Prevenção e Detecção de Intrusões em Redes IoT: Um Mapeamento Sistemático de Soluções na Borda e na Nuvem

Daniel Walmir dos Santos Alves[1], Bruno Dalmazo[2], Andre Riker[3], Geraldo P. Rocha Filho,[4] Roger Immich[1]

[1] Universidade Federal do Rio Grande do Norte (UFRN)

daniel.alves.109@ufrn.edu.br, roger@imd.ufrn.br

[2]Universidade Federal do Rio Grande (FURG)

dalmazo@furg.br

[3]Universidade Federal do Pará (UFPA)

ariker@ufpa.br

[4]Universidade Estadual do Sudoeste da Bahia (UESB)

geraldo.rocha@uesb.edu.br

Abstract. *This paper presents a systematic overview of intrusion detection and prevention systems (IDS/IPS) for Internet of Things (IoT) networks, focusing on edge and cloud environments. The study analyzes 24 selected papers from four major databases, assessing their quality and relevance. The findings highlight various intrusion prevention approaches, including behavior-based, signature-based, and anomaly-based detection methods, with machine learning—particularly federated learning—emerging as a promising solution. However, challenges such as network complexity and device diversity remain significant. This review categorizes and compares existing approaches, providing key parameters and metrics to support replication in future IoT security research. Additionally, it offers guidelines for experimentation and enhances the reproducibility of research findings.*

Resumo. *Este artigo apresenta uma revisão sistemática sobre sistemas de detecção e prevenção de intrusão (IDS/IPS) em redes de Internet das Coisas (IoT), com foco na borda e na nuvem. A análise abrangeu 24 artigos selecionados de quatro bases de dados, avaliados quanto à qualidade e relevância. Os resultados indicam que soluções como detecção baseada em comportamento, assinaturas e anomalias têm sido exploradas para proteger redes IoT, com destaque para o aprendizado de máquina, especialmente o aprendizado federado. No entanto, desafios como a complexidade da rede e a diversidade de dispositivos ainda persistem. O estudo categoriza e compara abordagens, fornecendo parâmetros e métricas para replicação em futuras pesquisas sobre segurança em IoT. Além disso, contribui com diretrizes para experimentação e reprodutibilidade de resultados.*

1. Introdução

A Internet das Coisas (IoT) tem transformado diversos setores, conectando dispositivos e sistemas para otimizar eficiência e qualidade de vida. No entanto, essa expansão também amplia as vulnerabilidades a ameaças cibernéticas [Atzori et al. 2010]. A crescente adoção de dispositivos IoT aumenta a superfície de ataque, expondo redes a ameaças como negação de serviço (DoS), ataques *man-in-the-middle* e injeções de código malicioso [Ge et al. 2019], afetando sistemas críticos como saúde, transporte e infraestrutura pública.

Nesse cenário, os Sistemas de Detecção (IDS) e Prevenção de Intrusão (IPS) são essenciais para mitigar riscos, pois detectam e respondem automaticamente a atividades suspeitas [Rash et al. 2005]. Contudo, em redes IoT, desafios como a diversidade de dispositivos e restrições de hardware dificultam sua implementação. Abordagens tradicionais, baseadas em assinaturas ou detecção de anomalias, apresentam limitações, sendo ineficazes contra ataques *zero-day* ou gerando altos índices de falsos positivos [Yang et al. 2022, Shirazi 2017].

Diante disso, técnicas avançadas como aprendizado de máquina e aprendizado federado surgem como alternativas promissoras [Nguyen and Et al. 2021]. O aprendizado federado, em particular, permite a construção de modelos distribuídos sem comprometer a privacidade dos dados, sendo uma solução viável para IoT. No entanto, desafios persistem, como a escassez de recursos computacionais nos dispositivos e dificuldades na interoperabilidade [Noura et al. 2019]. Estratégias como o processamento em nuvem ajudam a contornar esses problemas, mas introduzem novas vulnerabilidades, como a dependência de conexões seguras [Jimmy 2024].

