n. 6, p. 101575, 2023. Disponível em: <https://www.sciencedirect.com/science/article/pii/S1319157823001295>. Acesso em: 15 dez. 2025.

ALOTAIBI, B. A survey on industrial internet of things security: Requirements, attacks, ai-based solutions, and edge computing opportunities. **Sensors**, MDPI, v. 23, n. 17, p. 7470, 2023. Disponível em: <https://www.mdpi.com/1424-8220/23/17/7470>. Acesso em: 21 jan. 2025.

ALRAYES, F. S.; ZAKARIAH, M.; AMIN, S. U.; KHAN, Z. I.; HELAL, M. Intrusion detection in iot systems using denoising autoencoder. **IEEE Access**, IEEE, 2024. Disponível em: <https://ieeexplore.ieee.org/abstract/document/10658641/>. Acesso em: 22 jan. 2025.

ALSALAMAH, H. A.; ISMAIL, W. N. Evolutionary computation for feature optimization and image-based dimensionality reduction in iot intrusion detection. **Mathematics**, MDPI AG, v. 13, n. 23, p. 3869, 2025. Disponível em: <https://www.mdpi.com/2227-7390/13/23/3869>. Acesso em: 10 dez. 2025.

ALSALAMAH, H. A.; ISMAIL, W. N. A swarm-based multi-objective framework for lightweight and real-time iot intrusion detection. **Mathematics**, MDPI, v. 13, n. 15, p. 2522, 2025. Disponível em: <https://www.mdpi.com/2227-7390/13/15/2522>. Acesso em: 10 dez. 2025.

ALSHATHRI, S.; EL-SAYED, A.; SHAFAI, W. E.; HEMDAN, E. E.-D. An efficient intrusion detection framework for industrial internet of things security. **Comput. Syst. Sci. Eng.**, v. 46, n. 1, p. 819–834, 2023. Disponível em: <https://www.researchgate.

net/profile/Walid-El-Shafai/publication/367332967_An_Efficient_Intrusion_Detection_Framework_for_Industrial_Internet_of_Things_Security/links/63cd0e3dd9fb5967c2f84310/An-Efficient-Intrusion-Detection-Framework-for-Industrial-Internet-of-Things-Security.pdf?origin=journalDetail&_tp=eyJwYWdlIjoiam91cm5hbERldGFpbCJ9>. Acesso em: 22 jan. 2025.

ALSOUFI, M. A.; SIRAJ, M. M.; GHALEB, F. A.; AL-RAZGAN, M.; AL-ASALY, M. S.; ALFAKIH, T.; SAEED, F. Anomaly-based intrusion detection model using deep learning for iot networks. **Computer Modeling in Engineering & Sciences**, Tech Science, v. 141, n. 1, p. 823–845, 2024. Disponível em: <https://www.sciencedirect.com/org/science/article/pii/S1526149224002479>. Acesso em: 15 dez. 2025.

ALZUBI, O. A.; ALZUBI, J. A.; QIQIEH, I.; AL-ZOUBI, A. An iot intrusion detection approach based on salp swarm and artificial neural network. **International Journal of Network Management**, Wiley Online Library, p. e2296, 2024. Disponível em: <https://onlinelibrary.wiley.com/doi/abs/10.1002/nem.2296?casa_token=_VjtfhJ7tbEAAAAA:FHnVF9lIwfQa7rpFGDLbcrhMoYPlOwl6n_b9Xl9sm-c11vbn117FeJj_L2ctZQQxUwdDXcBYWC78mH7e>. Acesso em: 22 jan. 2025.

AMMAR, M.; JAVAID, N.; SAUDAGAR, A. K. J.; AHMED, I. An optimized deep and active learning oriented framework for intrusion detection in internet of sensor things. **Ain Shams Engineering Journal**, Elsevier, v. 16, n. 10, p. 103607, 2025. Disponível em: <https://www.sciencedirect.com/science/article/pii/S209044792500348X>. Acesso em: 15 dez. 2025.

AMMOUN, L.; JENA, L.; CHITHALURU, P.; GUPTA, S.; MOHANTY, M. Internet of medical things (iomt): A succinct study. In: ____. [S.l.: s.n.], 2024. p. 76–83. ISBN 9789362521552. Acesso em: 23 jan. 2025.

AMUTHADEVI, C.; VENKATESAN, R.; MYTHILY, M.; CANESSANE, R. A. Tinyml-based intrusion detection systems for sustainable and energy-constrained iot devices. **Results in Engineering**, Elsevier, p. 108013, 2025. Disponível em: <https://www.sciencedirect.com/science/article/pii/S2590123025040642>. Acesso em: 15 dez. 2025.

ASLAM, M. M.; TUFAIL, A.; KIM, K.-H.; APONG, R. A. A. H. M.; RAZA, M. T. A comprehensive study on cyber attacks in communication networks in water purification and distribution plants: challenges, vulnerabilities, and future prospects. **Sensors**, MDPI, v. 23, n. 18, p. 7999, 2023. Disponível em: <https://www.mdpi.com/1424-8220/23/18/7999>. Acesso em: 17 jan. 2025.

ATZORI, L.; IERA, A.; MORABITO, G. The internet of things: A survey. **Computer networks**, Elsevier, v. 54, n. 15, p. 2787–2805, 2010. Disponível em: <https://www.sciencedirect.com/science/article/pii/S1389128610001568?casa_token=_Cpcn3nIL5wAAAAA:ePdLo7QLtc3oD1HV8zr0HtnXAWfskvnou9vWz1GbrldRGthral-psFI_LVZmi8c3KmBq5-dEjP0>. Acesso em: 23 jan. 2025.

BAKHSH, S. A.; KHAN, M. A.; AHMED, F.; ALSHEHRI, M. S.; ALI, H.; AHMAD, J. Enhancing iot network security through deep learning-powered intrusion detection system. **Internet of Things**, Elsevier, v. 24, p. 100936, 2023. Disponível em: <https://www.sciencedirect.com/science/article/pii/S2542660523002597>. Acesso em: 15 dez. 2025.

BANAD, Y. M.; SHARIF, S. S.; REZAEI, Z. Artificial intelligence and machine learning for smart grids: from foundational paradigms to emerging technologies with digital twin and large language model-driven intelligence. **Energy Conversion and Management: X**, Elsevier, v. 28, p. 101329, 2025. Disponível em: <https://www.sciencedirect.com/science/article/pii/S2590174525004611>. Acesso em: 15 dez. 2025.

BECERRA-SUAREZ, F. L.; FERNÁNDEZ-ROMAN, I.; FORERO, M. G. Improvement of distributed denial of service attack detection through machine learning and data processing. **Mathematics**, MDPI, v. 12, n. 9, p. 1294, 2024. Disponível em: <https://www.mdpi.com/2227-7390/12/9/1294>. Acesso em: 17 jan. 2025.

BENMALEK, M.; SEDDIKI, A.; HAOUAM, K.-D. Snn-iomt: A novel ai-driven model for intrusion detection in internet of medical things. **CMES-Computer Modeling in Engineering and Sciences**, v. 143, n. 1, p. 1157–1184, 2025. Disponível em: <https://www.sciencedirect.com/org/science/article/pii/S1526149225001079>. Acesso em: 15 dez. 2025.

BERGUIGA, A.; HARCHAY, A.; MASSAOUDI, A.; AYED, M. B.; BELMABROUK, H. Gmlp-ids: A novel deep learning-based intrusion detection system for smart agriculture. **Computers, Materials & Continua**, v. 77, n. 1, 2023. Disponível em: <https://www.sciencedirect.com/org/science/article/pii/S1546221823001194>. Acesso em: 15 dez. 2025.

BHARDWAJ, A.; TYAGI, R.; SHARMA, N.; KHARE, A.; PUNIA, M. S.; GARG, V. K. Network intrusion detection in software defined networking with self-organized constraint-based intelligent learning framework. **Measurement: Sensors**, Elsevier, v. 24, p. 100580, 2022. Disponível em: <https://www.sciencedirect.com/science/article/pii/S2665917422002148>. Acesso em: 15 dez. 2025.

BHUKYA, R.; MOEED, S. A.; MEDAVAKA, A.; KHADIDOS, A. O.; KHADIDOS, A. O.; SELVARAJAN, S. Spark and sad: Leading-edge deep learning frameworks for robust and effective intrusion detection in scada systems. **International Journal of Critical Infrastructure Protection**, Elsevier, v. 49, p. 100759, 2025. Disponível em: <https://www.sciencedirect.com/science/article/pii/S1874548225000204>. Acesso em: 15 dez. 2025.

BOTTA, A.; DONATO, W. D.; PERSICO, V.; PESCAPÉ, A. Integration of cloud computing and internet of things: a survey. **Future generation computer systems**, Elsevier, v. 56, p. 684–700, 2016. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0167739X15003015?casa_token=WlGAI7DPWfQAAAAA:bsh5hxEb9Jy98DckbzAI17rMCJXq_6cKVaEjGxv0fC41n053kCI0fGHyDnEvSKJLE7aJtyFCu0A>. Acesso em: 23 jan. 2025.

BOUZAACHANE, K.; GUARMAH, E. M. E.; ALNAJIM, A. M.; KHAN, S. Addressing modern cybersecurity challenges: A hybrid machine learning and deep learning approach for network intrusion detection. **Computers, Materials & Continua**, v. 84, n. 2, 2025. Disponível em: <https://www.sciencedirect.com/org/science/article/pii/S1546221825006083>. Acesso em: 15 dez. 2025.

CAPUANO, N.; FENZA, G.; LOIA, V.; STANZIONE, C. Explainable artificial intelligence in cybersecurity: A survey. **IEEE Access**, v. 10, p. 93575–93600, 2022. Disponível em: <https://ieeexplore.ieee.org/document/9877919>. Acesso em: 16 jan. 2025.

CENTENARO, M.; VANGELISTA, L.; ZANELLA, A.; ZORZI, M. Long-range communications in unlicensed bands: The rising stars in the iot and smart city scenarios. **IEEE Wireless Communications**, IEEE, v. 23, n. 5, p. 60–67, 2016. Disponível em: <https://ieeexplore.ieee.org/abstract/document/7721743/?casa_token=RJtjLoJOgtAAAAAA:IaA7XDXzTXcYPKeUpq-4kDxtJ-F-El12TAIk1x8-q_ob_lNs5R_q2Nt50dO2Vwp1pI5CtwlaCBY>. Acesso em: 23 jan. 2025.

CHEN, Z.; SIMSEK, M.; KANTARCI, B.; BAGHERI, M.; DJUKIC, P. Machine learning-enabled hybrid intrusion detection system with host data transformation and an advanced two-stage classifier. **Computer Networks**, Elsevier, v. 250, p. 110576, 2024. Disponível em: <https://www.sciencedirect.com/science/article/pii/S1389128624004080>. Acesso em: 15 dez. 2025.

CHIANG, M.; ZHANG, T. Fog and iot: An overview of research opportunities. **IEEE Internet of things journal**, IEEE, v. 3, n. 6, p. 854–864, 2016. Disponível em: <https://ieeexplore.ieee.org/abstract/document/7498684/?casa_token=B1QOk1OSpygAAAAA:u3H32G2Q8MGI5O2E0uY8WTqVR-0vvac7sXVL-oXFkJkp876YXgK5P5zxgslzXpXUe1jX6nitn4A>. Acesso em: 23 jan. 2025.

DAVIES, T.; EIZA, M. H.; SHONE, N.; LYON, R. A collaborative intrusion detection system using snort ids nodes. **arXiv preprint arXiv:2504.16550**, 2025. Disponível em: <https://arxiv.org/abs/2504.16550>. Acesso em: 21 jan. 2025.

DEMERTZI, V.; DEMERTZIS, S.; DEMERTZIS, K. An overview of privacy dimensions on the industrial internet of things (iiot). **Algorithms**, MDPI, v. 16, n. 8, p. 378, 2023. Disponível em: <https://www.mdpi.com/1999-4893/16/8/378>. Acesso em: 17 jan. 2025.

DEVINE, M.; ARDAKANI, S. P.; AL-KHAFAJIY, M.; JAMES, Y. Federated machine learning to enable intrusion detection systems in iot networks. **Electronics**, MDPI, v. 14, n. 6, p. 1176, 2025. Disponível em: <https://www.mdpi.com/2079-9292/14/6/1176>. Acesso em: 10 dez. 2025.

DIAN, F. J. **Fundamentals of Internet of Things: For Students and Professionals**. John Wiley & Sons, 2022. Disponível em: <https://books.google.com/books?hl=pt-BR&lr=&id=GrObEAAAQBAJ&oi=fnd&pg=PR16&dq=Fundamentals+of+Internet+of+Things:+For+Students+and+Professionals&ots=r99ulKaq0I&sig=hPrjWVLIRKpeiqfJx-HIAfsqcPo>. Acesso em: 21 jan. 2025.

DJENOURI, Y.; BELHADI, A.; SRIVASTAVA, G.; LIN, J. C.-W.; YAZIDI, A. Interpretable intrusion detection for next generation of internet of things. **Computer Communications**, v. 203, p. 192–198, 2023. ISSN 0140-3664. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0140366423000841>. Acesso em: 15 dez. 2025.

DOGHRAMACHI, D. F.; AMEEN, S. Y. Internet of things (iot) security enhancement using xgboost machine learning techniques. **Computers, Materials & Continua**, v. 77, n. 1, 2023. Disponível em: <https://www.sciencedirect.com/org/science/article/pii/S1546221823001091>. Acesso em: 15 dez. 2025.

EL-SHAFEIY, E.; ELSAYED, W. M.; ELWAHSH, H.; ALSABAAN, M.; IBRAHEM, M. I.; ELHADY, G. F. Deep complex gated recurrent networks-based iot network

intrusion detection systems. **Sensors**, MDPI, v. 24, n. 18, p. 5933, 2024. Disponível em: <https://www.mdpi.com/1424-8220/24/18/5933>. Acesso em: 17 jan. 2025.

ELSAYED, R. A.; HAMADA, R. A.; ABDALLA, M. I.; ELSAID, S. A. Securing iot and sdn systems using deep-learning based automatic intrusion detection. **Ain Shams Engineering Journal**, Elsevier, v. 14, n. 10, p. 102211, 2023. Disponível em: <https://www.sciencedirect.com/science/article/pii/S2090447923001004>. Acesso em: 15 dez. 2025.

ESMAEILI, M.; RAHIMI, M.; PISHDAST, H.; FARAHMANDAZAD, D.; KHAJAVI, M.; SARAY, H. J. Machine learning-assisted intrusion detection for enhancing internet of things security. **arXiv preprint arXiv:2410.01016**, 2024. Disponível em: <https://arxiv.org/abs/2410.01016>. Acesso em: 15 dez. 2025.

FARES, I. A.; ELAZIZ, M. A.; ASEERI, A. O.; ZIED, H. S.; ABDELLATIF, A. G. Tfkan: transformer based on kolmogorov–arnold networks for intrusion detection in iot environment. **Egyptian Informatics Journal**, Elsevier, v. 30, p. 100666, 2025. Disponível em: <https://www.sciencedirect.com/science/article/pii/S1110866525000593>. Acesso em: 15 dez. 2025.

FAROOQ, M. S.; SALEEM, M.; KHAN, M.; KHAN, M. F.; SIDDIQUI, S. Y.; ASLAM, M. S.; ADNAN, K. M. Interpretable federated learning model for cyber intrusion detection in smart cities with privacy-preserving feature selection. **Computers, Materials and Continua**, v. 85, n. 3, p. 5183–5206, 2025. Disponível em: <https://www.sciencedirect.com/org/science/article/pii/S1546221825009683>. Acesso em: 15 dez. 2025.

FERRAG, M. A.; FRIHA, O.; KANTARCI, B.; TIHANYI, N.; CORDEIRO, L.; DEBBAH, M.; HAMOUDA, D.; AL-HAWAWREH, M.; CHOO, K.-K. R. Edge learning for 6g-enabled internet of things: A comprehensive survey of vulnerabilities, datasets, and defenses. **IEEE Communications Surveys Tutorials**, v. 25, n. 4, p. 2654–2713, 2023. Disponível em: <https://ieeexplore.ieee.org/document/10255264>. Acesso em: 16 jan. 2025.

FRANCO, A. d. O. d. R. Adaptação automática de histórias para rpgs não-lineares: uma abordagem com inteligência artificial generativa e otimização evolutiva. 2025. Disponível em: <https://repositorio.ufc.br/handle/riufc/83270>. Acesso em: 21 jan. 2025.

FRANCO, A. d. O. da R.; CARVALHO, W. V. de; SILVA, J. W. F. da; MAIA, J. G. R.; CASTRO, M. F. de. Managing and controlling digital role-playing game elements: A current state of affairs. **Entertainment Computing**, Elsevier, v. 51, p. 100708, 2024. Disponível em: <https://www.sciencedirect.com/science/article/pii/S1875952124000764?casa_token=5pWMVUeN7bcAAAAA:oqlS9DMJOicnYk867_wNx0tnRpgYn_FwZlECrS1IzGyap0fCnDd7BgK9Wb5JLV9RQ2htU1XhdDI>. Acesso em: 21 jan. 2025.

FU, S.; XU, H.; ALI, A.; SAJID, S. Prifed-ids: A privacy-preserving federated reinforcement learning framework for secure and intelligent intrusion detection in digital health systems. **Electronics**, MDPI, v. 14, n. 23, p. 4590, 2025. Disponível em: <https://www.mdpi.com/2079-9292/14/23/4590>. Acesso em: 10 dez. 2025.

GAD, A. R.; HAGGAG, M.; NASHAT, A. A.; BARAKAT, T. M. A distributed intrusion detection system using machine learning for iot based on ton-iot dataset. **International**

Journal of Advanced Computer Science and Applications, Science and Information (SAI) Organization Limited, v. 13, n. 6, 2022. Disponível em: <https://www.researchgate.net/profile/Abdallah-Gad-7/publication/361669587_A_Distributed_Intrusion_Detection_System_using_Machine_Learning_for_IoT_based_on_ToN-IoT_Dataset/links/62bf036dc0556f0d63146a5c/A-Distributed-Intrusion-Detection-System-using-Machine-Learning-for-IoT-based-on-ToN-IoT-Dataset.pdf>. Acesso em: 22 jan. 2025.

GAINA, L.; STANGACIU, C. S.; STANESCU, D.; GUSITA, B.; MICEA, M. V. Unidirectional communications in secure iot systems—a survey. **Sensors**, MDPI, v. 24, n. 23, p. 7528, 2024. Disponível em: <https://www.mdpi.com/1424-8220/24/23/7528>. Acesso em: 17 jan. 2025.

GHENI, H. Q.; AL-YASEEN, W. L. Two-step data clustering for improved intrusion detection system using ciciot2023 dataset. **e-Prime-Advances in Electrical Engineering, Electronics and Energy**, Elsevier, v. 9, p. 100673, 2024. Disponível em: <https://www.sciencedirect.com/science/article/pii/S2772671124002535>. Acesso em: 15 dez. 2025.

GOYAL, S.; RAJAWAT, A. S.; SOLANKI, R. K.; ZAABA, M. A. M.; LONG, Z. A. Integrating ai with cyber security for smart industry 4.0 application. In: **2023 International Conference on Inventive Computation Technologies (ICICT)**. [s.n.], 2023. p. 1223–1232. Disponível em: <https://ieeexplore.ieee.org/document/10134374>. Acesso em: 16 jan. 2025.

GUBBI, J.; BUYYA, R.; MARUSIC, S.; PALANISWAMI, M. Internet of things (iot): A vision, architectural elements, and future directions. **Future generation computer systems**, Elsevier, v. 29, n. 7, p. 1645–1660, 2013. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0167739X13000241?casa_token=k7dvRym9SAcAAAAA:mc_9DtbSwUBk8xWd3RUg3mD7YB-5FZ1vyjkq27wQOs-1tajuMlnMrNgwAjHBKE-F_w8QOKVMGqc>. Acesso em: 23 jan. 2025.

GUPTA, C.; JOHRI, I.; SRINIVASAN, K.; HU, Y.-C.; QAISAR, S. M.; HUANG, K.-Y. A systematic review on machine learning and deep learning models for electronic information security in mobile networks. **Sensors**, MDPI, v. 22, n. 5, p. 2017, 2022. Disponível em: <https://www.mdpi.com/1424-8220/22/5/2017>. Acesso em: 21 jan. 2025.

HAFID, A.; RAHOUTI, M.; ALEDHARI, M. Optimizing intrusion detection in iomt networks through interpretable and cost-aware machine learning. **Mathematics**, MDPI, v. 13, n. 10, p. 1574, 2025. Disponível em: <https://www.mdpi.com/2227-7390/13/10/1574>. Acesso em: 10 dez. 2025.

HAGHIGHI, M. S.; FARIVAR, F.; JOLFAEI, A. A machine-learning-based approach to build zero-false-positive ipss for industrial iot and cps with a case study on power grids security. **IEEE Transactions on Industry Applications**, v. 60, n. 1, p. 920–928, 2024. Disponível em: <https://ieeexplore.ieee.org/document/9146688>. Acesso em: 16 jan. 2025.

HANIF, A. A.; ILYAS, M. Effective feature engineering framework for securing mqtt protocol in iot environments. **Sensors**, MDPI, v. 24, n. 6, p. 1782, 2024. Disponível em: <https://www.mdpi.com/1424-8220/24/6/1782>. Acesso em: 10 dez. 2025.

HASAN, T.; TASNIM, S. Multidimensional feature learning enhancement in iot intrusion detection: An adaptive cost-sensitive autoencoder and weighted ensemble approach. In: **2024 IEEE 10th World Forum on Internet of Things (WF-IoT)**. [s.n.], 2024. p. 536–541. Disponível em: <https://ieeexplore.ieee.org/document/10811174>. Acesso em: 9 dez. 2025.

HASSAN, M. B.; ALI, E. S.; MOKHTAR, R. A.; SAEED, R. A.; CHAUDHARI, B. S. Nb-iot: Concepts, applications, and deployment challenges. In: **LPWAN Technologies for IoT and M2M Applications**. Elsevier, 2020. p. 119–144. Disponível em: <https://www.sciencedirect.com/science/article/pii/B9780128188804000065>. Acesso em: 23 jan. 2025.

HIRSI, A.; AUDAH, L.; SALH, A.; ALHARTOMI, M. A.; AHMED, S. Detecting ddos threats using supervised machine learning for traffic classification in software defined networking. **IEEE Access**, v. 12, p. 166675–166702, 2024. Disponível em: <https://ieeexplore.ieee.org/document/10734092>. Acesso em: 16 jan. 2025.

HOSSAIN, M. S.; ISLAM, M. S.; RAHMAN, M. A. A cyber range framework for emulating secure and private it/ot consumer service verticals toward 6g. **IEEE Transactions on Consumer Electronics**, v. 70, n. 2, p. 4709–4716, 2024. Disponível em: <https://ieeexplore.ieee.org/document/10496463>. Acesso em: 16 jan. 2025.

HOSSAIN, M. Z.; IMTEAJ, A.; ZAMAN, S.; SHAHID, A. R.; TALUKDER, S.; AMINI, M. H. Flid: Intrusion attack and defense mechanism for federated learning empowered connected autonomous vehicles (cavs) application. In: **2023 IEEE Conference on Dependable and Secure Computing (DSC)**. [s.n.], 2023. p. 1–8. Disponível em: <https://ieeexplore.ieee.org/document/10354149>. Acesso em: 16 jan. 2025.

HOUDA, Z. A. E.; BRIK, B.; KHOUKHI, L. "why should i trust your ids?": An explainable deep learning framework for intrusion detection systems in internet of things networks. **IEEE Open Journal of the Communications Society**, v. 3, p. 1164–1176, 2022. Disponível em: <https://ieeexplore.ieee.org/abstract/document/9825734/>. Acesso em: 21 jan. 2025.