Este trabalho apresenta um mapeamento sistemático das abordagens mais recentes para a prevenção e detecção de intrusões em redes IoT, buscando catalogar soluções eficazes e viáveis. Além de identificar tendências, o estudo visa contribuir para a evolução da pesquisa, equilibrando inovação tecnológica e aplicabilidade prática, reforçando a segurança e a resiliência na era da IoT.

O texto está organizado da seguinte forma: Na Seção 2, detalhamos a metodologia utilizada no mapeamento. Na Seção 3, discutimos os resultados alcançados. Por fim, a Seção 4 traz as conclusões e sugestões para futuras pesquisas.

2. Metodologia do Mapeamento Sistemático

O objetivo principal é mapear as soluções atuais, identificar lacunas no estado da arte e propor um modelo eficiente de IPS/IDS que aproveite as vantagens da descentralização da borda e a robustez da nuvem, minimizando a latência e preservando a privacidade dos dados

2.1. Questões de Pesquisa

Cinco questões de pesquisa (QP) foram estabelecidas.

- (QP1) Quais são os principais métodos de detecção e prevenção de intrusão e datasets utilizados em redes IoT?
- (QP2) Como os sistemas de detecção e prevenção de intrusão podem ser implementados em redes IoT na extremidade da rede e na nuvem?
- (QP3) Quais são os desafios associados à implementação de sistemas de detecção e prevenção de intrusão em redes IoT?
- (QP4) Como os sistemas de detecção e prevenção de intrusão baseados em aprendizado de máquina podem ser utilizados em redes IoT?
- (QP5) Quais são as métricas de desempenho e eficácia utilizadas para avaliar IPS e IDS em IoT?

2.2. Estratégia de Busca e Seleção

Inicialmente, foram definidos os termos de busca relevantes para a mapeamento, como “prevenção de intrusão”, “redes IoT”, “sistemas de segurança” e “aprendizado de máquina”. As pesquisas foram conduzidas nas principais bases de dados, incluindo IEEE Xplore, ACM Digital Library, ScienceDirect e Scopus. A string de busca utilizada foi: (“Intrusion Prevention Systems” OR “Intrusion Detection Systems”) AND “Internet of Things” AND “Federated Learning” AND (“Edge Computing” OR “Cloud Computing”) AND (“Security” OR ”Privacy”).

2.3. Critérios de Inclusão e Exclusão

Na análise dos artigos, foram aplicados critérios de inclusão e exclusão pré-definidos para garantir a seleção de estudos relevantes e de qualidade. Os critérios de inclusão e exclusão foram: CI1 - Artigos que abordavam sistemas de detecção e prevenção de intrusão em redes IoT na extremidade da rede e na nuvem; CI2 - Artigos que descreviam diferentes métodos de detecção e prevenção de intrusão em redes IoT; CI3 - Artigos que apresentavam desafios e soluções para a implementação de sistemas de detecção e prevenção de intrusão em redes IoT; CI4 - Artigos que discutiam a eficácia de diferentes tipos de sistemas de detecção e prevenção de intrusão em redes IoT; CI5 - Artigos publicados em inglês nos últimos 5 anos; CE1 - Artigos que não estavam relacionados a sistemas de prevenção de intrusão em redes IoT ou detecção; CE2 - Artigos que não estavam em inglês; CE3 - Artigos que não estavam disponíveis na íntegra; CE4 - Artigos duplicados.

2.4. Seleção e Classificação

As buscas foram realizadas em quatro bases de dados reconhecidas na área de Tecnologia da Informação: IEEE, ACM, Science Direct e Scopus, retornando um total de 556 artigos. A Figura 1 apresenta a consolidação dos resultados. Os estudos duplicados foram eliminados, reduzindo o número para 268 artigos. Em seguida, foi realizada uma análise preliminar dos títulos e resumos, aplicando critérios de inclusão e exclusão previamente definidos, o que resultou na seleção de 69 artigos relevantes. Esses estudos foram, então, submetidos a uma leitura detalhada das seções de introdução e conclusão, resultando na identificação de 46 artigos elegíveis para uma análise mais aprofundada e 24 artigos primários foram selecionados para compor a base do estudo.

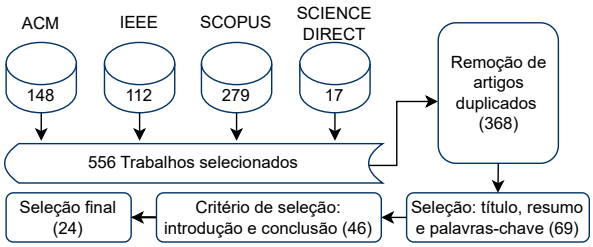

Figura 1. Protocolo de seleção de artigos

3. Resultados e Discussão

3.1. (QP1)Quais são os principais métodos de detecção e prevenção de intrusão e datasets utilizados em redes IoT?

Muitos trabalhos adotam os dataset tradicionais, porém há uma tendência clara de migração para datasets mais especializados em IoT, como BoT-IoT, TON-IoT, MQTTSet Edge-IIoTset, que refletem cenários mais próximos da realidade dos dispositivos conectados. A Figura 2 apresenta a distribuição dos datasets mais utilizados na literatura.

O tradicional dataset KDD Cup 99 aparece como o mais citado nos artigos, e sua versão aprimorada, NSL-KDD. Embora sejam considerados datasets mais antigos e menos representativos dos ataques modernos em redes IoT. [Abou El Houda et al. 2023a] e [Zhang et al. 2022] mencionam esses datasets em experimentos para testar abordagens clássicas de detecção de intrusão.

Por outro lado, o dataset BoT-IoT aparece como sendo amplamente utilizado para avaliar ataques de botnets e tráfego malicioso em redes IoT. Em seguida, o TON-IoT e o MQTTset também se destacam, especialmente por sua aplicabilidade na análise de ataques específicos em redes industriais e IoT baseadas no protocolo MQTT

[Ferrag et al. 2021, Friha et al. 2023]. A falta de um padrão consolidado para avaliar modelos de detecção de intrusão em IoT ainda é um desafio, o que sugere a necessidade de pesquisas futuras para o desenvolvimento de novos conjuntos de dados mais representativos.

Adicionalmente, os principais métodos de detecção e prevenção de intrusão em redes IoT são focados em três grandes abordagens: detecção baseada em anomalias, detecção baseada em comportamentos e aprendizado de máquina, com destaque para aprendizado federado. A Figura 3 mostra os principais métodos encontrados.

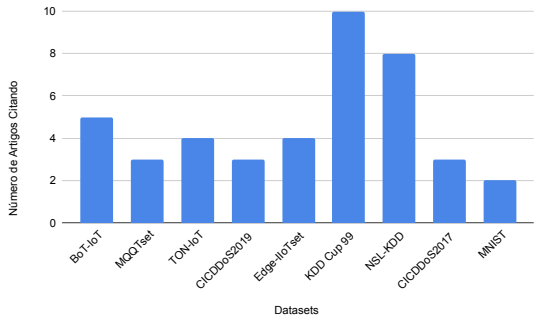

Figura 2. Datasets utilizados

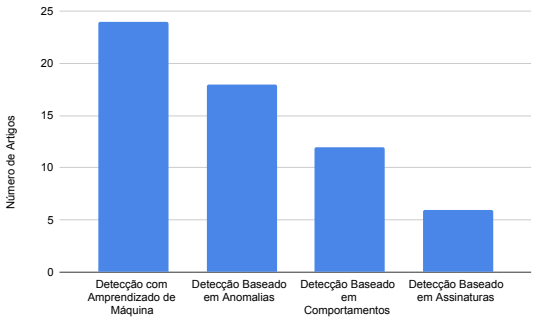

Figura 3. Métodos de detecção

A detecção baseada em anomalias se destaca como um dos métodos mais aplicados em redes IoT, devido à capacidade de identificar ataques desconhecidos. O estudo de [Xiang et al. 2024] mostrou que a detecção de anomalias pode identificar comportamentos não usuais em redes IoT, sem a necessidade de conhecer padrões de ataques pré-existentes. Esse método é particularmente útil para detectar novos tipos de ataques, como DDoS ou invasões internas, que não possuem uma assinatura conhecida. O artigo de [Roy et al. 2023] também destaca que a detecção de anomalias permite identificar desvios significativos no tráfego de rede, com alta taxa de detecção.