HOUICHI, M.; JAIDI, F.; BOUHOULA, A. Cyber security within smart cities: A comprehensive study and a novel intrusion detection-based approach. **Computers, Materials & Continua**, v. 81, n. 1, 2024. Disponível em: <https://www.sciencedirect.com/org/science/article/pii/S1546221824007240>. Acesso em: 15 dez. 2025.

ISLAM, M. M.; ABDULLAH, W. M.; SAHA, B. N. Privacy-preserving hierarchical fog federated learning (pp-hffl) for iot intrusion detection. **Sensors (Basel, Switzerland)**, v. 25, n. 23, p. 7296, 2025. Disponível em: <https://www.mdpi.com/1424-8220/25/23/7296>. Acesso em: 10 dez. 2025.

JAAFOURI, L.; ET-TOLBA, M.; HANIN, C.; LAHSEN-CHERIF, I. Iot network security: Ensemble-based approaches for anomaly detection. In: **2025 International Conference on Circuit, Systems and Communication (ICCSC)**. [s.n.], 2025. p. 1–6. Disponível em: <https://ieeexplore.ieee.org/document/11135113>. Acesso em: 9 dez. 2025.

JADIDI, Z.; PAL, S.; K, N. N.; SELVAKKUMAR, A.; CHANG, C.-C.; BEHESHTI, M.; JOLFAEI, A. Security of machine learning-based anomaly detection in cyber physical systems. In: **2022 International Conference on Computer Communications and Networks (ICCCN)**. [s.n.], 2022. p. 1–7. Disponível em: <https://ieeexplore.ieee.org/document/9868845>. Acesso em: 16 jan. 2025.

JAMSHIDI, S.; NIKANJAM, A.; WAZED, N. K.; KHOMH, F. Leveraging machine learning techniques in intrusion detection systems for internet of things. **arXiv preprint arXiv:2504.07220**, 2025. Disponível em: <https://arxiv.org/abs/2504.07220>. Acesso em: 15 dez. 2025.

JANIESCH, C.; ZSCHECH, P.; HEINRICH, K. Machine learning and deep learning. **Electronic Markets**, Springer Science and Business Media LLC, v. 31, n. 3, p. 685–695, abr. 2021. ISSN 1422-8890. Disponível em: <http://dx.doi.org/10.1007/s12525-021-00475-2>. Acesso em: 21 jan. 2025.

JOHANESA, T. V. A.; EQUETER, L.; MAHMOUDI, S. A. Survey on ai applications for product quality control and predictive maintenance in industry 4.0. **Electronics**, MDPI, v. 13, n. 5, p. 976, 2024. Disponível em: <https://www.mdpi.com/2079-9292/13/5/976>. Acesso em: 21 jan. 2025.

JOHNSTONE, J.; AKINFADERIN, A. Mapping cyber threats in iot-driven msps: An explainable machine learning approach for remote work security. In: **2025 IEEE 4th International Conference on AI in Cybersecurity (ICAIC)**. [s.n.], 2025. p. 1–9. Disponível em: <https://ieeexplore.ieee.org/document/10848740>. Acesso em: 9 dez. 2025.

KANG, M.; PARK, S.; LEE, Y. A survey on satellite communication system security. **Sensors**, MDPI, v. 24, n. 9, p. 2897, 2024. Disponível em: <https://www.mdpi.com/1424-8220/24/9/2897>. Acesso em: 17 jan. 2025.

KANNADHASAN, S.; NAGARAJAN, R. Intrusion detection in machine learning based e-shaped structure with algorithms, strategies and applications in wireless sensor networks. **Heliyon**, v. 10, n. 9, p. e30675, 2024. ISSN 2405-8440. Acesso em: 15 dez. 2025.

KAREEM, S. W. Enhanced intrusion detection system using hybrid-inspired algorithms and conditional generative adversarial networks for internet of things security. **Egyptian Informatics Journal**, Elsevier, v. 31, p. 100763, 2025. Disponível em: <https://www.sciencedirect.com/science/article/pii/S1110866525001562>. Acesso em: 15 dez. 2025.

KESHK, M.; KORONIOTIS, N.; PHAM, N.; MOUSTAFA, N.; TURNBULL, B.; ZOMAYA, A. Y. An explainable deep learning-enabled intrusion detection framework in iot networks. **Information Sciences**, Elsevier, v. 639, p. 119000, 2023. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0020025523005856>. Acesso em: 15 dez. 2025.

KHAN, A. R.; KASHIF, M.; JHAVERI, R. H.; RAUT, R.; SABA, T.; BAHAJ, S. A. Deep learning for intrusion detection and security of internet of things (iot): current analysis, challenges, and possible solutions. **Security and Communication Networks**, Wiley Online Library, v. 2022, n. 1, p. 4016073, 2022. Disponível em: <https://onlinelibrary.wiley.com/doi/abs/10.1155/2022/4016073>. Acesso em: 21 jan. 2025.

KIM, J.; PARK, S.; CHA, J.; SON, E.; SON, Y. Novel synthetic dataset generation method with privacy-preserving for intrusion detection system. **Applied Sciences**, MDPI, v. 15, n. 19, p. 10609, 2025. Disponível em: <https://www.mdpi.com/2076-3417/15/19/10609>. Acesso em: 10 dez. 2025.

KUMAR, S. S.; SELVI, M.; KANNAN, A. A comprehensive survey on machine learning-based intrusion detection systems for secure communication in internet of things. **Computational Intelligence and Neuroscience**, Wiley Online Library, v. 2023, n. 1, p. 8981988, 2023. Disponível em: <https://onlinelibrary.wiley.com/doi/abs/10.1155/2023/8981988>. Acesso em: 22 jan. 2025.

LARRIVA-NOVO, X.; MIGUEL, L. P.; VILLAGRA, V. A.; ÁLVAREZ-CAMPANA, M.; SANCHEZ-ZAS, C.; JOVER, Ó. Post-hoc categorization based on explainable ai and reinforcement learning for improved intrusion detection. **Applied Sciences**, MDPI, v. 14, n. 24, p. 11511, 2024. Disponível em: <https://www.mdpi.com/2076-3417/14/24/11511>. Acesso em: 17 jan. 2025.

MAHMOUD, W. A.; FATHI, M.; EL-BADAWY, H.; SADEK, R. Performance analysis of ids$_m$*dlalgorithmtopredictintrusiondetectionforiotapplications.In* : **2023 40th National Radio Science C** $-149.$*Disponvelem* : <>. Acesso em: 16 jan. 2025.

MANGLIK, R.; EXPERTS, E.; COMMUNITY, E. **Intrusion Detection Systems**. EduGorilla Publication, 2024. ISBN 9789368178057. Disponível em: <https://books.google.com.br/books?id=mA08EQAAQBAJ>. Acesso em: 21 jan. 2025.

MANI, V.; VIVEKANANDAN, P. Dip-dark: A smart and innovative classifier for enhanced intrusion detection and security in heterogeneous iot networks. **Ain Shams Engineering Journal**, Elsevier, v. 16, n. 11, p. 103692, 2025. Disponível em: <https://www.sciencedirect.com/science/article/pii/S2090447925004332>. Acesso em: 15 dez. 2025.

MANYIKA, J.; CHUI, M.; BISSON, P.; WOETZEL, J.; DOBBS, R.; BUGHIN, J.; AHARON, D. Unlocking the potential of the internet of things. **McKinsey Global Institute**, v. 1, p. 1–2, 2015. Disponível em: <http://aegex.com/images/uploads/white_papers/Unlocking_the_potential_of_the_Internet_of_Things___McKinsey__Company.pdf>. Acesso em: 21 jan. 2025.

MARTÍNEZ, A. L.; PÉREZ, M. G.; RUIZ-MARTÍNEZ, A. A comprehensive review of the state-of-the-art on security and privacy issues in healthcare. **ACM Computing Surveys**, ACM New York, NY, USA, v. 55, n. 12, p. 1–38, 2023. Disponível em: <https://dl.acm.org/doi/10.1145/3571156>. Acesso em: 18 jan. 2025.

MCINTOSH, T.; SUSNJAK, T.; LIU, T.; XU, D.; WATTERS, P.; LIU, D.; HAO, Y.; NG, A.; HALGAMUGE, M. Ransomware reloaded: Re-examining its trend, research and mitigation in the era of data exfiltration. **ACM Computing Surveys**, ACM New York, NY, v. 57, n. 1, p. 1–40, 2024. Disponível em: <https://dl.acm.org/doi/10.1145/3691340>. Acesso em: 18 jan. 2025.

MÉDARD, K. B.; BAKARY, B. A.; AYIKPA, K. J.; DIARRA, M.; JÉRÔME, C. M. Z. Top-k feature selection for iot intrusion detection: Contributions of xgboost, lightgbm, and random forest. **Future Internet**, MDPI AG, v. 17, n. 11, p. 529, 2025. Disponível em: <https://www.mdpi.com/1999-5903/17/11/529>. Acesso em: 10 dez. 2025.

MESA, M. V. C.; PATINO-RODRIGUEZ, C. E.; CARAZAS, F. J. G. Cybersecurity at sea: A literature review of cyber-attack impacts and defenses in maritime supply chains. **Information**, MDPI, v. 15, n. 11, p. 710, 2024. Disponível em: <https://www.mdpi.com/2078-2489/15/11/710>. Acesso em: 17 jan. 2025.

MIORANDI, D.; SICARI, S.; PELLEGRINI, F. D.; CHLAMTAC, I. Internet of things: Vision, applications and research challenges. **Ad hoc networks**, Elsevier, v. 10, n. 7, p. 1497–1516, 2012. Disponível em: <https://www.sciencedirect.com/science/article/pii/S1570870512000674?casa_token=S_UEr0q7s9YAAAAA:DYbIWikNauum3NM5JLq6eojk4ucbYGBw9VjrgiFbE40RAnezUzAAgfLC4 Acesso em: 23 jan. 2025.

MOHANTY, S.; CHATTERJEE, J.; SATPATHY, S. **Internet of Things and Its Applications**. Springer International Publishing, 2021. (EAI/Springer Innovations in Communication and Computing). ISBN 9783030775285. Disponível em: <https://books.google.com.br/books?id=KjNREAAAQBAJ>. Acesso em: 21 jan. 2025.

MORETTIN, P. A.; TOLOI, C. M. **Análise de séries temporais: modelos lineares univariados**. Editora Blucher, 2018. Disponível em: <https://books.google.com/books?hl=pt-BR&lr=&id=UwC5DwAAQBAJ&oi=fnd&pg=PA1&dq=Analise+de+series+temporais:+modelos+lineares+univariados&ots=l-JojZ3MV0&sig=0E9XvdMOU5YgQShxGwFP5JZOcPk>. Acesso em: 21 jan. 2025.

MOUSTAFA, N.; KORONIOTIS, N.; KESHK, M.; ZOMAYA, A. Y.; TARI, Z. Explainable intrusion detection for cyber defences in the internet of things: Opportunities and solutions. **IEEE Communications Surveys Tutorials**, v. 25, n. 3, p. 1775–1807, 2023. Disponível em: <https://ieeexplore.ieee.org/document/10136827>. Acesso em: 16 jan. 2025.

MUKHAMEDIEV, R. I.; POPOVA, Y.; KUCHIN, Y.; ZAITSEVA, E.; KALIMOLDAYEV, A.; SYMAGULOV, A.; LEVASHENKO, V.; ABDOLDINA, F.; GOPEJENKO, V.; YAKUNIN, K. *et al.* Review of artificial intelligence and machine learning technologies: classification, restrictions, opportunities and challenges. **Mathematics**, MDPI, v. 10, n. 15, p. 2552, 2022. Disponível em: <https://www.mdpi.com/2227-7390/10/15/2552>. Acesso em: 21 jan. 2025.

MUNAWEERA, P.; PRASAD, S.; HEWA, T.; SIRIWARDHANA, Y.; YLIANTTILA, M. Federated learning-powered ddos attack detection for securing cyber physical systems in 5g and beyond networks. In: **Proceedings of the 14th International Conference on the Internet of**

Things. [s.n.], 2024. p. 273–278. Disponível em: <https://dl.acm.org/doi/10.1145/3703790.3703822>. Acesso em: 12 dez. 2025.

MUTAMBIK, I. An efficient flow-based anomaly detection system for enhanced security in iot networks. **Sensors**, MDPI, v. 24, n. 22, p. 7408, 2024. Disponível em: <https://www.mdpi.com/1424-8220/24/22/7408>. Acesso em: 10 dez. 2025.

NARAYAN, K. R.; MOOKHERJI, S.; ODELU, V.; PRASATH, R.; TURLAPATY, A. C.; DAS, A. K. Iids: Design of intelligent intrusion detection system for internet-of-things applications. In: **2023 IEEE 7th Conference on Information and Communication Technology (CICT)**. [s.n.], 2023. p. 1–6. Disponível em: <https://ieeexplore.ieee.org/abstract/document/10455720/?casa_token=FRHHhjRxmJsAAAAA:ZVlDNKsBhrtRZvHCQSn3zhbUcm9uh0GM5oZh3Qk5rCK9Vpju8iaRbDol Acesso em: 22 jan. 2025.

NGO, T.; YIN, J.; GE, Y.-F.; WANG, H. Optimizing iot intrusion detection—a graph neural network approach with attribute-based graph construction. **Information**, MDPI, v. 16, n. 6, p. 499, 2025. Disponível em: <https://www.mdpi.com/2078-2489/16/6/499>. Acesso em: 10 dez. 2025.

NIMMALA, R. Enhancing financial risk management: Utilizing machine learning in climate risk model benchmarking. **Journal of Mathematical & Computer Applications. SRC/JMCA-178. DOI: doi. org/10.47363/JMCA/2023 (2)**, v. 146, p. 2–4, 2023. Disponível em: <https://www.researchgate.net/profile/Rohit-Nimmala/publication/380387993_Enhancing_Financial_Risk_Management_Utilizing_Machine_Learning_in_Climate_Risk_Model_Benchmarking/links/66f6305a9e6e82486ff36466/Enhancing-Financial-Risk-Management-Utilizing-Machine-Learning-in-Climate-Risk-Model-Benchmarkin pdf>. Acesso em: 21 jan. 2025.

ORMAN, A. Cyberattack detection systems in industrial internet of things (iiot) networks in big data environments. **Applied Sciences**, MDPI, v. 15, n. 6, p. 3121, 2025. Disponível em: <https://www.mdpi.com/2076-3417/15/6/3121>. Acesso em: 10 dez. 2025.

OZTOPRAK, A.; HASSANPOUR, R.; OZKAN, A.; OZTOPRAK, K. Security challenges, mitigation strategies, and future trends in wireless sensor networks: A review. **ACM Computing Surveys**, ACM New York, NY, v. 57, n. 4, p. 1–29, 2024. Disponível em: <https://dl.acm.org/doi/10.1145/3706583>. Acesso em: 18 jan. 2025.

QUAN, W.; XU, Z.; LIU, M.; CHENG, N.; LIU, G.; GAO, D.; ZHANG, H.; SHEN, X.; ZHUANG, W. Ai-driven packet forwarding with programmable data plane: A survey. **IEEE**

Communications Surveys Tutorials, v. 25, n. 1, p. 762–790, 2023. Disponível em: <https://ieeexplore.ieee.org/document/9931326>. Acesso em: 16 jan. 2025.

QURESHI, S. S.; HE, J.; QURESHI, S. U.; ZHU, N.; WAJAHAT, A.; NAZIR, A.; ULLAH, F.; WADUD, A. Advanced ai-driven intrusion detection for securing cloud-based industrial iot. **Egyptian Informatics Journal**, Elsevier, v. 30, p. 100644, 2025. Disponível em: <https://www.sciencedirect.com/science/article/pii/S1110866525000374>. Acesso em: 15 dez. 2025.

RADOGLOU-GRAMMATIKIS, P.; KIOSEOGLOU, E.; ASIMOPOULOS, D.; SIAVVAS, M.; NANOS, I.; LAGKAS, T.; ARGYRIOU, V.; PSANNIS, K. E.; GOUDOS, S.; SARIGIANNIDIS, P. Surveying cyber threat intelligence and collaboration: A concise analysis of current landscape and trends. In: **2023 IEEE International Conference on Cloud Computing Technology and Science (CloudCom)**. [s.n.], 2023. p. 309–314. Disponível em: <https://ieeexplore.ieee.org/document/10475684>. Acesso em: 16 jan. 2025.

RAIMUNDO, R. J.; ROSÁRIO, A. T. Cybersecurity in the internet of things in industrial management. **Applied Sciences**, MDPI, v. 12, n. 3, p. 1598, 2022. Disponível em: <https://www.mdpi.com/2076-3417/12/3/1598>. Acesso em: 17 jan. 2025.

RAMEZANI, M.; TAKIAN, A.; BAKHTIARI, A.; RABIEE, H. R.; FAZAELI, A. A.; SAZGARNEJAD, S. The application of artificial intelligence in health financing: a scoping review. **Cost Effectiveness and Resource Allocation**, Springer, v. 21, n. 1, p. 83, 2023. Disponível em: <https://link.springer.com/article/10.1186/s12962-023-00492-2>. Acesso em: 21 jan. 2025.

RAMPONE, G.; IVANIV, T.; RAMPONE, S. A hybrid federated learning framework for privacy-preserving near-real-time intrusion detection in iot environments. **Electronics**, MDPI, v. 14, n. 7, p. 1430, 2025. Disponível em: <https://www.mdpi.com/2079-9292/14/7/1430>. Acesso em: 10 dez. 2025.

RAVIKUMAR, K.; CHIRANJEEVI, P.; DEVARAJAN, N. M.; KAUR, C.; TALOBA, A. I. Challenges in internet of things towards the security using deep learning techniques. **Measurement: Sensors**, Elsevier, v. 24, p. 100473, 2022. Disponível em: <https://www.sciencedirect.com/science/article/pii/S2665917422001076>. Acesso em: 21 jan. 2025.

REHMAN, E.; DIN, M. Haseeb-ud; MALIK, A. J.; KHAN, T. K.; ABBASI, A. A.; KADRY, S.; KHAN, M. A.; RHO, S. Intrusion detection based on machine learning in the internet of things, attacks and counter measures. **The Journal of Supercomputing**, Springer, p. 1–35, 2022. Disponível em: <https://idp.springer.com/authorize/casa?redirect_uri=https://link.springer.com/article/

10.1007/s11227-021-04188-3&casa_token=rOW8H32cqD4AAAAA:0rB2jV8x5aPbN8y9oYKb55Ax1F6db
Acesso em: 21 jan. 2025.

RJOUB, G.; BENTAHAR, J.; WAHAB, O. A.; MIZOUNI, R.; SONG, A.; COHEN, R.; OTROK, H.; MOURAD, A. A survey on explainable artificial intelligence for cybersecurity. **IEEE Transactions on Network and Service Management**, v. 20, n. 4, p. 5115–5140, 2023. Disponível em: <https://ieeexplore.ieee.org/document/10143992>. Acesso em: 16 jan. 2025.

S, B.; N, M.; G, G.; T, A.; T, S.; G, V. Hybrid intrusion detection system for iot against adversarial threats using intelligent rdls model. In: **2024 5th International Conference on Data Intelligence and Cognitive Informatics (ICDICI)**. [s.n.], 2024. p. 172–179. Disponível em: <https://ieeexplore.ieee.org/document/10810937>. Acesso em: 9 dez. 2025.

SAINI, H.; BALA, S.; IDA, S.; KUMAR, K. S.; SWETHA, S.; P, D. Machine learning approach for mitigating security threats in iot environment. In: **2023 5th International Conference on Inventive Research in Computing Applications (ICIRCA)**. [s.n.], 2023. p. 1398–1405. Disponível em: <https://ieeexplore.ieee.org/document/10220759>. Acesso em: 16 jan. 2025.

SAMONTE, M. J. C.; GOC-ONG, A. E.; MATOZA, R. B. F.; VIERNES, R. G. A. Evaluating the effectiveness of artificial intelligence in integrated system architectures to combat cybersecurity threats. In: **2024 IEEE 7th International Conference on Computer and Communication Engineering Technology (CCET)**. [s.n.], 2024. p. 222–226. Disponível em: <https://ieeexplore.ieee.org/document/10838195>. Acesso em: 16 jan. 2025.

SATTARPOUR, S.; BARATI, A.; BARATI, H. An intrusion detection system in internet of things using grasshopper optimization algorithm and machine learning algorithms. **arXiv preprint arXiv:2509.01724**, 2025. Disponível em: <https://arxiv.org/abs/2509.01724>. Acesso em: 15 dez. 2025.

SAYADI, H.; ALIASGARI, M.; AYDIN, F.; POTLURI, S.; AYSU, A.; EDMONDS, J.; TEHRANIPOOR, S. Towards ai-enabled hardware security: Challenges and opportunities. In: **2022 IEEE 28th International Symposium on On-Line Testing and Robust System Design (IOLTS)**. [s.n.], 2022. p. 1–10. Disponível em: <https://ieeexplore.ieee.org/document/9897507>. Acesso em: 16 jan. 2025.

SAYADI, H.; HE, Z.; MAKRANI, H. M.; HOMAYOUN, H. Intelligent malware detection based on hardware performance counters: A comprehensive survey. In: **2024 25th International**

Symposium on Quality Electronic Design (ISQED). [s.n.], 2024. p. 1–10. Disponível em: <https://ieeexplore.ieee.org/document/10528369>. Acesso em: 16 jan. 2025.

SCHMITT, M. Securing the digital world: Protecting smart infrastructures and digital industries with artificial intelligence (ai)-enabled malware and intrusion detection. **Journal of Industrial Information Integration**, Elsevier, v. 36, p. 100520, 2023. Disponível em: <https://www.sciencedirect.com/science/article/pii/S2452414X23000936>. Acesso em: 15 dez. 2025.

SERRANO, W. Cyberaibot: Artificial intelligence in an intrusion detection system for cybersecurity in the iot. **Future Generation Computer Systems**, Elsevier, v. 166, p. 107543, 2025. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0167739X24005077>. Acesso em: 15 dez. 2025.

SEYEDI, B.; POSTOLACHE, O. Securing iot communications via anomaly traffic detection: Synergy of genetic algorithm and ensemble method. **Sensors**, MDPI, v. 25, n. 13, p. 4098, 2025. Disponível em: <https://www.mdpi.com/1424-8220/25/13/4098>. Acesso em: 10 dez. 2025.

SEZGIN, A.; BOYACI, A. Aid4i: An intrusion detection framework for industrial internet of things using automated machine learning. **Computers, Materials & Continua**, v. 76, n. 2, 2023. Disponível em: <https://www.sciencedirect.com/org/science/article/pii/S1546221823001583>. Acesso em: 15 dez. 2025.

SHAFIQ, M.; GU, Z.; CHEIKHROUHOU, O.; ALHAKAMI, W.; HAMAM, H. The rise of "internet of things": Review and open research issues related to detection and prevention of iot-based security attacks. **Wireless Communications and Mobile Computing**, Wiley Online Library, v. 2022, n. 1, p. 8669348, 2022. Disponível em: <https://onlinelibrary.wiley.com/doi/abs/10.1155/2022/8669348>. Acesso em: 21 jan. 2025.

SHARMA, P.; DASH, B. Impact of big data analytics and chatgpt on cybersecurity. In: **2023 4th International Conference on Computing and Communication Systems (I3CS)**. [s.n.], 2023. p. 1–6. Disponível em: <https://ieeexplore.ieee.org/document/10127411>. Acesso em: 16 jan. 2025.

SHI, W.; CAO, J.; ZHANG, Q.; LI, Y.; XU, L. Edge computing: Vision and challenges. **IEEE internet of things journal**, Ieee, v. 3, n. 5, p. 637–646, 2016. Disponível em: <https://ieeexplore.ieee.org/abstract/document/7488250/?casa_token=Uqo_MTFpR4cAAAAA:SlRR5QHMybfc_cQoc81UICRC
mP-u8xzxHWwpdGal6aMedvH2DK6tY0>. Acesso em: 23 jan. 2025.

SHIN, Y.; KIM, M.; KIM, H. *et al.* Towards unbalanced multiclass intrusion detection with hybrid sampling methods and ensemble classification. **Applied Soft Computing**, Elsevier, v. 157, p. 111517, 2024. Disponível em: <https://www.sciencedirect.com/science/article/pii/S1568494624002916>. Acesso em: 15 dez. 2025.

SHIRLEY, J. J.; PRIYA, M. A comprehensive survey on ensemble machine learning approaches for detection of intrusion in iot networks. In: IEEE. **2023 International Conference on Innovations in Engineering and Technology (ICIET)**. 2023. p. 1–10. Disponível em: <https://ieeexplore.ieee.org/abstract/document/10220795/>. Acesso em: 22 jan. 2025.

SI-AHMED, A.; AL-GARADI, M. A.; BOUSTIA, N. Survey of machine learning based intrusion detection methods for internet of medical things. **Applied Soft Computing**, Elsevier, v. 140, p. 110227, 2023. Disponível em: <https://arxiv.org/abs/2202.09657>. Acesso em: 15 dez. 2025.

SILVA, L. K. d. M. Avaliação eperimental do uso de agentes baseados em llms como assistentes de pesquisa científica. Universidade Federal do Rio Grande do Norte, 2025. Disponível em: <https://repositorio.ufrn.br/bitstreams/72af8ae6-1f09-4264-b67b-42a55f58bda4/download>. Acesso em: 21 jan. 2025.

SINGH, A.; KANISHKA; DUBEY, S. K. Analytical approach towards cybersecurity through ai-enabled threat intelligence. In: **2024 11th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)**. [s.n.], 2024. p. 1–6. Disponível em: <https://ieeexplore.ieee.org/document/10522422>. Acesso em: 16 jan. 2025.

SINGH, N.; BUYYA, R.; KIM, H. Securing cloud-based internet of things: challenges and mitigations. **Sensors**, MDPI, v. 25, n. 1, p. 79, 2024. Disponível em: <https://www.mdpi.com/1424-8220/25/1/79>. Acesso em: 17 jan. 2025.

SISINNI, E.; SAIFULLAH, A.; HAN, S.; JENNEHAG, U.; GIDLUND, M. Industrial internet of things: Challenges, opportunities, and directions. **IEEE transactions on industrial informatics**, IEEE, v. 14, n. 11, p. 4724–4734, 2018. Disponível em: <https://ieeexplore.ieee.org/abstract/document/8401919/?casa_token=bH0eMe_MvkIAAAAA:hCLI2FfldMJUQKVGAy32Awo-mx3Oei59NoLg
Acesso em: 23 jan. 2025.

SONG, W.; ZHU, X.; REN, S.; TAN, W.; PENG, Y. A hybrid blockchain and machine learning approach for intrusion detection system in industrial internet of things. **Alexandria Engineering**

Journal, Elsevier, v. 127, p. 619–627, 2025. Disponível em: <https://www.sciencedirect.com/science/article/pii/S1110016825006507>. Acesso em: 15 dez. 2025.

SPADACCINO, P.; CUOMO, F. Intrusion detection systems for iot: opportunities and challenges offered by edge computing and machine learning. **arXiv preprint arXiv:2012.01174**, 2020. Disponível em: <https://arxiv.org/abs/2012.01174>. Acesso em: 21 jan. 2025.

SUBASI, O.; BEL, O.; MANZANO, J.; BARKER, K. **The Landscape of Modern Machine Learning: A Review of Machine, Distributed and Federated Learning**. 2023. Disponível em: <https://arxiv.org/abs/2312.03120>. Acesso em: 21 jan. 2025.

SUKHNI, B. A.; MANNA, S. K.; DAVE, J. M.; ZHANG, L. Extracting optimal number of features for machine learning models in multilayer iot attacks. **Sensors**, MDPI, v. 24, n. 24, p. 8121, 2024. Disponível em: <https://www.mdpi.com/1424-8220/24/24/8121>. Acesso em: 10 dez. 2025.

SURYA, V.; SHANTHI, C. Cross model verification of intrusion detection system on iot using convolutional neural network. In: **2023 IEEE International Conference on ICT in Business Industry Government (ICTBIG)**. [s.n.], 2023. p. 1–12. Disponível em: <https://ieeexplore.ieee.org/document/10456135>. Acesso em: 16 jan. 2025.

TABASSUM, I.; BAZAI, S. U.; ZALAND, Z.; MARJAN, S.; KHAN, M. Z.; GHAFOOR, M. I. Cyber security's silver bullet - a systematic literature review of ai-powered security. In: **2022 3rd International Informatics and Software Engineering Conference (IISEC)**. [s.n.], 2022. p. 1–7. Disponível em: <https://ieeexplore.ieee.org/document/9998305>. Acesso em: 16 jan. 2025.

THANTHARATE, P.; T, A. Cybria - pioneering federated learning for privacy-aware cybersecurity with brilliance. In: **2023 IEEE 20th International Conference on Smart Communities: Improving Quality of Life using AI, Robotics and IoT (HONET)**. [s.n.], 2023. p. 56–61. Disponível em: <https://ieeexplore.ieee.org/document/10374608>. Acesso em: 16 jan. 2025.

THE, V. H.; KERN, D.; TAN, P. N.; KRAUSS, C. Improving anomaly detection for electric vehicle charging with generative adversarial networks. In: **Proceedings of the 40th ACM/-SIGAPP Symposium on Applied Computing**. [s.n.], 2025. p. 1800–1809. Disponível em: <https://dl.acm.org/doi/10.1145/3672608.3707823>. Acesso em: 12 dez. 2025.

THOMAS, L.; BHAT, S. A study on intrusion detection system for iot environment based on machine learning. **IEEE Access**, IEEE, 2024. Acesso em: 22 jan. 2025.

TRIPATHY, B.; ANURADHA, J. **Internet of Things (IoT): Technologies, Applications, Challenges and Solutions**. CRC Press, 2017. ISBN 9781351980296. Disponível em: <https://books.google.com.br/books?id=LHQ5DwAAQBAJ>. Acesso em: 21 jan. 2025.

ULLAH, S.; WU, J.; KAMAL, M. M.; MOHAMED, H. G.; SHERAZ, M.; CHUAH, T. C. Mbid: A scalable multi-tier blockchain architecture with physics-informed neural networks for intrusion detection in large-scale iot networks. **Computer Modeling in Engineering & Sciences (CMES)**, v. 144, n. 2, 2025. Disponível em: <https://www.sciencedirect.com/org/science/article/pii/S1526149225002747>. Acesso em: 15 dez. 2025.

VIVIAN, G. A.; BAUDER, R. A.; KHOSHGOFTAAR, T. M. A comprehensive survey on machine learning for workplace injury analysis: risk prediction, return to work strategies, and demographic insights. **Journal of Big Data**, Springer, v. 12, n. 1, p. 167, 2025. Disponível em: <https://link.springer.com/article/10.1186/s40537-025-01229-z>. Acesso em: 21 jan. 2025.

VS, D. P.; SETHURAMAN, S. C.; KHAN, M. K. Blockchain-based deep learning models for intrusion detection in industrial control systems: Frameworks and open issues. **Journal of Network and Computer Applications**, Elsevier, p. 104286, 2025. Disponível em: <https://www.sciencedirect.com/science/article/pii/S1084804525001833>. Acesso em: 15 dez. 2025.

WAKILI, A.; BAKKALI, S. A resilient iot intrusion detection system using hybrid feature selection and explainable ensemble learning. **Results in Engineering**, Elsevier, p. 107392, 2025. Disponível em: <https://www.sciencedirect.com/science/article/pii/S2590123025034474>. Acesso em: 15 dez. 2025.

WAKILI, A.; BAKKALI, S.; IBRAHIM, I. A. A digital twin-enhanced cybersecurity framework for iot in healthcare: Applications in industry 4.0. **Telematics and Informatics Reports**, Elsevier, v. 20, p. 100254, 2025. Disponível em: <https://www.sciencedirect.com/science/article/pii/S2772503025000684>. Acesso em: 15 dez. 2025.

WALI, A.; ALSHEHRY, F. A survey of security challenges in cloud-based scada systems. **Computers**, MDPI, v. 13, n. 4, p. 97, 2024. Disponível em: <https://www.mdpi.com/2073-431X/13/4/97>. Acesso em: 17 jan. 2025.

WANG, M.; YANG, N.; GUNASINGHE, D. H.; WENG, N. On the robustness of ml-based network intrusion detection systems: An adversarial and distribution shift perspective. **Computers**, MDPI, v. 12, n. 10, p. 209, 2023. Disponível em: <https://www.mdpi.com/2073-431X/12/10/209>. Acesso em: 17 jan. 2025.

WOLFERT, S.; GE, L.; VERDOUW, C.; BOGAARDT, M.-J. Big data in smart farming–a review. **Agricultural systems**, Elsevier, v. 153, p. 69–80, 2017. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0308521X16303754>. Acesso em: 23 jan. 2025.

WOODMAN, R. J.; MANGONI, A. A. A comprehensive review of machine learning algorithms and their application in geriatric medicine: present and future. **Aging Clinical and Experimental Research**, Springer, v. 35, n. 11, p. 2363–2397, 2023. Disponível em: <https://link.springer.com/article/10.1007/s40520-023-02552-2>. Acesso em: 21 jan. 2025.

XAVIER, B. M.; DZAFERAGIC, M.; VILà, I.; MARTINELLO, M.; RUFFINI, M. Cross-domain ai for early attack detection and defense against malicious flows in o-ran. In: **ICC 2024 - IEEE International Conference on Communications**. [s.n.], 2024. p. 2384–2389. Disponível em: <https://ieeexplore.ieee.org/document/10622345>. Acesso em: 16 jan. 2025.

YALLI, J. S.; HASAN, M. H.; BADAWI, A. A. Internet of things (iot): Origins, embedded technologies, smart applications, and its growth in the last decade. **IEEE Access**, v. 12, p. 91357–91382, 2024. Disponível em: <https://ieeexplore.ieee.org/abstract/document/10570411/>. Acesso em: 21 jan. 2025.

YAN, Y.; YANG, Y.; FANG, S.; GAO, M.; CHEN, Y. Mus model: A deep learning-based architecture for iot intrusion detection. **Computers, Materials & Continua**, v. 80, n. 1, 2024. Disponível em: <https://www.sciencedirect.com/org/science/article/pii/S1546221824004715>. Acesso em: 15 dez. 2025.

YU, J.; SHVETSOV, A. V.; ALSAMHI, S. H. Leveraging machine learning for cybersecurity resilience in industry 4.0: Challenges and future directions. **IEEE Access**, v. 12, p. 159579–159596, 2024. Disponível em: <https://ieeexplore.ieee.org/document/10721279>. Acesso em: 16 jan. 2025.

ZANELLA, A.; BUI, N.; CASTELLANI, A.; VANGELISTA, L.; ZORZI, M. Internet of things for smart cities. **IEEE Internet of Things journal**, Ieee, v. 1, n. 1, p. 22–32, 2014. Disponível em: <https://ieeexplore.ieee.org/abstract/document/6740844/>. Acesso em: 23 jan. 2025.

ZHANG, H.; UPADHYAY, D.; ZAMAN, M.; JAIN, A.; SAMPALLI, S. Sc-mlids: Fusion-based machine learning framework for intrusion detection in wireless sensor networks. **Ad Hoc Networks**, Elsevier, p. 103871, 2025. Disponível em: <https://www.sciencedirect.com/science/article/pii/S1570870525001192>. Acesso em: 15 dez. 2025.

ZHANG, S.; FU, Q.; AN, D. Network security situation prediction model based on vmd decomposition and dwoa optimized bigru-attn neural network. **IEEE Access**, v. 11, p. 129507–129535, 2023. Disponível em: <https://ieeexplore.ieee.org/document/10320087>. Acesso em: 16 jan. 2025.

ZHANG, Z.; HAMADI, H. A.; DAMIANI, E.; YEUN, C. Y.; TAHER, F. Explainable artificial intelligence applications in cyber security: State-of-the-art in research. **IEEE Access**, v. 10, p. 93104–93139, 2022. Disponível em: <https://ieeexplore.ieee.org/document/9875264>. Acesso em: 16 jan. 2025.

ZHOU, Z.; LIU, S. **Machine Learning**. Springer Nature Singapore, 2021. ISBN 9789811519673. Disponível em: <https://books.google.com.br/books?id=ctM-EAAAQBAJ>. Acesso em: 21 jan. 2025.

ZHUKABAYEVA, T.; AHMAD, Z.; ADAMOVA, A.; KARABAYEV, N.; ABDILDAYEVA, A. An edge-computing-based integrated framework for network traffic analysis and intrusion detection to enhance cyber–physical system security in industrial iot. **Sensors**, MDPI, v. 25, n. 8, p. 2395, 2025. Disponível em: <https://www.mdpi.com/1424-8220/25/8/2395>. Acesso em: 10 dez. 2025.

ZUBAIDI, A. A. A. M. H. A. Iot cyber attacks detection - survey. In: **2024 16th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)**. [s.n.], 2024. p. 1–6. Disponível em: <https://ieeexplore.ieee.org/document/10607501>. Acesso em: 16 jan. 2025.

APÊNDICE A – TABELAS DAS ANÁLISES DOS ARTIGOS

Artigo	Ano	Objetivo	Algorítimos	Características de IoT Analisada	Resultado	Contribuição	Desafios
(SAMONTE *et al.*, 2024)	2024	Explorar a eficácia de técnicas de IA na identificação e defesa contra ameaças cibernéticas em arquiteturas de sistemas integrados	Machine Learning, Deep Learning	Vulnerabilidades e ameaças de segurança em redes de IoT e sistemas ciber-físicos	A IA demonstrou potencial significativo para melhorar a detecção de ameaças e a resposta a incidentes, superando medidas de segurança tradicional.	Fornece uma análise abrangente sobre a aplicação de IA em segurança cibernética, destacando sua importância em sistemas integrados.	Enfrenta limitações relacionadas à precisão na classificação de ataques específicos e à dependência da qualidade dos dados para treinamento dos modelos de IA.
(HIRSI *et al.*, 2024)	2024	O artigo visa desenvolver um framework para a detecção de ataques DDoS em ambientes de SDN utilizando ML.	Regressão Logística, SVM, Random Forest, KNN, XGBoost.	O estudo analisou o tráfego de IoT em redes, focando na detecção de padrões de ataque e tráfego benigno.	O framework alcançou altas taxas de precisão na detecção de ataques, com resultados superiores a 99% em alguns casos.	A pesquisa introduziu um novo conjunto de dados customizado e avaliou a eficácia de diferentes algoritmos de aprendizado de máquina para a detecção de intrusões.	O artigo enfrenta desafios como a falta de diversidade nos cenários de ataque testados e a necessidade de abordar a robustez contra novas estratégias ofensivas.
(YU *et al.*, 2024)	2024	O artigo visa explorar como a ML pode fortalecer a resiliência cibernética na Indústria 4.0.	Aprendizagem supervisionada, não supervisionada, por reforço	As características analisadas incluem vulnerabilidades, riscos de violação de dados e a necessidade de processamento de dados em tempo real em ambientes de IoT.	Os resultados destacam a eficácia da ML em detectar ameaças e melhorar a resposta a incidentes em tempo real.	O artigo contribui ao fornecer uma visão abrangente sobre a aplicação de ML em cibersegurança, identificando tendências emergentes e direções futuras de pesquisa.	Os desafios incluem a qualidade e diversidade dos dados de treinamento, a necessidade de métodos de preservação da privacidade e a complexidade da integração de dispositivos IoT em ambientes industriais.
(XAVIER *et al.*, 2024)	2024	Propor uma metodologia de aprendizado de máquina cross-domain para detecção e mitigação de ataques em redes O-RAN.	Machine Learning, treinamento contínuo	Tráfego de rede relacionado a dispositivos IoT, incluindo classificação de tráfego e detecção de anomalias.	O classificador RAN alcançou uma precisão de 93%, com melhoria contínua por meio de feedback do classificador In-Network.	Introduz uma abordagem inovadora para integrar dados de diferentes domínios (RAN e redes de transporte) para melhorar a segurança em redes móveis.	Enfrentar limitações como granularidade temporal nos dados, ruído causado por erros de rotulagem e restrições computacionais nas redes RAN.
(ZUBAIDI, 2024)	2024	Revisar e comparar técnicas de IDS para dispositivos IoT, abordando desafios específicos de segurança.	ML (supervisionado, não supervisionado), CNN, análise comportamental.	Heterogeneidade, restrições de recursos, comunicação em tempo real, privacidade de dados e ambientes escaláveis.	Avanços significativos em precisão, redução de falsos positivos e integração com edge computing para maior eficiência.	Fornece uma análise abrangente das técnicas de IDS para IoT, destacando melhorias por meio de IA e big data.	Construção de datasets rotulados, restrições computacionais de dispositivos IoT e interpretabilidade de modelos complexos.
(SAYADI *et al.*, 2024)	2024	Analisar e discutir técnicas baseadas em contadores de desempenho de hardware (HPCs) integradas a algoritmos de aprendizado de máquina para detecção inteligente de malware.	CNN, MLP, SVM, Ensemble Learning (AdaBoost, Random Forest), Transfer Learning.	Heterogeneidade de dispositivos, restrições de recursos computacionais e a aplicação de técnicas leves para detecção em tempo real.	Melhor precisão na detecção de malware em sistemas embarcados e IoT, com taxas de detecção acima de 90% em alguns casos e melhorias na eficiência energética.	Proporciona um panorama abrangente sobre técnicas de segurança assistidas por hardware, abordando desafios e propondo soluções baseadas em aprendizado de máquina para melhorar a detecção de malware.	Limitação na generalização de técnicas para arquiteturas diferentes, dificuldades na seleção de recursos relevantes em HPCs e desafios na preservação de privacidade durante a detecção de malware.
(SINGH *et al.*, 2024a)	2024	Explorar o uso de inteligência artificial habilitada para inteligência de ameaças (AI-TI) na detecção e resposta a ataques cibernéticos.	Random Forest, KNN, ANN Quantum Machine Learning.	Automação de tarefas de segurança, detecção de ameaças em tempo real e aprendizado contínuo em sistemas conectados.	Melhor eficiência na detecção de ameaças complexas, redução do tempo de resposta e aprimoramento da postura de segurança das organizações.	Apresenta uma abordagem inovadora para integrar IA em sistemas de inteligência de ameaças, destacando os benefícios e desafios da implementação.	Alto custo de implementação, necessidade de grandes volumes de dados para treinamento e dificuldade em interpretar decisões geradas pelos modelos de IA.
(ABDI *et al.*, 2024)	2024	Investigar abordagens de segurança tradicionais, baseadas em IA e defesa de alvo móvel (MTD) para proteger os planos de controle e dados em redes definidas por software (SDN).	Machine Learning, Deep Learning, aprendizam supervisionada, não supervisionada, por reforço.	Desafios de segurança relacionados à comunicação em tempo real, gerenciamento de tráfego, escalabilidade e adaptação dinâmica em ambientes SDN.	Melhorias significativas em detecção de ameaças, mitigação de DDoS e integração de estratégias dinâmicas de defesa com MTD.	Fornece uma análise abrangente das soluções de segurança para SDN, destacando a combinação de técnicas tradicionais, IA e MTD como pilares fundamentais para enfrentar ameaças emergentes.	Lidar com a complexidade da integração de estratégias heterogêneas, padronização limitada e impacto de desempenho em redes de larga escala.
(HOSSAIN *et al.*, 2024)	2024	Propor um framework de Cyber Range baseado em Digital Twin Metaverse Network (DTMN) para reforçar a segurança e privacidade em redes IT/OT no contexto de 6G.	Deep Learning, Federated Learning.	Integração em tempo real de dispositivos conectados, segurança de dados, baixa latência e escalabilidade em ambientes de redes de consumo.	O framework proposto demonstrou eficiência em proteger dados de usuários, detectar ameaças cibernéticas e garantir alta precisão em modelos baseados em IA, com melhorias nas métricas de segurança.	Introduziu um modelo inovador de Cyber Range que combina técnicas de IA e 6G para aumentar a resiliência cibernética em aplicações de consumidores, como dispositivos IoT.	Superar complexidades de integração em larga escala, balancear ética e privacidade nos modelos de IA e lidar com o aumento da superfície de ataque devido à conectividade massiva.
(ALHARBI *et al.*, 2024)	2023	O artigo visa aprimorar a segurança das redes de IoT integrando as tecnologias de IA e Blockchain para enfrentar os desafios de segurança cibernética	Deep Learning, DeepDCA, ANNs, Random Forest, NIS	O artigo analisa as vulnerabilidades e os desafios de segurança das redes de IoT, com foco especial nos ataques de DDoS e DoS	A integração da IA com as tecnologias blockchain supera outros estudos na satisfação de métricas predefinidas para segurança de IoT, embora nenhum estudo atenda a todas as métricas	O artigo contribui propondo uma estrutura descentralizada e colaborativa baseada em Blockchain (BC-IDSs) que vincula vários IDSs para aprimorar a segurança da IoT	O artigo identifica desafios como os problemas de escalabilidade do armazenamento do Blockchain e a necessidade de tratamento profissional dos dados armazenados no Blockchain
(HAGHIGHI *et al.*, 2024)	2020	O artigo visa projetar um firewall de aprendizado que minimize os alarmes falsos e, ao mesmo tempo, garanta a segurança de sistemas críticos, como redes elétricas	Classificadores Z	O artigo analisa especificamente a segurança dos sistemas industriais de IoT, particularmente em ambientes onde qualquer interrupção é intolerável, como usinas de energia e tubulações	O algoritmo proposto foi testado em um sistema de monitoramento da rede elétrica e no conjunto de dados KDD CUP'99, confirmando sua eficácia em atingir zero falsos positivos	O artigo contribui fornecendo um novo algoritmo que pode converter qualquer classificador genérico em um classificador de zero falso-positivo, aumentando a segurança dos sistemas de prevenção de intrusões	Um desafio mencionado é a necessidade de trabalhos futuros para garantir que o algoritmo mantenha a consciência dos limites para evitar traçar o limite de decisão muito próximo das amostras de treinamento, o que pode levar a falsos positivos durante o teste

Tabela 5 – Análise dos Artigos

(RADOGLOU-GRAMMATIKIS *et al.*, 2023)	2023	O artigo pretende analisar o cenário atual e as tendências da Inteligência de Ameaças Cibernéticas (CTI) e dos mecanismos de colaboração para aprimorar as estratégias de segurança cibernética contra ameaças em evolução	Random Forest Classifier, OneClassSVM, autoencoders	Embora as características específicas da IoT não sejam detalhadas nos contextos fornecidos, o artigo enfatiza a importância do compartilhamento de inteligência de ameaças e da colaboração entre dispositivos de IoT para melhorar as medidas de segurança	Os resultados indicam que os modelos propostos, particularmente os codificadores automáticos, classificam efetivamente as cargas HTTP modificadas como maliciosas, apresentando recursos de detecção aprimorados	O artigo contribui para o campo ao propor uma estrutura para compartilhamento e conscientização orquestrados de informações, aprimorando as capacidades de detecção e resposta dos sistemas de segurança cibernética	Os desafios destacados incluem a necessidade de adaptação contínua dos mecanismos de inteligência de ameaças para combater a natureza evolutiva dos ataques cibernéticos conduzidos por IA
(SURYA; SHANTHI, 2023)	2023	O artigo visa aprimorar a segurança dos dispositivos de IoT por meio da aplicação de IDS usando técnicas de IA, com foco particular na verificação de modelos cruzados com CNNs	CNNs, SELBEST	A pesquisa analisa dados de tráfego de rede de vários dispositivos de IoT, enfatizando os desafios exclusivos impostos pelo aumento do número de dispositivos conectados e pela evolução das ameaças cibernéticas	Os resultados indicam que a abordagem proposta atinge uma precisão de mais de 80-95% em três conjuntos de dados, com melhor desempenho e tempo de classificação reduzido	O artigo contribui para o campo ao demonstrar a eficácia da verificação cruzada de modelos na melhoria da precisão e resiliência do IDS para ambientes de IoT	O principal desafio abordado é a dificuldade do IDS tradicional em se adaptar às características exclusivas dos ambientes de IoT, que são suscetíveis a vários tipos de ataques
(THANTHARATE; T, 2023)	2023	O artigo apresenta o Cybria, uma estrutura de Federated Learnig para detecção colaborativa de ameaças cibernéticas, preservando a privacidade dos dados	Machine Learning, Federated Learnig	O artigo analisa a segurança em redes de IoT, abordando a detecção de intrusões em dados de tráfego de rede e logs de sistemas	O modelo Cybria alcançou uma precisão de 89,6% na detecção de ameaças, superando a precisão de 81,4% de um modelo de rede neural profunda centralizado	A principal contribuição é a apresentação de um modelo de aprendizado federado que permite a detecção de ameaças cibernéticas sem comprometer a privacidade dos dados	Os desafios incluem a heterogeneidade estatística dos dados, ataques de envenenamento de dados e a necessidade de protocolos de agregação seguros
(HOSSAIN *et al.*, 2023)	2023	Detectar ataques de intrusão no contexto de Federated Learning e desenvolver um mecanismo de defesa.	Redes Neurais Convolucional	Intrusão em dados durante o treinamento de modelos de Federated Learning	Avaliação do desempenho do modelo após treinamento com dados perturbados e comparação com o modelo de defesa.	Proposta de um mecanismo de defesa que melhora a robustez do Federated Learning contra ataques maliciosos.	Gerenciar a agregação de atualizações locais e descartar dados corrompidos sem comprometer o desempenho do modelo.
(ZHANG *et al.*, 2023)	2023	Desenvolver um modelo híbrido para previsão da situação de segurança de rede usando técnicas como VMD, DWOA, BiGRU e ATTN para melhorar a precisão das previsões.	BiGRU, ATTN, DWOA	Desafios de segurança devido a vulnerabilidades, configurações padrão e ataques que podem comprometer dispositivos e redes IoT.	O modelo proposto demonstrou melhora nos valores de R^2 variando de 6,34% a 52,61% em comparação com métodos existentes.	Introdução de um modelo preditivo que combina VMD, DWOA e BiGRU-ATTN, oferecendo melhor desempenho na previsão da situação de segurança de rede.	Lidar com a alta não-estacionaridade das sequências de segurança de rede e a necessidade de otimização precisa dos hiperparâmetros para melhorar a desempenho preditiva.
(FERRAG *et al.*, 2023)	2023	Analisar as vulnerabilidades, datasets e soluções de segurança para sistemas IoT habilitados para 6G, com foco no aprendizado em borda (Edge Learning).	Centralized Learning, Federated learning, Distributed learning	Segurança de dispositivos em borda, privacidade de dados, escalabilidade, e integração com redes 6G.	Identificação de oito categorias de ataques contra aprendizado de máquina e propostas de métodos de defesa eficazes baseados em Federated e técnicas avançadas de IA.	Fornece uma taxonomia abrangente de métodos de defesa e destaca as oportunidades e desafios de segurança em sistemas IoT baseados em 6G.	Enfrentar a complexidade de ataques sofisticados, garantir privacidade em redes densas e lidar com limitações de dispositivos IoT em termos de recursos.
(SAINI *et al.*, 2023)	2023	Mitigar ameaças de segurança em ambientes IoT usando um modelo de detecção de intrusões baseado em aprendizado de máquina.	Naive Bayes, SVM, Decision Tree.	Padrões de movimento dos dispositivos IoT para identificar comportamentos anômalos e prevenir ataques DDoS.	Alta precisão na detecção de ameaças, com NB alcançando 97.4%, SVM 96.1% e DT 98.1%.	Proposta de um framework inovador que integra técnicas de ML para detectar e prevenir eficientemente ataques DDoS em redes IoT.	Dificuldade em distinguir ataques DDoS de solicitações legítimas e a necessidade de algoritmos sofisticados para análises em tempo real devido ao alto volume de dados em redes modernas.
(MAHMOUD *et al.*, 2023)	2023	Desenvolver um IDS eficiente baseado em IoT para detectar vulnerabilidades em dispositivos IoT.	ML, DL, RF, DT, NB, GB, RNN, LSTM.	Detecção de anomalias, seleção de atributos e ataque em redes IoT.	Avaliação de desempenho superior do modelo proposto em comparação com trabalhos relacionados.	Proposição de um IDS eficiente para melhorar a detecção de intrusões em ambientes IoT.	Melhorar a precisão dos modelos de previsão de ataques em dispositivos IoT limitados em energia e computação.
(RJOUB *et al.*, 2023)	2023	Desenvolver modelos XAI confiáveis e adequados para aplicações em IoT.	Decision Tree, Modelagem Estatística.	Segurança de rede no IIoT e comportamento dos consumidores para otimizar o consumo de energia.	Efetividade do modelo TRUST XAI em segurança de rede e redução de custos de energia usando IoB e XAI.	Desenvolvimento do modelo TRUST XAI para gerar confiança em sistemas de IA e integração de IoB para influenciar comportamento do consumidor.	Garantir que os sistemas de IA sejam confiáveis, explicáveis e otimizem a interação humano-tecnológica.
(GOYAL *et al.*, 2023)	2023	Explorar a integração de IA com cibersegurança para aplicações da Indústria 4.0, visando melhorar a proteção contra ataques cibernéticos.	CNN, LSTM, CNN+LSTM.	Automação industrial, detecção de anomalias em tempo real, e segurança em redes inteligentes com conectividade massiva.	O modelo híbrido CNN+LSTM alcançou a maior precisão (95%) em comparação com abordagens isoladas, mostrando eficácia na detecção de anomalias em ambientes da Indústria 4.0.	Proporciona uma abordagem inovadora para combinar técnicas de deep learning na detecção de ameaças e anomalias, otimizando a cibersegurança em sistemas industriais.	Alta demanda computacional, necessidade de grandes volumes de dados para treinamento e dificuldades na adaptação para diferentes cenários industriais.
(MOUSTAFA *et al.*, 2023)	2023	Revisar técnicas de XAI para detecção de intrusões baseadas em anomalias em redes IoT.	Machine Learning, Deep Learning	Natureza distribuída, heterogeneidade, geração de dados de alta dimensão e multimodais.	Algoritmos de ML/DL alcançaram bom desempenho na prevenção de ataques desconhecidos em IDS.	Prover um panorama das técnicas de XAI em IDS, explorando desafios e futuras pesquisas.	Explicar modelos de DL e lidar com conjuntos de dados desatualizados ou desequilibrados.
(SHARMA; DASH, 2023)	2023	Investigar o impacto de análises de Big Data e da inteligência artificial (IA), incluindo o ChatGPT, na mitigação e potencial intensificação de ameaças cibernéticas.	NLP, Machine Learning, Deep Learnig, ChatGPT.	Análise de grandes volumes de dados gerados por dispositivos IoT, segurança em redes heterogêneas e proteção contra ataques como phishing e malware.	Demonstrações de como a IA pode melhorar a detecção de ameaças cibernéticas e destacar o uso potencial do ChatGPT por atacantes para criar malwares sofisticados.	Proporciona uma visão equilibrada sobre os benefícios e riscos do uso de IA na cibersegurança, discutindo métodos proativos para conter ameaças crescentes.	Gerenciar os riscos associados ao uso malicioso de IA, como o ChatGPT, e integrar ferramentas de Big Data com soluções de segurança para enfrentar ameaças emergentes.
(QUAN *et al.*, 2023)	2022	Proporcionar um sistema de priorização de filas baseado em FL para aplicações sensíveis a atrasos na rede IoT.	XGBoost, RNN, SVM, SOM.	Tipo e localização das aplicações para sensibilidade de atraso e análise comportamental para detecção de ataques DDoS.	Melhoria na qualidade do serviço, redução do atraso fim a fim e detecção precisa de ataques DDoS.	Implementação de sistemas de gestão de fila e detecção de ataques utilizando IA e PDP, proporcionando detecção precisa e priorização dinâmica de redes.	Implementar AQM em PDP e a complexidade de depuração de modelos de IA em switches tradicionais.

Tabela 6 – Análise dos Artigos

(TABASSUM *et al.*, 2022)	2022	Desenvolvimento de sistemas de IDS com foco em inteligibilidade e segurança duradoura.	DT, XGBoost, SOMs XAI, RF, ANN, SVM.	Utilização de datasets desequilibrados e explicabilidade dos modelos para segurança.	Implementação de métodos que conseguem explicar e interpretar resultados para maior segurança em IoT.	Proposta de métodos explicáveis e interpretáveis para melhor compreensão e eficácia das estratégias de segurança em IoT.	Detectar ataques adversariais e lidar com distribuições de dados desequilibradas.
(SAYADI *et al.*, 2022)	2022	Investigar o papel crescente de técnicas de IA/ML na segurança de hardware e discutir os desafios e oportunidades nesse campo.	Ensemble Learning, AdaBoost, Bagging, Machine Learning.	Limitações de recursos em sistemas embarcados e IoT que dificultam a aplicação de técnicas tradicionais de detecção baseadas em software.	A eficácia dos detectores baseados em IA em tempo real foi demonstrada, mostrando rápido tempo de detecção e baixo overhead.	Fornece um entendimento exaustivo sobre a aplicação de IA/ML para deteção assistida por hardware e ataques de canais laterais.	A detecção de malware furtivo, a explicação das interações entre HPC e comportamento do malware, e a validação para diferentes arquiteturas de microprocessadores.
(ZHANG *et al.*, 2022)	2022	Revisar as aplicações de IA Explicável (XAI) em cibersegurança.	Machine Learning, Deep Learning	Integração de XAI para melhorar a transparência e a explicabilidade em decisões	A eficácia das abordagens XAI em detectar e defender contra ameaças cibernéticas	Análise abrangente das técnicas XAI e suas aplicações em diversos setores	A necessidade de superar a natureza "caixa-preta"dos modelos de IA e a vulnerabilidade a ataques adversariais.
(CAPUANO *et al.*, 2022)	2022	Propor técnicas baseadas em IA para detecção de intrusões em sistemas de IoT e ambientes de rede.	AutoEncoder, RF, SVM, Fast Learning Network, SO, RNN, Métodos Adversariais, SHAP, DT.	Comportamento de dispositivos, arrays numéricos para treinar algoritmos de ML e detecção de anomalias na nuvem.	Melhor seleção de características e explicabilidade dos modelos para detecção de intrusões.	Introdução de modelos híbridos e métodos explicáveis para melhorar a precisão e credibilidade na detecção de intrusões.	Garantir a precisão nas classificações minimizando as mudanças adversárias e explicando de forma clara as decisões dos modelos.
(JADIDI *et al.*, 2022)	2022	Desenvolver uma estratégia defensiva contra ataques adversariais em sistemas de detecção de intrusões baseados em Deep Learning em redes IoT e IIoT	ANN, Fast Gradient Sign Method (FGSM)	A detecção de atividades normais e de ataque em redes IoT e IIoT.	A eficácia do modelo retrainado em defender contra ataques adversariais, mostrando alta precisão na detecção de ataques.	Proposta de um modelo que se auto-sustenta contra ataques adversariais em larga escala.	Necessidade de lidar com vulnerabilidades desconhecidas e a eficácia das defesas em um ambiente em constante evolução.
(SINGH *et al.*, 2024b)	2025	Propor um framework abrangente que categoriza sistemas baseados em nuvem IoT em tipos distintos, abordando vulnerabilidades e questões específicas de segurança.	O artigo não menciona	Privacidade, interoperabilidade, escalabilidade e desafios específicos de dispositivos IoT portáteis e veículos conectados.	Proporcionou uma categorização sistemática dos sistemas IoT baseados em nuvem e delineou medidas de mitigação para riscos de segurança identificados.	Preenchimento de lacunas ao categorizar vulnerabilidades em sistemas IoT baseados em nuvem e sugerir soluções de segurança específicas para domínios pouco explorados.	Enfrentar novos riscos de segurança emergentes devido à integração da IoT com infraestruturas de nuvem e a ausência de regulamentações uniformes.
(LARRIVA-NOVO *et al.*, 2024)	2024	Desenvolver um sistema de detecção de intrusão que use Aprendizado por Reforço e IA Explicável para categorizar tráfego malicioso e fornecer explicações multi-nível.	Aprendizado por Reforço PPO, SHAP.	O artigo menciona pesquisas relacionadas que analisam explicabilidade em sistemas de IoT, mas não se concentra especificamente em características de IoT.	Foi proposto um sistema de detecção de intrusão com explicações em nível de característica usando a base de dados UNSW-NB15, alcançando 70% de acurácia.	Introdução de um método para melhorar a detecção de intrusões através de explicações multi-nível de ataques usando XAI no contexto de RL.	Superar as limitações das explicações de modelos "caixa preta"para melhorar a interpretabilidade e eficácia de modelos de detecção de intrusão baseados em RL.
(GAINA *et al.*, 2024)	2024	Avaliar métodos de comunicação unidirecional no contexto da segurança em sistemas IoT.	Machine Learning	Arquitetura, conectividade, protocolos de comunicação e gestão.	Classificação e análise de soluções de comunicação unidirecional quanto à segurança, confiabilidade e tipo de dispositivo.	Identificação de gaps no estudo das comunicações unidirecionais e proposta de melhoria na segurança e eficiência dos sistemas IoT.	Superar limitações físicas de diodos de dados, abordar problemas de interoperabilidade e gerenciar a falta de feedback na comunicação unidirecional.
(MESA *et al.*, 2024)	2024	Desenvolver uma taxonomia abrangente de ciberataques e práticas recomendadas para a segurança cibernética na cadeia de suprimentos marítima.	Machine Learning	A integração de tecnologias digitais para fortalecer defesas cibernéticas.	Os resultados obtidos destacam a prevalência de ataques DDoS e malware, além de 18 práticas recomendadas para mitigação.	Sistematização do conhecimento sobre ciberataques e na oferta de um modelo de classificação para gestores da cadeia de suprimentos marítima.	Os desafios incluem a necessidade de abordagens holísticas que considerem as complexidades operacionais e geopolíticas do setor marítimo.
(EL-SHAFEIY *et al.*, 2024)	2024	Avaliar a eficácia das técnicas de redes neurais recorrentes para detecção de intrusões em dados de IoT.	RNN, GRU, autoencoders, CNN, DNN	Dados de IoT são de alta dimensionalidade, temporais e multimodais.	A estratégia CNN+CGRN mostrou eficácia na detecção de anomalias em IoT, aumentando precisão e eficiência.	Proposta do sistema DCGR_IoT para segurança de redes IoT, otimizando a detecção de intrusões.	Análise e detecção de dados IoT complexos devido à sua natureza multidimensional e temporal.
(KANG *et al.*, 2024)	2024	O artigo visa categorizar e analisar sistematicamente ataques e defesas em sistemas de comunicação por satélite focando em ameaças à confidencialidade, integridade e disponibilidade.	Machine Learning	Não há menção específica às características de IoT analisadas nestes trechos.	A ampla cobertura e a natureza sem fios dos SCSs não só melhoram a acessibilidade do serviço, como também aumentam a suscetibilidade a ameaças graves.	Proporciona uma visão sistemática das ameaças de segurança e contramedidas para sistemas de comunicação por satélite.	Identifica a complexidade em comparar múltiplas propostas de segurança devido à variedade e diversidade das mesmas.
(BECERRA-SUAREZ *et al.*, 2024)	2024	Melhorar a detecção de ataques DDoS através de técnicas de Machine Learning e processamento de dados.	RF, DT, ADA, XGB, MLP, DNN.	O artigo não fornece especificamente características de IoT analisadas.	O classificador Random Forest alcançou a melhor taxa de acurácia de 99,97%.	Apresenta uma metodologia exaustiva para pré-processamento e seleção de características no contexto de ataques DDoS.	Detalhamento insuficiente sobre o tempo de resposta aos ataques e questões de pre-processamento de dados em alguns estudos anteriores referenciados.

Tabela 7 – Análise dos Artigos

(WALI; ALSHEHRY, 2024)	2024	Oferecer uma pesquisa abrangente sobre as principais vulnerabilidades e ciberataques que afetam sistemas SCADA baseados em nuvem.	O artigo não menciona	Integração de sistemas ciberfísicos/IoT para facilitar a coleta de dados em tempo real e automação.	O artigo identifica vulnerabilidades e categoriza ciberataques em sistemas SCADA baseados em nuvem, além de propor soluções de segurança.	Fornece uma visão abrangente dos desafios de segurança em sistemas SCADA em nuvem e soluções para mitigar ameaças cibernéticas.	Enfrentar desafios de segurança cibernética devido à acessibilidade e exposição em ambientes em nuvem.
(WANG *et al.*, 2023)	2023	Avaliar e melhorar a robustez de sistemas de detecção de intrusão em redes baseados em Machine Learning contra ataques adversariais e mudanças de distribuição.	Machine Learning, Constrained Learning	O documento não fornece detalhes sobre características específicas de IoT analisadas.	O artigo revisa avanços em robustez de NIDSs, identificando lacunas de pesquisa e propondo direções futuras.	Propõe um levantamento sistemático das técnicas para aprimorar a robustez de NIDSs baseados em Machine Learning.	O desafio principal é abordar sistematicamente as vulnerabilidades dos NIDSs a ataques adversariais e mudanças de distribuição em todo o fluxo de trabalho de ML.
(ASLAM *et al.*, 2023)	2023	Revisar os ataques cibernéticos em redes de comunicação de plantas de purificação e distribuição de água, destacando desafios, vulnerabilidades e perspectivas futuras.	Neural Networks, Supervised Unsupervised Learning, Behavioral Analysis	Sensores, atuadores e sistemas de controle em tempo real integrados a redes industriais críticas e a conectividade de TI e OT.	Identificação de ataques reais, desenvolvimento de métodos de defesa e avaliação de vulnerabilidades em sistemas de controle industrial.	Apresenta um panorama abrangente das ameaças à segurança em plantas de tratamento de água, propondo abordagens para melhorar a resiliência cibernética.	Escassez de algoritmos universais para proteção abrangente, alto custo de implementação de tecnologias modernas e dificuldades na integração de soluções em sistemas legados.
(DEMERTZI *et al.*, 2023)	2023	Explorar o impacto transformador do IIoT, integração com IA e Industry 4.0, e desafios de implementação com foco em segurança e privacidade.	Machine Learning, IA, Automação Inteligente	Conectividade ubíqua, troca de dados autônoma, privacidade e segurança, integração de dados, automação, e otimização de processos industriais.	Uma visão geral das abordagens e soluções contemporâneas para lidar com os riscos de privacidade na IIoT, tais como técnicas de encriptação e anonimização e controles de acesso.	Identifica e aborda a importância da segurança e privacidade no IIoT, fornecendo recomendações para um ecossistema seguro e privado.	Principais desafios na implementação do IIoT incluem riscos de segurança, vulnerabilidades a ataques sofisticados, e questões de compatibilidade e padronização.
(GUPTA *et al.*, 2022)	2022	Investigar modelos de Machine Learning e Deep Learning para segurança eletrônica da informação em redes móveis.	ANN, Naive Bayes, CNN, SVM	O artigo não detalha as características específicas de IoT analisadas nos trechos fornecidos.	O estudo analisa artigos e propõe que modelos de IA podem ser utilizados para criar um ambiente seguro contra várias ameaças de segurança cibernética.	Fornece uma revisão abrangente das técnicas de ML e DP aplicadas à segurança da informação eletrônica em redes móveis.	Lidar com ataques adversários a modelos de Machine Learning e a complexidade de proteger redes móveis multifacetadas.
(RAIMUNDO; ROSÁRIO, 2022)	2022	Analisar a integração de tecnologias como IoT, segurança cibernética, ML e suas aplicações na indústria e na nuvem.	Machine Learning, Decision Tree	Integração de sensores, conectividade, segurança, e o impacto no gerenciamento de redes de dispositivos.	Desenvolvimento de sistemas de detecção de intrusão e melhoria de countermeasures cibernéticas usando IA.	Discutir as interseções entre IoT, segurança cibernética e ML para melhorar a proteção de redes e dispositivos.	Lidar com as complexidades da segurança IoT e a necessidade de capacidades avançadas de cibersegurança.
(ADIL *et al.*, 2024)	2024	Realizar uma revisão sistemática da literatura sobre métricas de Qualidade de Serviço (QoS) em aplicações IoT assistidas por UAV de 2015 a 2023, destacando contribuições e desafios.	Machine Learning in QoS	Comunicação assistida por UAV em cenários como monitoramento de incêndios, áreas costeiras, desmatamento e operações militares sensíveis.	Identificação de lacunas e desafios nas métricas de QoS para UAVs-IoT, com propostas de melhorias e roadmap para pesquisas futuras.	Destaca a importância das métricas de QoS negligenciadas na literatura, propondo direções de pesquisa para aprimorar o desempenho em aplicações IoT assistidas por UAV.	Enfrentar limitações de QoS, como latência, confiabilidade e escalabilidade, que restringem a aplicabilidade em cenários complexos e críticos.
(OZTOPRAK *et al.*, 2024)	2024	Categorizar ataques em redes de sensores sem fio (WSNs), identificando vulnerabilidades e estratégias de mitigação, além de explorar direções de pesquisa no campo de segurança.	O artogo não menciona	Integração de redes de sensores sem fio no ecossistema de IoT e seu papelnas aplicações inovadoras e sustentáveis.	Análise detalhada das vulnerabilidades em WSNs e propostas de estratégias de mitigação eficazes.	Fornecer uma análise categorizada de ataques e uma exploração aprofundada das direções de pesquisa em segurança de WSNs.	Lidar com a segurança contínua de WSNs em um ambiente de rápida evolução tecnológica e a integração com novas direções de pesquisa.
(AHMED *et al.*, 2023)	2023	Fornecer uma visão clara e abrangente dos avanços dos Sistemas de Manufatura Cibernética(CMS).	Machine Learning	Coleta, análise e controle de dados em tempo real para otimização de processos.	Aumento da eficiência dos processos de produção e redução de custos.	Apresenta uma compreensão aprofundada dos CMS, incluindo conceitos, exemplos, e medidas de avaliação.	Necessidade de melhor segurança, escalabilidade e eficiência de custo.
(MARTÍNEZ *et al.*, 2023)	2023	Investigar a integração de algoritmos de IA em sistemas de IoT para otimização de desempenho.	ANN, Supervised Machine Learning	Conectividade, escalabilidade e segurança.	Melhoria na eficiência operacional e na precisão dos dados.	Proposta de um framework inovador que integra IA e IoT para aplicações inteligentes.	Superar limitações de segurança e gerenciamento de grandes volumes de dados.
(MCINTOSH *et al.*, 2024)	2024	Reavaliar e redirecionar o foco das pesquisas sobre ransomware para alinhar com sua evolução contemporânea e ameaças emergentes de exfiltração de dados.	Machine Learning	O artigo não menciona a análise de características específicas de IoT.	A pesquisa conclui que muitos estudos acadêmicos se tornaram irrelevantes diante da atual realidade do ransomware e destacam a necessidade de priorizar a ameaça de exfiltração de dados.	Propõe a integração do gerenciamento de riscos de ransomware na gestão de riscos de cibersegurança organizacional e destaca a importância da inteligência cibernética e da conformidade regulatória.	O desafio é alinhar as pesquisas acadêmicas de ransomware com as constantes evoluções e complexidades das ameaças atuais e emergentes na indústria.
(NARAYAN *et al.*, 2023)	2023	Estudar o impacto de técnicas de seleção de características e balanceamento de classes em algoritmos de aprendizado de máquina para melhorar a detecção de intrusões em dispositivos IoT	Machine Learning, CFS, BRFC	Conjunto de dados CICIoT2023, que inclui 33 tipos de ataques em uma topologia de rede com 105 dispositivos IoT reais	O modelo proposto melhorou em 3.72% 3.75% e 4.69% em precisão recall e F1-score e obteve uma melhoria significativa de 7.9% com análise de classes não saturadas.	Contribui para o desenvolvimento de um sistema de detecção de intrusões mais eficazes em ambientes IoT destacando a importância do balanceamento de classes e seleção de características	Coleta de dados em uma topologia de rede real e a necessidade de lidar com conjuntos de dados desequilibrados

Tabela 8 – Análise dos Artigos

(HASAN; TASNIM, 2024)	2024	Desenvolver um sistema de detecção de intrusões em tempo real (IDS) para IoT utilizando um autoencoder sensível a custos (CSAE-WA) para lidar com amostras de treinamento desbalanceadas.	CSAE-WA, XGBoost (XGB)	33 tipos distintos de ataques em 105 dispositivos IoT incluindo DDoS, DoS, Recon, e Spoofing, utilizando os conjuntos de dados CICIoT2023 e DS2OS.	O modelo CSAE-WA demonstrou desempenho superior em comparação com seis técnicas de detecção de intrusões existentes, apresentando melhor precisão e F1-score.	A pesquisa propõe um IDS inovador que melhora a aprendizagem de características em cenários de IoT dinâmicos, abordando a transferência de conhecimento entre diferentes sistemas de IDS.	Adaptação a ataques raros, a alta taxa de falsos positivos em IDS, a necessidade de desenvolver um sistema inteligente que aprenda com amostras de treinamento desbalanceadas.
(S *et al.*, 2024)	2024	O trabalho visa aprimorar a segurança em ambientes de Internet das Coisas (IoT) através de sistemas de detecção de intrusões (IDS) e abordagens de aprendizado de máquina.	Machine Learning, adversarial training, Deep Learning, hybrid methods	O estudo focou em dispositivos comuns de IoT em ambientes de smart home, abordando a heterogeneidade dos dispositivos e as limitações de recursos.	O sistema alcançou 96,2% de precisão na detecção de comportamentos normais, 90,0% na detecção de dados prejudiciais e 98,0% na classificação de ataques, demonstrando eficácia robusta.	O trabalho oferece um framework sistemático para classificar abordagens de segurança em IoT, além de fornecer diretrizes práticas para engenheiros e profissionais.	Os principais desafios incluem a integração de soluções de segurança em ambientes heterogêneos, a privacidade dos dados e a eficiência computacional em redes complexas.
(JOHNSTONE; AKINFADERIN, 2025)	2025	Avaliar modelos de machine learning supervisionados para prever e classificar ameaças cibernéticas em ambientes de trabalho remoto de Provedores de Serviços Gerenciados (MSPs) nos EUA, integrados com dispositivos IoT.	Random Forest , XGBoost, Artificial Neural Networks, Recursive Feature Elimination , LIME, SHAP	Vulnerabilidades como falta de criptografia, autenticação e atualizações de firmware; camadas da arquitetura IoT suscetíveis a ataques (física a aplicação);	Random Forest alcançou 98.98% de acurácia com taxa de falso positivo de 0.0044 no dataset NF-UQ-NIDS-v2; XGBoost demonstrou generalização para ameaças diversas; ANN classificou padrões complexos; features reduzidas mantiveram alta performance; mapeamento para Cyber Kill Chain contextualizou estágios de ameaças.	Forneceu insights acionáveis de ML para fortalecer defesas cibernéticas de MSPs em ambientes IoT-remotos; mapeamento de features para Cyber Kill Chain melhora interpretabilidade e resposta a incidentes; modelos eficientes com features mínimas reduzem custos computacionais.	Fornece insights acionáveis de ML para fortalecer defesas cibernéticas de MSPs em ambientes IoT-remotos; mapeamento de features para Cyber Kill Chain melhora interpretabilidade e resposta a incidentes; modelos eficientes com features mínimas reduzem custos computacionais.
(JAAFOURI *et al.*, 2025)	2025	Apresentar um framework baseado em ensemble learning para detecção de anomalias em redes IoT, otimizando precisão e eficiência computacional para aplicações de segurança em tempo real contra ameaças como DDoS, ransomware e phishing.	Gradient Boosting, Random Forest, Isolation Forest, ensembles Bagging, Boosting, Stacking, Voting, Logistic Regression, Decision Trees, SVM, KNN, Naive Bayes, AdaBoost, Extra Trees, bayesian optimization, IQR, Z-score, Min-Max Scaling, PCA, RFE, encoding.	limitações computacionais/ energéticas, falta de segurança em dispositivos; interconectividade expandindo superfície de ataque; tráfego heterogêneo e dinâmico; cenários reais de dispositivos; ataques comuns como Mirai, Bashlite, DDoS, botnets.	Ensemble stacking (RF+XGBoost+GBM) alcançou 88.37% acurácia, 88% F1-score e 95.6% AUC no UNSW-NB15; 89.65% acurácia no IoT-23; 91.21% no CICIDS2017; redução de 12% em falsos negativos para DDoS e 8% em falsos positivos.	Framework escalável e adaptável integrando ensembles com otimização bayesiana, melhorando detecção robusta e resiliência em IoT; insights para integração em sistemas reais, reduzindo sobrecarga operacional e aprimorando defesas contra ameaças evolutivas.	Manuseio de datasets desbalanceados e heterogêneos; adaptação a tráfego dinâmico; otimização de hiperparâmetros; limitações computacionais em dispositivos IoT; generalização para ameaças emergentes; escalabilidade em redes complexas.
(MUNAWEERA *et al.*, 2024)	2025	Propor uma abordagem para proteger sistemas ciber-físicos críticos (CPS) em redes 5G contra ataques DDoS, usando detecção de anomalias com LSTM Autoencoder e Federated Learning (FL), avaliando defesas contra envenenamento de dados.	LSTM Autoencoder, Federated Learning, FedAvg, Krum, Multi-Krum, Trimmed Mean, Bulyan, Random Noise Injection, Trigger-based Backdoor, Constrained Perturbation, Feature-based, Temporal Pattern, Gradient Matching Attack, Differential Privacy, Data Sanitization	Vulnerabilidades em redes 5G/IoT como baixa latência e alta conectividade expandindo superfície de ataques DDoS; dados multivariados de tempo série de tráfego, métricas Kubernetes e logs; simulações com UERANSIM/Open5GS para cenários reais; foco em privacidade e descentralização em ambientes distribuídos.	Modelo centralizado: 93.12% acurácia, 92.19% precisão, 97.5% recall; FL sem ataques: 89.74% acurácia, 89.32% precisão, 95.2% recall; sob poisoning com FedAvg: ~47.86% acurácia média; com defesas, Bulyan alcança 88% acurácia sob ataques.	Modelo LSTM adaptado para dados 5G; framework FL para IDS colaborativo e preservador de privacidade; definição/avaliação de poisoning em dados de tempo série não supervisionados; insights sobre defesas robustas para redes 5G críticas.	Vulnerabilidades de FL a poisoning em setups descentralizados; detecção de ameaças evoluídas em ambientes 5G dinâmicos; trade-off entre performance e complexidade computacional em defesas; gap de performance entre FL e centralizado.
(THE *et al.*, 2025)	2025	Propor uma abordagem baseada em GAN para gerar dados de ataques realistas em sessões de carregamento de veículos elétricos (EV), identificando falhas em IDS e melhorando seu treinamento para maior robustez.	GAN, LSTM, Leaky ReLU, IDS Random Forest, Multilayer Perceptron, Local Outlier Factor, ensemble, Adam optimizer	Vulnerabilidades ciber-físicas em EVs e CPs; dados de sessões como perfis de carga, parâmetros de troca (ISO 15118), medidores (OCPP); expansão da superfície de ataque por interconexões; ataques como Mud e FDI impactando baterias e grids.	Amostras adversariais reduzem TPR dos IDS em até 93% (amostragem normal) e 16% (amostragem ataque); re-treinamento melhora AUC; t-SNE e ROC confirmam realismo e evasão; LOF mais resiliente, mas ainda afetado.	Framework GAN-LSTM para geração de ataques EV; avaliação de IDS e re-treinamento para eliminar viés; datasets/code públicos; insights para detecção em infraestruturas ciber-físicas.	Escassez de datasets com ataques realistas; viés em anomalias aleatórias/manuais; manipulação de séries temporais; trade-off TPR/FPR; necessidade de resiliência a poisoning/evasion em IDS.
(SATTARPOUR *et al.*, 2025)	2025	Introduzir um sistema de detecção de intrusões inteligente de duas camadas para ambientes IoT, utilizando otimização de features para manter precisão e reduzir sobrecarga computacional, com foco em detectar atividades indesejadas que afetam confidencialidade, integridade e disponibilidade.	Grasshopper Optimization Algorithm, Support Vector Machine, GOA-SVM, dataset NSL-KDD	Vulnerabilidades de segurança como integração de sensores e comunicação sem fio; ameaças a confidencialidade, integridade e disponibilidade; heterogeneidade de dispositivos, topologia dinâmica de rede e restrições de recursos.	Melhora na acurácia em comparação a outras abordagens; desempenho superior a métodos como Safaldin et al. e Almaslukh et al. em métricas como precisão, recall e F1-score via validação cruzada.	Abordagem híbrida GOA-SVM para detecção eficiente; seleção otimizada de features reduzindo complexidade; melhora taxas de detecção com alto TPR e baixo FPR em IoT.	Vulnerabilidades cibernéticas impedindo implantação; restrições de recursos em dispositivos IoT; heterogeneidade e topologia dinâmica; complexidade de treinamento, escalabilidade e dependência de grandes datasets.
(JAMSHIDI *et al.*, 2025)	2025	Explorar a integração de técnicas de ML e DL em IDS para melhorar a detecção e mitigação de ameaças em redes IoT, analisando forças, fraquezas, desafios, considerações éticas e o potencial de LLMs.	SVM, LSSVM, SVM-ACO, Naive Bayes, NB, NBTree, KNN, Decision Tree, Random Forest, RF-PSO, K-means, DL, LSTM, CNN, Autoencoders (AE, VAE, CFLVAE), RNN, ASRNN, DBN, ACO, PSO, ASO, EO, GA, GWO	Heterogeneidade e interconectividade de dispositivos; restrições de recursos (energia, computação); expansão da superfície de ataque; vulnerabilidades a intrusões físicas, de rede, software e criptográficas; estratégias de IDS (centralizada, distribuída, edge, híbrida) e análise (anomalia, assinatura, especificação, híbrida).	Revisão de literatura mostra accuracies de 97-99% em datasets como NSL-KDD, UNSW-NB15; DL superior para padrões complexos vs. ML tradicional; LLMs melhoram detecção adaptativa e correlação de alertas.	Framework para IDS adaptativos; análise abrangente de ML/DL em IoT; insights sobre GenAI/LLMs para vulnerabilidades, manutenção preditiva e detecção avançada; orientação para pesquisa futura em ética e privacidade.	Falsos positivos altos; datasets desatualizados; detecção em tempo real; correlação de alertas; tráfego criptografado; distinção de ataques vs. anomalias benignas; evasão adversarial; segurança em ICS; viés em ML; ética, privacidade e consumo de energia.
(ESMAEILI *et al.*, 2024)	2024	Investigar pesquisas recentes sobre estratégias de detecção de intrusões baseadas em ML para segurança IoT, focando em responsividade em tempo real, acurácia e eficiência algorítmica; fornecer taxonomia de abordagens existentes, destacar lacunas e limitações de frameworks atuais.	SVM, KNN, DT, RF, NB, AdaBoost, J48, OneR, ZeroR, Random Tree, não supervisionado (K-means), DL, LSTM, CNN, AE, RNN, DBN, DNN, MLP, LASSO, ACO, PSO, GA, CNN-LSTM	Vulnerabilidades como baixa potência/processamento, heterogeneidade de dispositivos, expansão de superfície de ataque; ameaças físicas, de rede (DDoS, eavesdropping), software e criptográficas; protocolos (RPL, LoWPAN, IEEE802.15.4, CoAP); taxonomia de ameaças em camadas.	Revisão de literatura mostra acurácias de 75-99% em datasets como NSL-KDD; compara KPIs como consumo de energia, privacidade, detecção de zero-day; DL supera ML clássico em padrões complexos, mas com trade-offs computacionais.	Taxonomia abrangente de ameaças e métodos ML/DL para IoT; análise de lacunas em detecção em tempo real e datasets; insights práticos para direções futuras em segurança escalável e adaptativa.	Restrições de recursos em dispositivos IoT; heterogeneidade e tráfego dinâmico; datasets desbalanceados/ desatualizados; altos falsos positivos; treinamento em dados massivos; evasão adversarial; necessidade de modelos híbridos e edge/fog computing.
(SI-AHMED *et al.*, 2023)	2022	Investigar como IDS baseados em ML podem abordar segurança e privacidade no IoMT; descrever arquitetura de três camadas, requisitos de segurança, ameaças; analisar vantagens, desvantagens, métodos e datasets de soluções ML por camada; discutir desafios e limitações.	SVM (linear/não-linear), DT, polynomial regression, OS-ELM, CNN, cu-GRU, DNN, cu-BLSTM, RNN, LSTM, KNN, multinomial NB, EMA	Heterogeneidade de dispositivos (wearables, implantados, ambientais, estacionários); comunicação sem fio vulnerável; limitações de computação, armazenamento e energia; big data gerado (velocidade, variedade, volume); arquitetura em camadas (aquisição, servidor pessoal, servidor médico).	Sumário de literatura mostra acurácias de 98%, TPR=0.914, AUC=0.947; DL supera ML tradicional em precisão e recall; comparações destacam trade-offs entre desempenho e overhead.	Taxonomia de soluções ML para IoMT; extensão de surveys prévios ao incluir segurança em nível de servidor médico; identificação de gaps e direções futuras para pesquisa.	Escassez de datasets públicos representativos; implantação em dispositivos limitados (bateria, modificações); generalizabilidade de modelos; detecção em tempo real; falsos positivos; black-box vs. explicabilidade; dados desbalanceados; escalabilidade e privacidade em abordagens federadas.
(ALSALAMAH; ISMAIL, 2025a)	2025	Introduzir um framework evolutivo para transformar dados tabulares IoT em representações de imagem, otimizando seleção de features via algoritmos metaheurísticos para detecção de intrusões eficiente e robusta.	Random Forest, XGBoost, Genetic Algorithm, Particle Swarm Optimization , Variable Neighborhood Search, CNN-IDS, CNN-LSTM Hybrid, ViT-IDS	Dados heterogêneos (leituras de sensores, fluxos de rede, metadados); vulnerabilidades a ataques cibernéticos manipulando dados; alta dimensionalidade, ruído, redundância; modalidades tabular e imagem para padrões espaciais e correlações.	VNS-XGBoost alcançou acurácia de 0.99997 em IDS2017/2018; redução de erros Tipo II de 212/6 para 4/1 em imagem; redução de features em ~45-52%; tempos de inferência baixos (0.003-0.077s); superior a DL end-to-end.	Framework multimodal com otimização evolutiva; análise comparativa de modalidades; seleção de features eficiente para edge; validação em datasets benchmark; insights para IDS adaptáveis.	Optima locais e escalabilidade em seleção de features; alta complexidade computacional em DL; desbalanceamento de classes; variabilidade em recall para classes semelhantes; necessidade de ajustes em hiperparâmetros; limitações em generalização para ataques zero-day.
(ISLAM *et al.*, 2025)	2025	Propor o PP-HFFL para detecção de intrusões em IoT, usando nós fog como intermediários para treinamento colaborativo, incorporando PFL para dados non-IID e DP para privacidade, superando riscos de privacidade, overhead de comunicação e limitações centralizadas.	Federated Learning, FedAvg, Personalized Federated Learning, Multi-Layer Perceptron, Differential Privacy	Heterogeneidade de dispositivos e dados non-IID; restrições de recursos (computação, energia, memória); expansão de superfície de ataque; privacidade em dados sensíveis (saúde, localização); imbalance de classes em datasets; distribuição edge-fog-cloud para escalabilidade.	Acurácia ~99% em RT-IoT e ~90% em CIC-IoT, comparável a centralizada; DP reduz acurácia em 1-6%; PFL melhora performance local; redução de overhead; robustez a non-IID e privacidade preservada.	Framework PP-HFFL integrando fog-FL, PFL e DP; avaliação em benchmarks reais; solução escalável e privacy-preserving para IDS em IoT; insights para heterogeneidade e ameaças.	Non-IID impactando convergência; trade-off acurácia-privacidade; restrições de recursos em edge; escalabilidade em grandes redes; churn dinâmico; não aborda ataques Byzantinos ou cenários reais completos.

Tabela 9 – Análise dos Artigos

(FU *et al.*, 2025)	2025	Introduzir o PriFed-IDS, um framework de IDS baseado em FL e RL preservador de privacidade para detecção inteligente de intrusões em sistemas de saúde digital (IoMT), otimizando desempenho, minimizando overhead de comunicação e lidando com ameaças cibernéticas evolutivas.	Federated Learning, Reinforcement Learning	Extensão para IoMT com sensores, dispositivos médicos e IoT para monitoramento de dados; vulnerabilidades a ciberameaças avançadas; restrições computacionais e energéticas em dispositivos; escassez de datasets de alta qualidade; riscos de vazamento de dados sensíveis.	PriFed-IDS supera benchmarks em acurácia de detecção e eficiência; avaliações experimentais e análise teórica confirmam aplicabilidade prática em redes IoMT reais.	Framework PriFed-IDS integrando FL e RL para IDS personalizado e seguro; estratégia adaptativa de treinamento para otimização; insights para personalização e contextualização em SHSs.	Vazamento de dados e consentimento de pacientes; escassez de datasets IoMT grandes e de qualidade; custos computacionais altos para IDS tradicionais em dispositivos limitados; ameaças cibernéticas evolutivas baseadas em IA.
(ALMALAWI, 2025)	2025	Propor o CLAIRE, um framework de active learning de quatro camadas para detecção de intrusões em IoT, selecionando instâncias representativas e informativas para reduzir custos de rotulagem por especialistas e melhorar IDS baseados em ML.	Sequencial clustering, ensemble-based uncertainty, Machine Learning	Crescimento exponencial (40.6 bilhões de conexões até 2034); vulnerabilidades a ameaças como DoS, DDoS; integração em infraestruturas críticas (energia, saúde, residências); dados heterogêneos e imbalanced.	Resultados promissores em datasets N-BaIoT e CICIoT2023; captura distribuições de dados em cenários imbalanced com pequeno conjunto de instâncias; superior a baselines em eficiência e cobertura.	Framework CLAIRE combinando clustering e uncertainty para active learning em IDS IoT; avaliação abrangente em datasets reais, reduzindo custos de anotação.	Alto custo de rotulagem por especialistas; datasets imbalanced e ameaças sofisticadas; necessidade de seleção eficiente de instâncias em ambientes dinâmicos.
(MÉDARD *et al.*, 2025)	2025	Propor uma abordagem otimizada de detecção de intrusões em IoT baseada em seleção de features Top-K combinada com modelos de ensemble learning, avaliada no dataset CICIoMT2024, para melhorar eficiência e adaptabilidade em sistemas distribuídos vulneráveis a ciberataques.	XGBoost, LightGBM, Random Forest	Crescimento exponencial de dispositivos interconectados; vulnerabilidades a ameaças como DDoS, intrusões stealth, spoofing e malware; foco em IoMT com riscos a disponibilidade de dispositivos críticos e segurança de pacientes.	Random Forest obteve melhor equilíbrio com 91.7% acurácia e 93% F1-score no Top-10, reduzindo tempo de processamento em 35%; superior em eficiência computacional vs. full features.	Estratégia Top-K aprimora interpretabilidade, precisão e eficiência de IDS em IoT; framework extensível para detecção adaptativa em tempo real e integração com edge computing em deployes em larga escala.	Limitações de métodos convencionais em espaços de features complexos e grandes; necessidade de mecanismos eficientes para processamento em ambientes distribuídos e heterogêneos.
(KIM *et al.*, 2025)	2025	Propor um modelo de geração de dados sintéticos preservador de privacidade baseado em framework de difusão tabular com Differential Privacy (DP), para fornecer dados úteis a IDS em IoT sem expor informações sensíveis reais.	TabDDPM, TabSyn, TabDiff, DP, Utility-Preserving DP, SDV Fidelity, DisclosureProtection, attribute inference, Membership Inference Attack.	Expansão de redes para coleta de dados em tempo real e automação em smart cities, saúde e agricultura; maior exposição a ameaças cibernéticas; heterogeneidade de dados sensíveis, exigindo grandes volumes para IDS com riscos de privacidade.	TabDiff com UP-DP alcançou SDV Fidelity de 0.98 e métricas estatísticas superiores; reduziu riscos de privacidade em dados sintéticos via DisclosureProtection, attribute inference e MIA, mantendo utilidade comparável a dados reais.	Abordagem inovadora que minimiza vazamento de padrões sensíveis, permitindo compartilhamento e análise segura de datasets para IDS em IoT, alinhada a regulamentações como GDPR.	Necessidade de grandes volumes de dados reais para IDS sem violar privacidade; riscos de abuso ou vazamento de informações pessoais em dados IoT; equilíbrio entre utilidade de dados sintéticos e proteção contra inferências maliciosas.
(ALSALAMAH; ISMAIL, 2025b)	2025	Desenvolver o MOOIDS-IoT, um framework multi-objetivo metaheurístico baseado em swarm integrado com ML para detecção eficiente, leve e em tempo real de intrusões em IoT, otimizando convergência, complexidade e acurácia enquanto lida com alta dimensionalidade, imbalance e dinâmica de redes.	Genetic Algorithm, Multi-Objective Particle Swarm Optimization, XGBoost, Random Forest, MOO-PSO-XGBoost, MOO-PSO-RF	Crescimento exponencial de conexões (14.4 bilhões em 2022); alta dimensionalidade, imbalance de classes e complexidade em tráfego de rede; natureza dinâmica de redes de sensores; limitações de recursos computacionais, exigindo escalabilidade e eficiência em ambientes restritos.	Em CICIoT2023: MOO-PSO-RF com 91.42% acurácia, MOO-PSO-XGBoost com 98.38%; em NSL-KDD: MOO-PSO-RF com 99.66%, MOO-PSO-XGBoost com 98.46%; redução de tempo de treinamento e redundância via GA.	Framework MOOIDS-IoT integrando GA e PSO multi-objetivo para IDS otimizado e leve em IoT; avaliação em benchmarks reais; adequado para aplicações com recursos limitados, preservando diversidade de soluções não-dominadas.	Alta dimensionalidade e redundância de features; imbalance de classes em datasets; complexidade computacional em redes dinâmicas; trade-offs multi-objetivo entre convergência, complexidade e acurácia em ambientes IoT restritos.
(SEYEDI; POSTOLACHE, 2025)	2025	Propor um framework avançado de detecção de anomalias em redes IoT, dividido em fases de pré-processamento de dados, seleção otimizada de features e classificação ensemble, para melhorar segurança contra ameaças como DoS, comportamentos anômalos e manipulação de dados.	Median-KS Test, Genetic Algorithm , ensemble, Decision Tree, Random Forest, XGBoost	Arquiteturas descentralizadas, dispositivos com restrições de recursos (computação, energia), ambientes de rede dinâmicos; vulnerabilidades a ameaças cibernéticas como DoS e manipulação de dados em setores como saúde, indústria e cidades inteligentes.	Melhora de 12.5% em acurácia (98%), 14% em taxa de detecção (95%), redução de 9.3% em falsos positivos (10%) e 10.8% em falsos negativos (5%), superando métodos existentes em eficiência e robustez.	Framework multi-fase adaptável e escalável que combina GA e ensemble para detecção precisa, reduzindo dimensionalidade e custos computacionais sem perda de acurácia, adequado para IoT reais contra ameaças evolutivas.	Vulnerabilidades inerentes a dispositivos limitados e redes dinâmicas; ruído, valores faltantes e desbalanceamento em datasets; necessidade de eficiência computacional em cenários heterogêneos e em evolução.
(NGO *et al.*, 2025)	2025	Abordar desafios de detecção de intrusões em IoT devido à complexidade e heterogeneidade do ecossistema, propondo o framework TKSGF que constrói grafos baseados em similaridade de atributos Top-K, utilizando GraphSAGE para representações escaláveis de nós e melhor desempenho em classificação binária e multi-classe.	GraphSAGE, LSTM, max-pooling, batch normalization, dropout,GCN e GAT, Decision Trees, Random Forest, KNN, Naive Bayes, XGBoost, cosine, Euclidean, FAISS	Heterogeneidade de dispositivos e dados; recursos limitados (computação, energia); vulnerabilidades a ameaças como DDoS, ransomware e MITM; escassez de datasets rotulados, desbalanceamento de classes; padrões temporais, diversidade de protocolos e comportamentos de rede.	Classificação binária: F1-score de 0.985 (NF-BoT IoT, dirigido, k=7) e 0.999 (NF-ToN IoT, não-dirigido, k=7); multi-classe: F1-score de 0.840 (NF-BoT IoT, não-dirigido, k=10) e 0.628 (NF-ToN IoT, não-dirigido, k=5); superou ML tradicionais e métodos gráficos existentes; cosine >Euclidean; não-dirigido melhor para multi-classe.	Framework TKSGF para construção de grafos baseada em atributos, melhorando representações de nós; desempenho superior em benchmarks; insights de ablações sobre direção de grafos, valores de K e arquiteturas GNN.	Misclassificações em ataques específicos (ex: DoS como DDoS) por não usar features de arestas; dependência de qualidade e escala de datasets; problemas de escalabilidade em GAT; necessidade de validação em mais datasets; desbalanceamento de classes afetando generalização.
(HAFID *et al.*, 2025)	2025	Desenvolver e avaliar um framework de detecção de intrusões para ambientes de Internet of Medical Things (IoMT) que fosse simultaneamente preciso, interpretável e sensível aos custos operacionais e de segurança, considerando a criticidade dos sistemas de saúde	XGBoost, Logistic Regression, SHAP	Contexto de IoMT, envolvendo tráfego de rede multi-protocolo (Wi-Fi, Bluetooth e MQTT), dispositivos médicos heterogêneos e atributos de comunicação como origem, destino, protocolo, tamanho e conteúdo informacional dos pacotes.	Os resultados demonstraram que o XGBoost alcançou alta acurácia (97%) e excelente capacidade de detecção, enquanto a fusão tardia apresentou um equilíbrio mais adequado entre precisão e recall, reduzindo falsos negativos e falsos positivos de forma conjunta.	A proposta de um modelo de detecção de intrusões interpretável e orientado a custos, validado em um dataset recente e realista (CIC IoMT 2024), além da análise explícita do trade-off entre segurança e custo operacional.	Forte desbalanceamento das classes, a necessidade de equilibrar precisão e recall em um contexto de alto risco, as limitações computacionais de dispositivos IoMT e a dificuldade de conciliar desempenho elevado com transparência e interpretabilidade dos modelos.
(ZHUKABAYEVA *et al.*, 2025)	2025	Propor e avaliar um framework integrado, baseado em edge computing, para análise de tráfego de rede e detecção de intrusões em sistemas ciberfísicos de Industrial Internet of Things (IIoT), visando aumentar a segurança, reduzir a latência e permitir a identificação de ameaças em tempo real em ambientes industriais.	k-means, DBSCAN, k-Nearest Neighbors, Random Forest, Logistic Regression	Tráfego de rede industrial, comunicação entre sensores, atuadores e dispositivos inteligentes, padrões de tráfego benigno e malicioso, volumes de dados de entrada e saída (IN_BYTES e OUT_BYTES), além da heterogeneidade de dispositivos, protocolos e comportamentos operacionais presentes em redes industriais.	o k-means apresentou boa qualidade de agrupamento, com silhouette score de 0,612, enquanto o DBSCAN obteve 0,473. o Random Forest e o KNN alcançaram desempenho próximo ao ideal, com valores elevados de precisão, recall, F1-score e acurácia, próximos de 0,99 a 1,00, sendo o Random Forest o modelo mais robusto.	Framework integrado que combina análise de tráfego, técnicas de clusterização, modelos de aprendizado de máquina supervisionados e edge computing para segurança em IIoT, validado em um dataset realista (NF-ToN-IoT-V2).	A heterogeneidade e complexidade dos ambientes IIoT, a variabilidade dos padrões de tráfego, o tratamento de grandes volumes de dados em tempo real, o balanceamento entre alta taxa de detecção e baixo número de falsos positivos, além das limitações computacionais e de recursos.
(RAMPONE *et al.*, 2025)	2025	Propor um framework híbrido com aprendizado federado para detecção de intrusões em IoT, garantindo privacidade dos dados, alta acurácia e detecção quase em tempo real sem centralizar informações sensíveis.	Logistic Regression, Support Vector Machine, Stochastic Gradient Descent, Random Forest, Federated Averaging	Ambientes IoT distribuídos, tráfego de rede, pacotes de dados, ataques cibernéticos, heterogeneidade de dispositivos, limitação computacional e preservação de dados locais.	O modelo alcançou alta acurácia, com até 100% no Random Forest, cerca de 98% na Regressão Logística e 97% no SVM, mantendo baixa latência e desempenho próximo ao aprendizado centralizado.	Demonstra a viabilidade do aprendizado federado híbrido para segurança em IoT, unindo privacidade, escalabilidade e detecção eficiente, validado em dados reais de ataques de rede.	Heterogeneidade dos dados, sobrecarga de comunicação, limitação de recursos dos dispositivos, risco de vazamento por atualizações de modelo e complexidade na agregação federada.
(DEVINE *et al.*, 2025)	2025	Desenvolver e avaliar um sistema de detecção de intrusões para redes IoT usando aprendizado federado, reduzindo requisitos computacionais, preservando dados locais e mantendo alta eficiência na detecção de ataques DDoS.	Support Vector Machine, Random Forest, Artificial Neural Network, Isolation Forest, Federated Averaging	Redes IoT distribuídas, tráfego de rede, ataques DDoS, dispositivos com recursos limitados, restrições de memória, consumo energético e comunicação entre nós federados.	O SVM federado alcançou acurácia próxima de 97%, F1-score elevado e desempenho comparável a modelos centralizados, com redução significativa de memória por nó, embora ainda superior a outros algoritmos.	Propõe o primeiro SVM federado aplicado a IDS em IoT, avalia desempenho físico e lógico dos modelos e fornece análise prática sobre viabilidade de aprendizado federado em ambientes IoT reais.	Limitações severas de memória em dispositivos IoT, sobrecarga computacional do SVM, balanceamento entre desempenho e custo físico, fragmentação dos dados e eficiência da agregação federada.
(ADEWOLE *et al.*, 2025)	2025	Visa desenvolver um sistema de detecção de intrusões (IDS) para redes IoT, utilizando métodos de aprendizado de máquina para identificar e explicar padrões de ataques.	XGBoost, CatBoost, Random Forest, Extreme Gradient Boosting, Convolutional Neural Network, Long Short-Term Memory	O estudo focou em diferentes conjuntos de dados de IoT, abordando a segurança de dispositivos heterogêneos e a eficácia de modelos de detecção de anomalias.	O modelo proposto demonstrou alta precisão, com o XGBoost alcançando 99,99% de acurácia, e o LSTM apresentando 99,8% com uma taxa de falso positivo de 0,02%.	O trabalho contribui para a transparência e explicabilidade dos modelos de IDS em IoT, integrando métodos de explicação como LIME e SHAP, além de propor uma abordagem de indução de regras.	Necessidade de grandes volumes de dados para treinamento, a detecção eficiente de rótulos de classes minoritárias e a generalização de algoritmos de extração de características em diferentes conjuntos de dados.

Tabela 10 – Análise dos Artigos

(ORMAN, 2025)	2025	Detectar ciberataques em ambientes de Internet das Coisas Industrial (IIoT) utilizando modelos de aprendizado de máquina e aprendizado profundo.	Random Forest, Logistic Regression, ExtraTreesClassifier, Deep Learnig	O trabalho analisou a segurança de sistemas SCADA e IIoT, focando em vulnerabilidades e tipos comuns de ataques.	O estudo demonstrou que a aplicação de técnicas de pré-processamento, como SMOTE, melhorou significativamente a precisão da classificação, com alguns modelos alcançando quase 100% de precisão.	O trabalho fornece uma análise detalhada das vulnerabilidades de segurança em IIoT, contribuindo para a literatura de cibersegurança e oferecendo insights valiosos para futuras pesquisas.	Os desafios incluíram a necessidade de otimização de hiperparâmetros e a superação de limitações de hardware durante a execução dos modelos.
(ALMOHAIMEED; ALBALWY, 2024)	2024	Desenvolver um modelo preditivo para a detecção precoce de ataques em redes IoT, utilizando seleção de características para melhorar a eficácia dos sistemas de detecção de intrusões (IDS).	Support Vector Machines, Random Forest, Multilayer Perceptron, Deep Learning, Federated Learning	O estudo focou em características de tráfego de rede IoT, como 'Fwd Packet Length Mean', para identificar vulnerabilidades e comportamentos anômalos.	A pesquisa demonstrou que a redução do conjunto de características melhorou a precisão e eficiência do classificador MLP, alcançando uma taxa de acurácia de 95,3% com um conjunto reduzido de 15 características.	O trabalho contribui para a segurança de ecossistemas IoT ao otimizar a seleção de características, facilitando a detecção de ameaças cibernéticas de forma mais eficiente e com menor uso de recursos computacionais.	Os principais desafios incluíram a complexidade da análise de grandes volumes de dados gerados por dispositivos IoT e a necessidade de desenvolver soluções de segurança que sejam eficazes em ambientes com recursos limitados.
(SUKHNI *et al.*, 2024)	2024	Extrair o número ótimo de características para modelos de Machine Learning em ataques multilayer em IoT.	Ensemble, Deep Learning, Gated Recurrent Units	Segurança em múltiplas camadas; Detecção de intrusões	Melhoria na eficiência dos modelos de Machine Learning com a seleção adequada de características, reduzindo o ruído nos dados.	Desenvolvimento de um modelo híbrido eficiente para detecção de intrusões em IoT, integrando expertise humana e algoritmos de Machine Learning.	Dificuldades em adaptar modelos a cenários do mundo real, como interferências e padrões de ataque em evolução, além da latência na detecção devido à natureza distribuída dos agentes móveis.
(MUTAMBIK, 2024)	2024	Desenvolver o IoT-FIDS, um sistema de detecção de intrusões baseado em fluxo para ambientes IoT, visando melhorar a segurança e eficiência na detecção de anomalias.	O artigo não menciona.	Padrões de comunicação de dispositivos, serviços utilizados e detalhes de cabeçalho de pacotes.	O IoT-FIDS detectou a maioria dos padrões de tráfego anormais com mínimas taxas de falsos positivos, demonstrando viabilidade para implementações reais.	Proporciona uma abordagem leve e prática para a segurança de redes IoT, evitando a complexidade dos modelos de machine learning.	A necessidade de simplificar a detecção de anomalias sem depender de dados de ataque pré-rotulados e a adaptação a dispositivos com recursos limitados.
(HANIF; ILYAS, 2024)	2024	Desenvolver um sistema de detecção de intrusões (IDS) para mitigar ataques maliciosos no protocolo MQTT em ambientes de IoT.	XGBoost, Long Short-Term Memory, Gated Recurrent Unit, Naive Bayes, Multi-Layer Perceptron, Random Forest, Gradient Boosting, Neural Networks, Decision Trees, CatBoost	Tráfego legítimo e malicioso no protocolo MQTT.	Alcançou alta precisão e F1-scores ao utilizar um conjunto de dados balanceado para treinar os modelos de ML.	A pesquisa fornece um novo conjunto de dados (MQTTset) e métodos para melhorar a detecção de anomalias em sistemas IoT baseados no protocolo MQTT.	Gerenciamento de grandes volumes de dados gerados por dispositivos IoT e a necessidade de otimização de recursos durante a construção do IDS.
(KAREEM, 2025)	2025	Desenvolver um framework de Sistema de Detecção de Intrusões (IDS) para melhorar a cibersegurança em ambientes de IoT.	XGBoost, LightGBM, Deep Neural Network, Support Vector Machine, Decision Trees	Tráfego de dados imbalanced e complexo, vulnerabilidades a ameaças cibernéticas como DDoS.	Melhorias significativas nas métricas de desempenho: XGBoost: 98.5% de acurácia; LightGBM: 98.3% de acurácia DNN: 98.7% de acurácia; SVM: 97.2% de acurácia; Decision Trees: 96.8% de acurácia	Proposta de um novo framework IDS que combina geração de dados sintéticos e seleção de características bio-inspiradas, melhorando a detecção de ameaças em redes IoT.	Extensa computação necessária para treinamento, restrições em dispositivos de baixo recurso, e a limitação de treinamento offline sem atualização dinâmica.
(SEZGIN; BOYACI, 2023)	2023	Automatizar processos essenciais de cibersegurança, incluindo seleção de características, otimização de hiperparâmetros e seleção de técnicas de machine learning para sistemas de detecção de intrusões em IIoT.	O artigo não menciona.	Interconexão de dispositivos em ambientes industriais (IIoT).	O framework AID4I demonstrou alta precisão na identificação de intrusões, melhorando a segurança e a eficácia dos sistemas de detecção.	Fornecer uma solução abrangente que automatiza o processo de machine learning para melhorar a segurança em redes IIoT.	A necessidade de lidar com dados incompletos e a complexidade da automação de processos de machine learning.
(SCHMITT, 2023)	2023	Integrar sistemas de detecção de intrusões baseados em IA/ML em ecossistemas digitais complexos para melhorar a detecção e mitigação de ameaças cibernéticas.	Decision Tree, Random Forest, K-Nearest Neighbors, Single Layer Neural Networks, Logistic Regression, Gradient Boosting, Deep Learning	Dispositivos IoT com CPUs fracas e a necessidade de modelos de baixa complexidade.	Modelos de ML demonstraram precisão adequada na detecção de ataques, com redes neurais de camada única sendo eficazes em ambientes com recursos limitados.	Proporciona uma visão sobre a integração de soluções de segurança baseadas em IA em sistemas digitais modernos, abordando desafios e propondo direções futuras para pesquisa.	Complexidade na integração de aplicações de ML devido à sua natureza de "caixa-preta", além de questões de resiliência, robustez e explicabilidade.
(SERRANO, 2025)	2025	Desenvolver um modelo CyberAIbot para detecção de ataques cibernéticos em ambientes IoT, utilizando algoritmos de aprendizado de máquina.	Long Short-Term Memory, Support Vector Machine, Deep Neural Networks, Random Forest, Decision Trees, Gradient Boosting, Gaussian Naive Bayes	Comportamento de tráfego de dispositivos IoT; Consumo de energia; Largura de banda; Utilização de memória	O algoritmo LSTM apresentou melhor desempenho em comparação ao SVM, embora detectasse menos tipos de tráfego. A arquitetura proposta resultou em economias significativas em custos operacionais e emissões de CO2.	Introdução de um método ágil que permite a adição de novos algoritmos de classificação à medida que novos ataques são detectados, sem a necessidade de aprendizado prévio.	Definição pré-estabelecida de variáveis e métricas, complexidade na escolha do modelo adequado, e a necessidade de evitar o overfitting ao selecionar características relevantes.
(AFROZ *et al.*, 2025)	2025	Desenvolver um sistema de detecção de intrusões baseado em machine learning para proteger casas inteligentes contra potenciais intrusões.	ensemble, Machine Learning	Comportamentos de rede de dispositivos IoT em ambientes de casas inteligentes.	O modelo demonstrou alta precisão na detecção e mitigação de ameaças cibernéticas em ambientes de casas inteligentes.	Proporciona um modelo de detecção de intrusões que se adapta a novas ameaças, contribuindo para a segurança do ecossistema IoT.	Dificuldades em adaptar soluções às mudanças nas exigências de segurança dos dispositivos IoT e a necessidade de testes em ambientes reais.
(BOUZAACHANE *et al.*, 2025)	2025	Desenvolver um sistema de detecção de intrusões (IDS) para redes de Internet das Coisas (IoT) utilizando técnicas de aprendizado de máquina e aprendizado profundo.	Support Vector Machine, Decision Trees, Adaboost, XGBoost, Random Forest, Gradient Boosting, K-Nearest Neighbors, Long Short-Term Memory	Detecção de ataques raros em dados desbalanceados.	O modelo LSTM-SMOTE demonstrou desempenho superior em comparação com métodos existentes, apresentando maior precisão e menos falsos positivos.	Fornecer uma abordagem prática e adaptável para melhorar a segurança em redes IoT, utilizando um modelo de aprendizado profundo integrado.	Dificuldades em lidar com dados desbalanceados e a necessidade de representar assinaturas de ataque contemporâneas em conjuntos de dados.
(DOGHRAMACHI; AMEEN, 2023)	2023	Modelar ataques em IoT em níveis binários, múltiplos e de sub-classificação utilizando modelos de Machine Learning, abordando o problema de dados desbalanceados.	Logistic Regression, Multilayer perceptron, Decision Tree, Random Forest, XGBoost	Distribuições de classes desbalanceadas nos conjuntos de dados de segurança de IoT.	O uso de técnicas de balanceamento de dados e múltiplos classificadores resultou em melhorias na precisão da detecção de ataques.	Proposta de metodologia que inclui técnicas de pré-processamento de dados e uso de SMOTE para tratar o desbalanceamento de classes.	Dificuldade em escolher a metodologia de Machine Learning ideal para dados específicos e a falta de consideração sobre a classificação e sub-classificação dos tipos de ataque.

Tabela 11 – Análise dos Artigos

(SONG *et al.*, 2025)	2025	Desenvolver um sistema de detecção de intrusões híbrido que utiliza técnicas de machine learning e blockchain para melhorar a segurança em redes de IoT industrial.	XGBoost, Variational Autoencoder, Bidirectional Long Short-Term Memory, K-Nearest Neighbors, Principal Component Analysis	Detecção de anomalias e atividades maliciosas em tráfego de IoT. Seleção de características dinâmicas e heterogêneas para detecção de anomalias.	Alta precisão de detecção (97,43%) utilizando o dataset BOT-IoT. Redução de falsos positivos através da otimização.	Proposta de um modelo de detecção de intrusões que combina machine learning e blockchain, garantindo dados imutáveis e comunicação segura entre dispositivos IoT.	Complexidade na integração de técnicas de aprendizado federado e blockchain. Necessidade de cenários de implantação em tempo real e modelos de aprendizado adaptativos para lidar com ameaças cibernéticas em evolução.
(BANAD *et al.*, 2025)	2025	Analisar a convergência de Inteligência Artificial (IA) e Internet das Coisas (IoT) para otimizar a gestão de energia e a resiliência da rede elétrica.	Machine Learning, Deep Learning, Deep Reinforcement Learning, Multiagent Reinforcement Learning, Federated Learning, Large Language Models	Coleta de dados em tempo real. Integração de dispositivos conectados. Análise de dados para monitoramento e segurança	Identificação de padrões complexos, melhorias na previsão de carga, detecção de anomalias e integração de veículos elétricos com a rede.	Proposição de arquiteturas híbridas que combinam Digital Twins e LLMs para sistemas de energia mais resilientes e autônomos.	Interoperabilidade, privacidade de dados, escalabilidade computacional e explicabilidade dos modelos.
(HOUICHI *et al.*, 2024)	2025	Mitigar desafios de cibersegurança em cidades inteligentes utilizando abordagens proativas e baseadas em dados.	Logistic Regression, Decision Tree, Random Forest, Kernelized Vector Machines, Support Vector Machines	Monitoramento de tráfego de rede em nós de neblina (fog nodes) para detectar atividades normais e anormais.	Modelos como Random Forest e Decision Tree demonstraram alta precisão e desempenho equilibrado em tarefas de classificação.	Fornece insights sobre a eficácia de diferentes modelos de machine learning para detecção de intrusões em redes IIoT, além de destacar a importância de abordagens de aprendizado profundo para futuras pesquisas.	Disparidades no desempenho do SVM e a necessidade de investigar metodologias de pré-processamento e configurações de modelo.
(ALOTAIBI; BARNAWI, 2023)	2023	Desenvolver um sistema de detecção de intrusões baseado em aprendizado federado (FL) para redes IoT, visando melhorar a segurança e a eficiência na detecção de ameaças cibernéticas.	Deep Learning, Gated Recurrent Units, Attention Mechanism, Anomaly Detection	Heterogeneidade dos dispositivos. Distribuição de dados locais. Comunicação síncrona e assíncrona.	O sistema proposto demonstrou melhor desempenho em termos de precisão e privacidade em comparação com abordagens clássicas de ML, além de reduzir o tempo de mitigação de ataques DDoS.	Introdução de um framework de aprendizado federado hierárquico que melhora a detecção de intrusões em redes IoT, integrando mecanismos de atenção e aproveitando a computação na borda.	Alto custo de comunicação e latência na transmissão de dados. Variação na distribuição e número de conjuntos de dados locais. Necessidade de múltiplas iterações para convergência do modelo.
(ZHANG *et al.*, 2025)	2025	Desenvolver um sistema de detecção de intrusões para dispositivos IoT utilizando técnicas de aprendizado de máquina.	Ensemble Learning, Deep Learning, Classificadores diversos (não especificados)	Segurança e privacidade de dados, Interconexão e comunicação entre dispositivos.	O sistema apresentou métricas de desempenho comparáveis a estudos anteriores, com precisão e recall ligeiramente inferiores, mas com maior precisão e F1-score em alguns casos.	Proporciona uma abordagem eficaz e preservadora de privacidade para a detecção de intrusões em ambientes IoT, abordando a sobrecarga de dados e questões de segurança.	Gerenciamento do grande volume de dados gerados por dispositivos IoT e a necessidade de processamento descentralizado para evitar problemas de privacidade e segurança.
(WAKILI; BAKKALI, 2025)	2025	Desenvolver um framework de detecção de intrusões em IoT que seja resiliente, interpretável e eficiente.	Neural Networks LSTM, Ensemble, Random Forest, SMOTE	Ambientes de dispositivos heterogêneos. Desafios de implementação em ambientes com recursos limitados	99.16% de precisão, 73.79% de macro F1-score, 0.9908 MCC em 33 categorias de ataque	Avanço na cibersegurança de IoT com benefícios sociais e econômicos, promovendo resiliência cibernética e confiança digital.	Falhas de componentes individuais sem mecanismos de fallback. Desbalanceamento extremo nas classes de ataque. Complexidade na implementação de estratégias adaptativas
(MANI; VIVEKANANDAN, 2025)	2025	Desenvolver uma metodologia de segurança inteligente para detectar intrusões em redes HetIoT.	Deep Learning, Convolutional Neural Networks, Long Short-Term Memory, Decision Tree, Logistic Regression, Stochastic Gradient Descent, Stacking Classifier	Heterogeneidade dos dispositivos. Volume de dados gerados	A metodologia proposta demonstrou maior taxa de reconhecimento e precisão em comparação com técnicas tradicionais, além de menor complexidade computacional.	Apresentação do modelo Dip-DARK, que integra técnicas de deep learning para atender às demandas de segurança específicas das redes HetIoT.	Aumento do tempo de treinamento e teste. Alta complexidade computacional. Problemas de overfitting e underfitting devido à limpeza inadequada dos dados. Necessidade de conjuntos de dados rotulados completos para treinamento eficaz.
(KANNADHASAN; NAGARAJAN, 2024)	2024	Desenvolver um sistema de detecção de intrusões (IDS) eficiente e consciente de energia para redes IoT, utilizando aprendizado de máquina.	Filtered Deep Learning Neural Network, Interval Type-2 Adaptive Neuro-Fuzzy Inference System, Lightweight Fuzzy Enhanced Hybrid Optimization	Autenticação de dispositivos, Comunicação entre sensores IoT, Transmissão segura de dados para a nuvem	Eficácia máxima de amostragem de pacotes de 97%, Acurácia de 96,12% para 500 nós no FDLNN, Desempenho superior do LFEHO em comparação com métodos existentes	Proposta de um sistema de IDS que combina algoritmos avançados para melhorar a segurança e eficiência em redes IoT.	Dificuldade em integrar armazenamento em nuvem eficiente com detecção de intrusões e identificação de ataques zero-day em redes IoT.
(DJENOURI *et al.*, 2023)	2023	Desenvolver um framework para detecção de intrusões na Internet das Coisas de próxima geração (NG-IoT).	Recurrent Neural Network, Marine Predator Algorithm, MinMax Normalization, Attention Mechanism, Shapley Values	Autonomia e adaptabilidade dos dispositivos. Segurança nas comunicações entre nós NG-IoT. Processamento e análise de grandes volumes de dados	Taxas de mais de 94% para verdadeiros negativos e positivos na detecção de intrusões, superando métodos existentes que ficam abaixo de 90%.	Proposta de um modelo de rede neural recorrente interpretável (IRNN) que melhora a detecção de intrusões e fornece explicações sobre a contribuição de cada recurso no processo de detecção.	Dificuldades em garantir a segurança e a eficiência do processamento de dados em dispositivos IoT com recursos limitados, além da necessidade de detectar novos padrões de ataque em tempo real.
(ALAHMARI; ALKHARASHI, 2025)	2025	Desenvolver um sistema de detecção de intrusões (IDS) que preserve a privacidade em ambientes de Internet das Coisas (IoT) utilizando aprendizado federado.	Chameleon Swarm Algorithm, Self-Attentive Variational Autoencoder, Osprey Optimization Algorithm	Segurança e privacidade de dados gerados por dispositivos IoT.	O modelo PEFLID-CSAAI demonstrou desempenho superior em precisão, recall e F1 score em comparação com métodos recentes, utilizando o conjunto de dados BoT-IoT.	Proporciona uma solução escalável e eficaz para a segurança em IoT, respeitando as restrições de privacidade e computacionais.	Limitações na generalização do modelo para outros ambientes IoT e a falta de avaliação em implementações em tempo real.
(BAKHSH *et al.*, 2023)	2023	Desenvolver sistemas de detecção de intrusões baseados em Deep Learning para melhorar a segurança em redes IoT.	Convolutional Neural Networks, Random Forest, Support Vector Machine, Recurrent Neural Networks, XGBoost, Deep Convolutional Neural Network	Vulnerabilidades e ataques em redes IoT. Necessidade de sistemas de detecção de intrusões (IDS). Desempenho e eficiência em dispositivos IoT de baixo consumo	Atingiu uma precisão de 98,68% na detecção de ataques com o classificador Random Forest. O modelo DCNN alcançou 77,55% de precisão utilizando o dataset IoTID20.	Proposta de um framework de IDS baseado em DL que melhora a detecção de intrusões e oferece soluções adaptáveis para diferentes tipos de usuários em ambientes IoT.	Necessidade de desenvolver algoritmos DL mais eficientes. Superar limitações de complexidade e tempo de classificação em dispositivos IoT. Lidar com a crescente sofisticação dos ataques cibernéticos.
(AKSHAYA *et al.*, 2023)	2023	Melhorar a segurança e a detecção de ataques em redes IoT.	Convolutional Neural Networks, LSTM, ESFCM, HCNN, EHOA, KH-AES, PSO-CNN	Detecção de ataques em dispositivos IoT, incluindo Raspberry Pi, e análise de tráfego de rede.	96% de precisão na detecção de ataques e melhorias significativas em comparação com métodos de detecção de ataques baseados em DL existentes.	Proposta de um modelo de detecção de ataques que melhora a precisão e a eficiência na identificação de ameaças em ambientes IoT.	Dificuldades em reconhecer ataques devido a conjuntos de dados desatualizados e limitações nas estratégias de detecção existentes.

Tabela 12 – Análise dos Artigos

(KESHK *et al.*, 2023)	2023	Desenvolver um framework de detecção de intrusões explicável para redes IoT, melhorando a interpretabilidade e a explicabilidade dos sistemas de defesa cibernética.	Long Short-Term Memory, Shapley Additive Explanations, Permutation Feature Importance, Individual Conditional Expectation, Partial Dependence Plot	Proliferação de dispositivos heterogêneos, geração de dados em alta dimensão e multimodalidade.	O framework proposto demonstrou eficácia em melhorar a interpretabilidade e a explicabilidade dos sistemas de defesa cibernética em redes IoT.	A introdução de métodos de XAI em modelos de detecção de intrusões, promovendo uma melhor compreensão do comportamento de ataques complexos.	A complexidade crescente dos modelos de detecção de intrusões baseados em IA, dificultando a interpretação e aplicação em setores críticos, como a defesa cibernética.
(AMUTHADEVI *et al.*, 2025)	2025	Desenvolver um sistema de detecção de intrusões leve e de baixo consumo de energia utilizando Tiny Machine Learning (TinyML) para detecção em tempo real de ameaças em dispositivos IoT.	Gradient Boosting, Adaptive Artificial Gorilla Troops Optimization, XGBoost, Autoencoders, Support Vector Machines, Artificial Neural Networks, Decision Trees, Random Forests	Desempenho em dispositivos de ultra-baixo consumo de energia e capacidade de adaptação em tempo real.	O modelo GraBoost-AAGT alcançou mais de 99,50% de precisão, 99,8% de precisão, 99,12% de recall, 99,45% de F1-score e 99,81% de especificidade, com um tempo de computação de 4,5 segundos.	Proporciona uma arquitetura de segurança escalável e sustentável para IoT, otimizando a detecção de ameaças em ambientes com restrições de energia.	Custos iniciais de implantação, limitações de energia sob ataques de alta frequência e capacidades de transferência de dados restritas em ambientes de ultra-baixo consumo.
(ULLAH *et al.*, 2025)	2025	O objetivo é analisar o comportamento de tráfego de IoT e detectar atividades de botnets utilizando um conjunto de características específicas.	Anomaly Detection Algorithms, Neural Networks, Decision Trees, Support Vector Machines	Duração do Fluxo, Comprimento do Cabeçalho, Tipo de Protocolo, Tamanho do Pacote, Tempo de Inter- chegada	Os resultados mostraram a eficácia na detecção de comportamentos maliciosos em dispositivos IoT, com alta taxa de precisão e baixa taxa de falsos positivos.	A pesquisa contribui para o desenvolvimento de sistemas de segurança mais robustos para IoT, melhorando a detecção de botnets e a proteção de dispositivos vulneráveis.	Os principais desafios incluíram a limitação de recursos dos dispositivos IoT, a diversidade de protocolos e a necessidade de minimizar a latência na detecção de anomalias.
(AHMAD *et al.*, 2022)	2022	Desenvolver um modelo de detecção de ciberataques baseado em Deep Learning (DL) para melhorar a segurança em sistemas de Internet das Coisas (IIoT).	Deep Learning, Random Neural Network, Particle Swarm Optimization, Sequential Quadratic Programming	Detecção de anomalias em tráfego de rede. Classificação de tipos de ataques	O modelo proposto apresentou altas taxas de precisão na detecção de ciberataques, superando outros sistemas de detecção de intrusões (IDS) em configurações binárias e multiclasses.	Introdução de um modelo de detecção de ciberataques eficiente e rápido, utilizando uma arquitetura avançada de rede neural e técnicas de otimização para melhorar a segurança em ambientes IIoT.	Dificuldades na representação de ambientes IIoT reais, necessidade de otimização de hiperparâmetros e a escassez de avaliações multiclasses em trabalhos anteriores.
(BERGUIGA *et al.*, 2023)	2023	Desenvolver um sistema de detecção de intrusões inteligente para sistemas IoT utilizando algoritmos de deep learning.	Convolutional Neural Networks, Long Short-Term Memory, Support Vector Machine, Decision Tree, Gated Recurrent Unit	Anomalias no tráfego de rede e comportamento anômalo em tempo real.	Alta taxa de detecção, baixa taxa de falsos positivos e desempenho superior em comparação com métodos tradicionais.	Proposta de uma abordagem distribuída para melhorar a segurança em sistemas IoT complexos.	Dependência da confiabilidade e segurança dos dispositivos de borda e nós de névoa, além da necessidade de dados rotulados e consideração da dinâmica das redes IoT.
(QURESHI *et al.*, 2025)	2025	Desenvolver um sistema de Detecção de Intrusões (IDS) baseado em IA para ambientes de Internet das Coisas Industrial (IIoT) que mitigue ameaças cibernéticas.	LSTM, GRU, Random Forest, Decision Tree, Naïve Bayes , K-Nearest Neighbors, Support Vector Machine	Segurança em ambientes de IIoT e a capacidade de detecção em tempo real de anomalias.	Taxa de detecção de 98,68%, taxa de falso negativo de 0,01% e F1 Score de 98,62%.	Aprimoramento das medidas de segurança em nuvem, proporcionando um sistema de IDS eficaz e adaptável para ambientes IIoT.	Limitações de recursos computacionais em dispositivos IIoT e a complexidade na aplicação de algoritmos de IDS mais avançados.
(ALNASSER *et al.*, 2025)	2025	Desenvolver um sistema de detecção de intrusões (IDS) híbrido para mitigar ameaças cibernéticas em ambientes de comunicação veicular e redes inteligentes.	Long Short-Term Memory, Support Vector Machine, Random Forest, Recurrent Neural Network	Comunicação veicular e redes inteligentes (smart grids).	O modelo proposto superou significativamente SVM, Random Forest e RNN em todas as métricas, com uma taxa de throughput de 7800 fluxos por segundo e latência aceitável para aplicações em tempo real.	Proposta de um modelo híbrido que combina detecção baseada em assinatura e anomalia, melhorando a identificação de vetores de ataque novos e conhecidos.	Necessidade de intervenção humana para validação de alertas devido à geração de falsos positivos e a demanda por recursos computacionais elevados para detecção de anomalias.
(AMMAR *et al.*, 2025)	2025	Desenvolver um sistema de detecção de intrusões para a Internet das Coisas (IoT) utilizando técnicas de aprendizado de máquina.	Convolutional Neural Network, Variational Autoencoder, Generative Adversarial Networks, Grasshopper Optimization Algorithm, Random Forest	Classe de desequilíbrio. Dados rotulados limitados. Necessidade de ajuste de hiperparâmetros	Melhoria na eficácia da detecção de intrusões, superando limitações de métodos tradicionais.	Proposta de um sistema de detecção de intrusões mais robusto e eficiente para ambientes de IoT.	Dificuldades com a classe de desequilíbrio, escassez de dados rotulados e complexidade no ajuste de hiperparâmetros.
(CHEN *et al.*, 2024)	2024	Desenvolver um sistema de detecção de intrusões (NIDS) para redes IoT utilizando técnicas de aprendizado de máquina e aprendizado profundo.	SMOTE, XGBoost, Recurrent Neural Networks, Expectation-Maximization, Ensemble Learning, Pseudo-Siamese Stacked Autoencoders, Neural Networks	Tráfego de rede. Recursos limitados dos dispositivos IoT	Desempenho promissor na detecção de ataques, com melhorias na precisão e eficiência do sistema.	Integração de técnicas de aprendizado de máquina e profundo para aprimorar a detecção de intrusões em ambientes IoT, especialmente em contextos com recursos limitados.	Dificuldade em treinar modelos devido à escassez de dados em classes raras e a necessidade de técnicas especiais para lidar com amostras limitadas.
(FAROOQ *et al.*, 2025)	2025	Desenvolver um framework integrado de detecção de intrusões cibernéticas para cidades inteligentes, combinando aprendizado federado, seleção de características que preservam a privacidade e técnicas de inteligência artificial explicável.	Deep Neural Network, Convolutional Neural Network, Long Short-Term Memory, Synthetic Minority Over-sampling Technique, Bidirectional Gated Recurrent Unit, Random Forest	Segurança em redes de IoT, Detecção de intrusões em ambientes complexos e dinâmicos	Alcançou uma precisão de 98,7% no conjunto de dados BoT-IoT, com um equilíbrio entre desempenho e interpretabilidade.	Proporciona um modelo de detecção de intrusões que garante privacidade, aprendizado colaborativo e decisões explicáveis, adaptadas para ambientes urbanos digitais.	Custo computacional elevado dos modelos de aprendizado profundo. Complexidade na escalabilidade do sistema. Necessidade de garantir a privacidade dos dados durante o treinamento do modelo.
(BENMALEK *et al.*, 2025)	2025	Desenvolver um modelo de detecção de intrusões, chamado SNN-IoMT, para ambientes de Internet das Coisas Médicas (IoMT).	Machine Learning , Deep Learning , Ensemble methods, Swarm-Neural Network, MNB, LR, LRSGD, LSVC, BG, GBC, RF, ADB, XGB	Segurança e privacidade em ambientes de IoMT.	O modelo SNN-IoMT superou frameworks existentes em precisão, com uma taxa de acurácia de 99,76%.	O trabalho aborda desafios em sistemas de saúde baseados em IA, melhorando a segurança e a confiança em ambientes IoMT.	Dificuldades em lidar com dados complexos gerados por IoMT e a necessidade de garantir a privacidade e a integridade dos dados dos pacientes.
(ELSAYED *et al.*, 2023)	2023	Propor um Sistema de Detecção de Intrusões Automático e Seguro (SATIDS) baseado em uma rede LSTM aprimorada para diferenciar entre tráfego de ataque e benigno em ambientes de IoT.	Long Short-Term Memory, One-class Support Vector Machine, Decision Tree, Naive Bayes, Random Forest	Tráfego de rede (normal e anômalo), Segurança e privacidade em ambientes de IoT	96.35% de precisão e 96% de taxa de detecção para o dataset ToN-IoT. 99.73% de precisão e 98.6% de taxa de detecção para o dataset InSDN	Desenvolvimento de um sistema de detecção de intrusões que supera outros sistemas existentes em termos de precisão e taxa de detecção, contribuindo para a segurança em redes IoT.	Dificuldade em distinguir entre comportamentos normais e anormais em um ambiente dinâmico e em larga escala. Necessidade de métodos novos para lidar com grandes volumes de dados gerados por IoT. Complexidade na aprendizagem de características que diferenciam tráfego normal de anômalo.

Tabela 13 – Análise dos Artigos

(VS *et al.*, 2025)	2025	Investigar frameworks de detecção de intrusões (IDS) baseados em deep learning e blockchain aplicáveis a sistemas de controle industrial (ICS).	Wide and Deep Neural Network, Deep Feedforward Neural Network, Multi-feature Data Clustering Optimization Model, Ensemble Attack Detection SAE, ModelBidirectional Simple Recurrent Unit	Segurança em redes de controle industrial e a integração de tecnologias de blockchain para gerenciamento de dados e confiança.	Modelos demonstraram alta precisão, com taxas de acurácia de 99.29% e 99.88% em conjuntos de dados IoT-Botnet e ToN-IoT, respectivamente.	Estabelece uma base para futuras pesquisas sobre a interseção de deep learning e blockchain na detecção de intrusões em ICS, além de propor arquiteturas adaptadas para esse contexto.	Falta de conjuntos de dados em tempo real, Dificuldades na detecção instantânea de ataques, Preocupações com a reprodutibilidade dos resultados, Complexidade computacional dos modelos, Necessidade de discussões sobre a eficácia do sistema.
(ALSOUFI *et al.*, 2024)	2025	Desenvolver e aprimorar um sistema de detecção de intrusões baseado em anomalias (AIDS) para redes IoT.	Sparse Autoencoder, Convolutional Neural Network	Alta dimensionalidade dos dados. Volume elevado de dados não estruturados. Recursos computacionais limitados	Acurácia: 99.9%. Precisão: 99.9% Recall: 100%. F1: 99.9%. Taxa de Falsos Positivos (FPR): 0.0003. Taxa de Verdadeiros Positivos (TPR): 0.9992	Desenvolvimento de um modelo de redução de dimensionalidade e um sistema de detecção de intrusões otimizado para redes IoT, validado com um dataset recente.	Necessidade de características leves para IDS em IoT. Dificuldade em encontrar datasets atualizados sobre padrões de ameaças. Complexidade na otimização de características do sistema.
(BHUKYA *et al.*, 2025)	2025	Desenvolver um modelo híbrido de aprendizado profundo integrado com técnicas de otimização para melhorar a segurança de sistemas SCADA contra ameaças cibernéticas.	Long Short-Term Memory, Sparse Variational Autoencoder, Bidirectional Recurrent Neural Network, Deep Convolutional Neural Networks, Ensemble Feature Selection	Heterogeneidade e escala dos dados gerados por dispositivos e protocolos diversos em redes SCADA.	Melhoria nas taxas de detecção e redução de falsos positivos, com eficiência computacional demonstrada em diferentes métricas.	Proporcionar uma nova abordagem para a detecção de intrusões em ambientes críticos, integrando técnicas de aprendizado de máquina e profundo para enfrentar ameaças cibernéticas emergentes.	Dificuldades na generalização dos modelos devido à natureza dinâmica e evolutiva das ameaças, além da alta complexidade e custo computacional dos algoritmos em ambientes com recursos limitados.
(YAN *et al.*, 2024)	2025	Desenvolver um framework de detecção de intrusões para IoT, denominado MUS, utilizando técnicas de aprendizado profundo e métodos de processamento de imagem.	Deep Neural Networks, Markov Transition Fields, Unsharp Masking, Soft-voting integration, MobileNet, VGGNet, ResNet	Tráfego de rede de dispositivos inteligentes. Diversidade de tipos de ataques e ambientes de rede	Aumento significativo na precisão da detecção de tráfego de ataque, com resultados experimentais mostrando eficácia em diferentes cenários de ataque e ambientes de rede.	Proposta de um framework de detecção de intrusões que combina técnicas de conversão de dados e integração de modelos, melhorando a performance em ambientes IoT.	Limitações na seleção de datasets, necessidade de otimização para restrições de recursos e a complexidade crescente do ambiente de rede IoT.
(BHARDWAJ *et al.*, 2022)	2022	Revisar e fornecer técnicas de detecção de intrusões eficazes e eficientes para sistemas de IoT, abordando as lacunas nos modelos tradicionais de IDS.	Proof of Work (PoW), Proof of Elapsed Time (PoET), Proof of Stake (PoS), Random Forest Classifier, Tree-based ML approaches	Segurança das interações de IoT, Monitoramento contínuo do tráfego de rede, Detecção de comportamentos suspeitos	O método sugerido apresentou menor latência, maior throughput e uma conexão IoT mais confiável, com melhorias de 13% em throughput, 39% na taxa de queda de dados, 11% na latência de dados e 46% em pacotes defeituosos.	Desenvolvimento de um framework de segurança baseado em SDN e NFV, com um protocolo de consenso inovador para identificar e relatar nós IoT suspeitos.	Alta taxa de falsos positivos em algoritmos de ML. Overfitting devido a dados ruidosos. Complexidade na não linearidade dos dados. Necessidade de melhorar a eficiência dos métodos de deep learning na detecção de ataques.
(SHIN *et al.*, 2024)	2024	Analisar e melhorar a detecção de intrusões em redes de Internet das Coisas (IoT) utilizando técnicas de aprendizado de máquina.	Random Forest, XGBoost, CatBoost, LightGBM, Deep Neural Networks, Decision Tree, Support Vector Machine, k-Nearest Neighbors	Tráfego de rede e dados relacionados a dispositivos.	A metodologia proposta alcançou uma precisão de 99%, recall de 98% e F1-score de 98% na detecção de intrusões.	Reforço da segurança em redes IoT, redução de falsos negativos e orientação para futuras pesquisas em sistemas de detecção de intrusões.	Classificação de dados desbalanceados e a necessidade de técnicas de pré-processamento eficazes para manter a integridade dos dados.
(FARES *et al.*, 2025)	2025	Desenvolver um sistema de detecção de intrusões (IDS) baseado em Machine Learning para melhorar a segurança em infraestruturas de IoT.	Long Short-Term Memory, Convolutional Neural Network, Transformer, TabNet	Tráfego de rede. Vulnerabilidades de dispositivos. Padrões de ataque	Melhoria na detecção de ataques cibernéticos com alta taxa de precisão e redução de falsos positivos.	Proposta de um framework inovador que integra técnicas de aprendizado de máquina para fortalecer a segurança em ambientes IoT.	Dificuldades em lidar com a heterogeneidade dos dispositivos IoT, escassez de dados para treinamento e a necessidade de otimização para processamento em tempo real.
(GHENI; AL-YASEEN, 2024)	2024	Construir um sistema de detecção de intrusões utilizando algoritmos de aprendizado profundo com base no novo conjunto de dados CICIoT2023.	BiLSTM, Random Forest, Catboost, MLP, DNN, CNN, RNN, KNN	O conjunto de dados CICIoT2023 inclui 232,885 conexões com 47 características, abrangendo 33 sub-ataques em sete classificações de ataque.	Redução de 62,45% no tamanho do conjunto de dados, melhorando a precisão e o tempo de implementação do sistema de detecção de intrusões.	Proposta de um novo modelo de detecção de intrusões que melhora a eficiência e a eficácia dos sistemas de detecção, além de sugerir a aplicação de outros algoritmos de aprendizado profundo.	Altas dimensões dos conjuntos de dados de detecção de intrusões e a necessidade de otimização para melhorar a eficiência do modelo.
(WAKILI *et al.*, 2025)	2025	Desenvolver um framework de segurança para IoT na área da saúde, utilizando tecnologias emergentes como machine learning e digital twins.	Support Vector Machine, Neural Networks, Random Forest	Segurança de dados. Análise de tráfego de rede. Detecção de anomalias	Melhoria na detecção de ameaças e na previsão de comportamentos anômalos em dispositivos IoT na saúde.	Proposta de um framework que integra múltiplas tecnologias para aumentar a segurança e a eficiência em ambientes de saúde conectados.	Alto custo computacional e a necessidade de validação em cenários do mundo real.

Tabela 14 – Análise dos Artigos

APÊNDICE B – TABELAS DE TERMOS DE ASSOCIAÇÕES

Artigos	Objetivo	Caracteristicas de IoT Analisadas	Resultado	Contribuição	Desafios
1	Explorar eficácia IA	Vulnerabilidades e Ameaças	Melhoria desempenho	Análise abrangente	Limitações e Restrições
2	Desenvolver framework segurança	Tráfego de Rede	Alta precisão	Análise abrangente	Necessidade de Melhoria
3	Explorar eficácia IA	Vulnerabilidades e Ameaças	Eficácia comprovada	Análise abrangente	Necessidade de Melhoria
4	Propor metodologia segurança	Tráfego de Rede	Alta precisão	Abordagem inovadora	Limitações e Restrições
5	Revisar técnicas IDS	Restrições de Recursos	Alta precisão	Análise abrangente	Limitações e Restrições
6	Analisar técnicas detecção	Restrições de Recursos	Alta precisão	Taxonomia abrangente	Complexidade e Dificuldade
7	Explorar eficácia IA	Vulnerabilidades e Ameaças	Redução de custos	Abordagem inovadora	Necessidade de Melhoria
8	Investigar abordagens segurança	Comunicação de Dados	Melhoria desempenho	Análise abrangente	Complexidade e Dificuldade
9	Propor metodologia segurança	Segurança e Dados	Alta precisão	Desenvolvimento de framework	Complexidade e Dificuldade
10	Aprimorar segurança redes	Vulnerabilidades e Ameaças	Eficácia comprovada	Melhorar segurança	Necessidade de Melhoria
11	Desenvolver framework segurança	Segurança e Dados	Eficácia comprovada	Desenvolvimento de framework	Necessidade de Melhoria
12	Analisar técnicas detecção	Vulnerabilidades e Ameaças	Eficácia comprovada	Melhorar segurança	Necessidade de Melhoria
13	Aprimorar segurança redes	Vulnerabilidades e Ameaças	Alta precisão	Abordagem inovadora	Complexidade e Dificuldade
14	Segurança em Redes IoT	Tráfego de Rede	Alta precisão	Desenvolvimento de framework	Necessidade de Melhoria
15	Desenvolver framework segurança	Intrusão em dados durante	Eficácia comprovada	Melhorar segurança	Necessidade de Melhora
16	Desenvolver framework segurança	Vulnerabilidades e Ameaças	Melhoria desempenho	Desenvolvimento de framework	Necessidade de Melhoria
17	Analisar técnicas detecção	Segurança e Dados	Detecção eficaz	Taxonomia abrangente	Limitações e Restrições
18	Propor metodologia de segurança	Comportamento de Dispositivos	Alta precisão	Taxonomia abrangente	Necessidade de Melhoria
19	Desenvolver framework segurança	Detecção de Anomalias	Melhoria desempenho	Melhorar segurança	Necessidade de Melhoria
20	Desenvolver framework segurança	Comportamento de Dispositivos	Eficácia comprovada	Desenvolvimento de framework	Complexidade e Dificuldade
21	Explorar eficácia IA	Conectividade e Integração	Eficácia comprovada	Abordagem inovadora	Necessidade de Melhoria
22	Revisar técnicas IDS	Tráfego de Rede	Alta precisão	Taxonomia abrangente	Limitações e Restrições
23	Investigar abordagens segurança	Segurança e Dados	Melhoria desempenho	Visão equilibrada	Ameaças Emergentes
24	Propor metodologia segurança	Detecção de Anomalias	Melhoria desempenho	Melhorar segurança	Complexidade e Dificuldade
25	Desenvolver framework segurança	Segurança e Dados	Eficácia comprovada	Desenvolvimento de framework	Complexidade e Dificuldade
26	Investigar abordagens segurança	Detecção de Anomalias	Eficácia comprovada	Análise abrangente	Complexidade e Dificuldade
27	Revisar técnicas IDS	Conectividade e Integração	Eficácia comprovada	Análise abrangente	Necessidade de Melhoria
28	Propor metodologia segurança	Detecção de Anomalias	Eficácia comprovada	Melhorar segurança	Complexidade e Dificuldade
29	Desenvolver framework segurança	Detecção de Anomalias	Eficácia comprovada	Desenvolvimento de framework	Necessidade de Melhoria
30	Propor metodologia segurança	Privacidade de Dados	Eficácia comprovada	Análise abrangente	Ameaças Emergentes
31	Desenvolver framework segurança	Sistemas de IoT	Alta precisão	Melhorar segurança	Limitações e Restrições
32	Avaliar métodos comunicação	Conectividade e Integração	Detecção eficaz	Análise abrangente	Limitações e Restrições
33	Desenvolver framework segurança	Conectividade e Integração	Eficácia comprovada	Desenvolvimento de framework	Necessidade de Melhoria
34	Avaliar métodos comunicação	Sistemas de IoT	Eficácia comprovada	Desenvolvimento de framework	Complexidade e Dificuldade
35	Analisar técnicas detecção	O artigo não menciona	Melhoria desempenho	Visão equilibrada	Complexidade e Dificuldade
36	Aprimorar segurança de redes	O artigo não menciona	Alta precisão	Melhorar segurança	Limitações e Restrições
37	Investigar abordagens de segurança	Conectividade e Integração	Eficácia comprovada	Análise abrangente	Desafios de Segurança
38	Avaliar métodos comunicação	O artigo não menciona	Eficácia comprovada	Taxonomia abrangente	Complexidade e Dificuldade
39	Revisar técnicas IDS	Conectividade e Integração	Detecção eficaz	Taxonomia abrangente	Complexidade e Dificuldade
40	Explorar eficácia IA	Segurança e Dados	Detecção eficaz	Melhorar segurança	Desafios de Segurança
41	Investigar abordagens segurança	O artigo não menciona	Detecção eficaz	Análise abrangente	Complexidade e Dificuldade
42	Analisar técnicas detecção	Conectividade e Integração	Melhoria desempenho	Análise abrangente	Necessidade de Melhoria
43	Realizar uma revisão sistemática	Comunicação de Dados	Melhoria desempenho	Análise abrangente	Limitações e Restrições
44	Explorar eficácia IA	Conectividade e Integração	Detecção eficaz	Taxonomia abrangente	Ameaças Emergentes
45	Avaliar métodos comunicação	Automação e Controle	Redução de custos	Análise abrangente	Necessidade de Melhoria
46	Investigar abordagens segurança	Segurança e Dados	Alta precisão	Desenvolvimento de framework	Limitações e Restrições
47	Avaliar métodos comunicação	O artigo não menciona	Redução de custos	Visão equilibrada	Complexidade e Dificuldade
48	Analisar técnicas de detecção	Tráfego de Rede	Melhoria de desempenho	Desenvolvimento de framework	Complexidade e Dificuldade
49	Propor metodologia de segurança	Tráfego de Rede	Melhoria de desempenho	Abordagem inovadora	Desafios de Segurança
50	Aprimorar segurança de redes	Sistemas de IoT	Alta precisão	Desenvolvimento de framework	Limitações e Restrições
51	Analisar técnicas de detecção	Vulnerabilidade e Ameaças	Alta precisão	Melhorar segurança	Desafios de Segurança
52	Desenvolver framework de segurança	Restrições de Recursos	Melhoria de desempenho	Desenvolvimento de framework	Complexidade e Dificuldade
53	Propor metodologia de segurança	Vulnerabilidade e Ameaças	Alta precisão	Abordagem inovadora	Limitações e Restrições
54	Propor metodologia de segurança	Vulnerabilidade e Ameaças	Eficácia comprovada	Abordagem inovadora	Ameaças Emergentes
55	Propor metodologia de segurança	Vulnerabilidade e Ameaças	Melhoria de desempenho	Desenvolvimento de framework	Limitações e Restrições
56	Revisar técnica de IDS	Sistemas de IoT	Melhoria de desempenho	Análise abrangente	Complexidade e Dificuldade
57	Investigar abordagens de segurança	Vulnerabilidade e Ameaças	Eficácia comprovada	Análise abrangente	Desafios de Segurança
58	Investigar abordagens de segurança	Sistemas de IoT	Eficácia comprovada	Taxonomia abrangente	Limitações e Restrições
59	Desenvolver framework de segurança	Tráfego de Rede	Eficácia comprovada	Taxonomia abrangente	Limitações e Restrições
60	Desenvolver framework de segurança	Sistemas de IoT	Melhoria de desempenho	Abordagem inovadora	Limitações e Restrições

Tabela 15 – Termos de Associações dos Artigos

61	Desenvolver framework de segurança	Sistemas de IoT	Alta precisão	Desenvolvimento de framework	Limitações e Restrições
62	Desenvolver framework de segurança	Sistemas de IoT	Eficácia comprovada	Desenvolvimento de framework	Desafios de Segurança
63	Propor metodologia de segurança	Sistemas de IoT	Eficácia comprovada	Desenvolvimento de framework	Complexidade e Dificuldade
64	Propor metodologia de segurança	Sistemas de IoT	Melhoria de desempenho	Desenvolvimento de framework	Limitações e Restrições
65	Desenvolver framework de segurança	Tráfego de Rede	Eficácia comprovada	Abordagem inovadora	Limitações e Restrições
66	Desenvolver framework de segurança	Restrições de Recursos	Melhoria de desempenho	Desenvolvimento de framework	Complexidade e Dificuldade
67	Desenvolver framework de segurança	Sistemas de IoT	Melhoria de desempenho	Desenvolvimento de framework	Limitações e Restrições
68	Desenvolver framework de segurança	Tráfego de Rede	Melhoria de desempenho	Desenvolvimento de framework	Complexidade e Dificuldade
69	Desenvolver framework de segurança	Tráfego de Rede	Alta precisão	Desenvolvimento de framework	Desafios de Segurança
70	Desenvolver framework de segurança	Tráfego de Rede	Alta precisão	Desenvolvimento de framework	Limitações e Restrições
71	Propor metodologia de segurança	Tráfego de Rede	Alta precisão	Desenvolvimento de framework	Limitações e Restrições
72	Explorar eficácia AI	Sistemas de IoT	Alta precisão	Desenvolvimento de framework	Limitações e Restrições
73	Analisar técnicas de detecção	Vulnerabilidade e Ameaças	Alta precisão	Melhorar segurança	Complexidade e Dificuldade
74	Propor metodologia de segurança	Tráfego de Rede	Alta precisão	Melhorar segurança	Limitações e Restrições
75	Propor metodologia de segurança	Segurança e Dados	Melhoria de desempenho	Desenvolvimento de framework	Complexidade e Dificuldade
76	Aprimorar segurança de redes	Comunicação de Dados	Melhoria de desempenho	Desenvolvimento de framework	Complexidade e Dificuldade
77	Aprimorar segurança de redes	Tráfego de Rede	Detecção eficaz	Melhorar segurança	Limitações e Restrições
78	Desenvolver framework de segurança	Tráfego de Rede	Alta precisão	Melhorar segurança	Necessidade de Melhoria
79	Propor metodologia de segurança	Conectividade e Integração	Melhoria de desempenho	Desenvolvimento de framework	Limitações e Restrições
80	Explorar eficácia AI	Restrições de Recursos	Detecção eficaz	Desenvolvimento de framework	Complexidade e Dificuldade
81	Explorar eficácia AI	Comportamento de Dispositivos	Detecção eficaz	Melhorar segurança	Desafios de Segurança
82	Aprimorar segurança de redes	Comportamento de Dispositivos	Redução de custos	Abordagem inovadora	Complexidade e Dificuldade
83	Explorar eficácia AI	Tráfego de Rede	Detecção eficaz	Melhorar segurança	Limitações e Restrições
84	Analisar técnicas de detecção	Tráfego de Rede	Alta precisão	Melhorar segurança	Complexidade e Dificuldade
85	Aprimorar segurança de redes	Tráfego de Rede	Melhoria de desempenho	Desenvolvimento de framework	Complexidade e Dificuldade
86	Aprimorar a segurança de redes	Sistemas de IoT	Alta precisão	Desenvolvimento de framework	Necessidade de Melhoria
87	Não aplicável	Tráfego de Rede	Não aplicável	Não aplicável	Limitações e Restrições
88	Propor metodologia de segurança	Sistemas de IoT	Alta precisão	Melhorar segurança	Limitações e Restrições
89	Aprimorar segurança de redes	Segurança e Dados	Alta precisão	Desenvolvimento de framework	Desafios de Segurança
90	Desenvolver framework de segurança	Sistemas de IoT	Detecção eficaz	Melhorar segurança	Limitações e Restrições
91	Propor metodologia de segurança	Sistemas de IoT	Alta precisão	Melhorar segurança	Limitações e Restrições
92	Aprimorar segurança de redes	Segurança e Dados	Melhoria de desempenho	Desenvolvimento de framework	Desafios de Segurança
93	Desenvolver framework de segurança	Sistemas de IoT	Alta precisão	Desenvolvimento de framework	Limitações e Restrições
94	Propor metodologia de segurança	Segurança e Dados	Alta precisão	Melhorar segurança	Necessidade de Melhoria
95	Explorar eficácia AI	Vulnerabilidade e Ameaças	Alta precisão	Desenvolvimento de framework	Limitações e Restrições
96	Aprimorar segurança de redes	Tráfego de Rede	Alta precisão	Melhorar segurança	Limitações e Restrições
97	Desenvolver framework de segurança	Sistemas de IoT	Melhoria de desempenho	Melhorar segurança	Desafios de Segurança
98	Aprimorar segurança de redes	Restrições de Recursos	Alta precisão	Melhorar segurança	Limitações e Restrições
99	Analisar técnicas de detecção	Tráfego de Rede	Alta precisão	Desenvolvimento de framework	Limitações e Restrições
100	Explorar eficácia AI	Tráfego de Rede	Detecção eficaz	Melhorar segurança	Limitações e Restrições
101	Aprimorar segurança de redes	Tráfego de Rede	Alta precisão	Melhorar segurança	Complexidade e Dificuldade
102	Aprimorar segurança de redes	Segurança e Dados	Detecção eficaz	Melhorar segurança	Limitações e Restrições
103	Aprimorar segurança de redes	Conectividade e Integração	Alta precisão	Melhorar segurança	Limitações e Restrições
104	Aprimorar segurança de redes	Tráfego de Rede	Detecção eficaz	Melhorar segurança	Complexidade e Dificuldade
105	Explorar eficácia AI	Tráfego de Rede	Detecção eficaz	Melhorar segurança	Limitações e Restrições
106	Desenvolver framework de segurança	Segurança e Dados	Alta precisão	Melhorar segurança	Limitações e Restrições
107	Explorar eficácia AI	Segurança e Dados	Alta precisão	Melhorar segurança	Limitações e Restrições
108	Propor metodologia de segurança	Tráfego de Rede	Alta precisão	Desenvolvimento de framework	Desafios de Segurança
109	Investigar abordagens de segurança	Segurança e Dados	Melhoria de desempenho	Abordagem inovadora	Complexidade e Dificuldade
110	Aprimorar segurança de redes	Tráfego de Rede	Eficácia comprovada	Taxonomia abrangente	Ameaças Emergentes
111	Aprimorar segurança de redes	Sistemas de IoT	Alta precisão	Desenvolvimento de framework	Limitações e Restrições
112	Desenvolver framework de segurança	Tráfego de Rede	Melhoria de desempenho	Abordagem inovadora	Complexidade e Dificuldade
113	Revisar técnica de IDS	Segurança e Dados	Melhoria de desempenho	Desenvolvimento de framework	Limitações e Restrições
114	Analisar técnicas de detecção	Tráfego de Rede	Detecção eficaz	Desenvolvimento de framework	Desafios de Segurança
115	Explorar eficácia AI	Tráfego de Rede	Alta precisão	Melhorar segurança	Complexidade e Dificuldade
116	Explorar eficácia AI	Tráfego de Rede	Alta precisão	Melhorar segurança	Limitações e Restrições
117	Desenvolver framework de segurança	Segurança e Dados	Melhoria de desempenho	Desenvolvimento de framework	Complexidade e Dificuldade

Tabela 16 – Termos de Associações dos Artigos

APÊNDICE C – ALGORÍTIMO APIORI

```
frequent_itemsets = apriori(df_encoded, min_support=0.05,
    use_colnames=True)
rules = association_rules(frequent_itemsets, metric="confidence",
    min_threshold=0.09)
rules = rules[rules['antecedents'].apply(lambda x: len(x) >= 1) &
    rules['consequents'].apply(lambda x: len(x) >= 1)]
print("Association Rules:", rules.shape[0])
print(rules[['antecedents', 'consequents', 'antecedent support',
       'consequent support', 'support', 'confidence', 'lift']].head
          (24))
```

Código-fonte 1 – Aplicação do algoritmo Apriori em Python

APÊNDICE D – TRATAMENTO DOS DADOS DOS ARTIGOS ANALISADOS

```
import csv
import matplotlib.pyplot as plt

with open('arquivo.csv', 'r') as f:
    res = csv.reader(f)
    algoritmos = []
    for row in res:
        algoritmos.append(row[colunaX].replace('\n', ' ').replace('
            ', ' ').split(','))

algoritmos = algoritmos[1:]
for i in range(len(algoritmos)):
    for j in range(len(algoritmos[i])):
        if algoritmos[i][j] == '':
            continue
        if algoritmos[i][j][0] == ' ':
            algoritmos[i][j] = algoritmos[i][j][1:]
        if algoritmos[i][j][-1] == ' ':
            algoritmos[i][j] = algoritmos[i][j][:-1]

contagem_algoritmos = []
for row in algoritmos:
    contagem_algoritmos += row

contagem_dict_algoritmos = {}
for algoritmo in contagem_algoritmos:
    if algoritmo in contagem_dict_algoritmos:
        contagem_dict_algoritmos[algoritmo] += 1
    else:
        contagem_dict_algoritmos[algoritmo] = 1

freq_minima = 2
algoritmos_min = {}
for chave_algoritmo in contagem_dict_algoritmos.keys():
    if contagem_dict_algoritmos[chave_algoritmo] >= freq_minima:
        algoritmos_min[chave_algoritmo] = contagem_dict_algoritmos[
            chave_algoritmo]
```

```
36
37 fig, ax = plt.subplots()
38 nomes_algoritmos = list(algoritmos_min.keys())
39 counts = list(algoritmos_min.values())
40 x = range(len(nomes_algoritmos))
41
42 ax.barh(nomes_algoritmos, counts, color='navy')
43 ax.set_yticks(x, nomes_algoritmos)
44 plt.show()
```

Código-fonte 2 – Leitura e contagem de algoritmos em arquivo CSV com visualização em gráfico de barras

APÊNDICE E – ANÁLISE DE CLUSTERIZAÇÃO (K-MEANS)

```python
import pandas as pd
from sklearn.preprocessing import MultiLabelBinarizer
from sklearn.cluster import KMeans
from sklearn.metrics import silhouette_score
import matplotlib.pyplot as plt
import numpy as np

try:
    df = pd.read_csv('articles_term.csv')
except FileNotFoundError:
    print("Erro: Arquivo 'articles_term.csv' nao encontrado.")
    exit()

INTERNAL_SEPARATOR = ','

CATEGORICAL_COLS = [
    'Objetivo',
    'Algoritimos',
    'Caracteristicas\nde IoT\nAnalisadas',
    'Resultado',
    'Contribuicao',
    'Desafios'
]

def apply_multilabel_binarizer(df, column, separator):
    list_of_labels = df[column].fillna('').apply(lambda x: [item.
        strip() for item in x.split(separator) if item.strip()])
    mlb = MultiLabelBinarizer()
    encoded_data = mlb.fit_transform(list_of_labels)
    encoded_df = pd.DataFrame(encoded_data, columns=[f'{column}_{
        label}' for label in mlb.classes_])
    return encoded_df

encoded_dfs = [apply_multilabel_binarizer(df, col, INTERNAL_SEPARATOR
    ) for col in CATEGORICAL_COLS]
X = pd.concat(encoded_dfs, axis=1)

```

```
sse = []
k_range = range(1, 11)

for k in k_range:
    kmeans = KMeans(n_clusters=k, random_state=42, n_init=10)
    kmeans.fit(X)
    sse.append(kmeans.inertia_)

plt.figure(figsize=(10, 6))
plt.plot(k_range, sse, marker='o')
plt.title('Metodo do Cotovelo para Determinacao do K otimo')
plt.xlabel('Numero de Clusters (K)')
plt.ylabel('Soma dos Quadrados dos Erros (SSE)')
plt.grid(True)
plt.savefig('metodo_cotovelo_tcc.png')
plt.close()

K_OPTIMO = 4

kmeans_final = KMeans(n_clusters=K_OPTIMO, random_state=42, n_init
    =10)
df['Cluster'] = kmeans_final.fit_predict(X)

df_clustered = pd.concat([df, X], axis=1)
cluster_analysis = df_clustered.groupby('Cluster')[X.columns].mean()
cluster_analysis = (cluster_analysis * 100).round(1)

for i in range(K_OPTIMO):
    print(f"\nCluster {i}:")
    relevant_features = cluster_analysis.loc[i][cluster_analysis.loc[
        i] > 20].sort_values(ascending=False)
    print(relevant_features)

print("\nContagem de Artigos por Cluster:")
print(df['Cluster'].value_counts().sort_index())

if K_OPTIMO > 1:
    score = silhouette_score(X, df['Cluster'])
    print(f"\nSilhouette Score para K={K_OPTIMO}: {score:.4f}")
```

```
72
73 df.to_csv('artigos_clusterizados_tcc.csv', index=False)
```

Código-fonte 3 – pré-processamento (One-Hot Encoding), a determinação do K ótimo e a aplicação do K-Means

APÊNDICE F – ANÁLISE DE TENDÊNCIAS TEMPORAIS

```python
import pandas as pd
from sklearn.preprocessing import MultiLabelBinarizer
import matplotlib.pyplot as plt
import numpy as np

try:
    df = pd.read_csv('articles_term.csv')
except FileNotFoundError:
    print("Erro: Arquivo 'articles_term.csv' nao encontrado.")
    exit()

INTERNAL_SEPARATOR = ','

CATEGORICAL_COLS = [
    'Algoritimos',
    'Caracteristicas\nde IoT\nAnalisadas',
    'Desafios'
]

def apply_multilabel_binarizer(df, column, separator):
    list_of_labels = df[column].fillna('').apply(lambda x: [item.
        strip() for item in x.split(separator) if item.strip()])
    mlb = MultiLabelBinarizer()
    encoded_data = mlb.fit_transform(list_of_labels)
    encoded_df = pd.DataFrame(encoded_data, columns=[f'{column}_{
        label}' for label in mlb.classes_])
    return encoded_df

encoded_dfs = [apply_multilabel_binarizer(df, col, INTERNAL_SEPARATOR
    ) for col in CATEGORICAL_COLS]
df_encoded = pd.concat([df['Ano'], *encoded_dfs], axis=1)


temporal_trends = df_encoded.drop(columns=['Ano']).groupby(df_encoded
    ['Ano']).sum()

articles_per_year = df_encoded['Ano'].value_counts().sort_index()
```

```
34 temporal_trends_normalized = temporal_trends.div(articles_per_year,
       axis=0) * 100
35
36
37 top_terms = temporal_trends.sum().sort_values(ascending=False).head
       (5).index.tolist()
38
39 plot_data = temporal_trends_normalized[top_terms]
40
41 plt.figure(figsize=(12, 7))
42 plot_data.plot(kind='line', marker='o', ax=plt.gca())
43
44 plt.title('Evolucao Temporal dos Termos Mais Frequentes (em %)')
45 plt.xlabel('Ano')
46 plt.ylabel('Porcentagem de Artigos que Mencionam o Termo (%)')
47 plt.xticks(temporal_trends_normalized.index)
48 plt.grid(True, linestyle='--', alpha=0.7)
49 plt.legend(title='Termo', bbox_to_anchor=(1.05, 1), loc='upper left')
50 plt.tight_layout()
51
52 plt.savefig('tendencias_temporais_tcc.png')
53 plt.close()
```

Código-fonte 4 – pré-processamento, o agrupamento por ano e a geração do gráfico de linhas