Outro método eficaz é a detecção baseada em comportamentos, que analisa as interações entre os dispositivos na rede. O estudo de [Roy et al. 2023] além da detecção de anomalias, propõe o uso de aprendizado de máquina para monitorar o comportamento dos dispositivos IoT e identificar desvios desse comportamento esperado, sinalizando atividades suspeitas. Por exemplo, um dispositivo IoT que começa a comunicar dados de maneira anômala ou solicita recursos de rede de forma incomum pode ser identificado como comprometido.

Os métodos baseados em aprendizado de máquina são amplamente utilizados para melhorar a precisão e a adaptabilidade dos sistemas de detecção de intrusão. Modelos como Redes Neurais Convolucionais 1D (1D-CNN) e Redes Recorrentes (LSTM, GRU) são aplicados para a análise de tráfego de rede e a detecção de padrões maliciosos [Hernandez-Ramos et al. 2023]. O estudo de [Singh and Et Al. 2022] destaca que a aplicação de aprendizado federado nesses modelos permite treinamento local nos dispositivos IoT, sem a necessidade de compartilhar dados sensíveis. [Fan et al. 2020] reforçam que a aprendizagem federada pode ser utilizada para melhorar a segurança das redes IoT enquanto preserva a privacidade dos dados. No estudo de [Han et al. 2024], a aplicação de 1D-CNN demonstrou ser eficaz para a detecção de DDoS e ataques Man in the Middle em redes IoT. Os modelos de aprendizado profundo permitem que o sistema aprenda com grandes volumes de dados e identifique novos tipos de ataques que poderiam passar despercebidos por sistemas baseados em assinaturas.

O aprendizado federado foi identificado em vários artigos como uma solução eficaz para superar os desafios de privacidade e sobrecarregar a rede. Como destacado por

[Nguyen et al. 2023], o aprendizado federado permite que modelos de aprendizado de máquina sejam treinados localmente, preservando os dados sensíveis dos dispositivos IoT, e as atualizações dos modelos são enviadas para servidores centrais, onde são agregadas para formar um modelo global. O aprendizado federado tem sido especialmente eficaz em redes IoT heterogêneas, onde dispositivos com capacidades computacionais limitadas podem treinar modelos de maneira colaborativa, como demonstrado no estudo de [Meng et al. 2024].

Embora os métodos de aprendizado federado e aprendizado de máquina tenham demonstrado grande eficácia na detecção de intrusões em redes IoT, alguns desafios persistem, como a latência nas atualizações de modelos e a eficiência computacional em dispositivos IoT com recursos limitados. No entanto, novas abordagens, como o uso de diferenciação privada e aprendizado federado descentralizado, têm sido propostas para melhorar a segurança e a eficácia dos sistemas de detecção em IoT.

3.2. (QP2)Como os IPS/IDS podem ser implementados em redes IoT na extremidade da rede e na nuvem?

A implementação de sistemas de detecção e prevenção de intrusão em redes IoT pode ocorrer em duas camadas, a borda e a nuvem. Ambas as abordagens têm vantagens distintas, dependendo das características da rede e dos requisitos de latência, privacidade e escalabilidade.

A computação de borda é uma das soluções mais vantajosas para redes IoT, principalmente em cenários que exigem detecção em tempo real e baixa latência [Bukhari et al. 2024]. Em redes IoT com dispositivos heterogêneos, a detecção local e o aprendizado federado ajudam a reduzir o tráfego de dados, pois somente os modelos atualizados são compartilhados, em vez de dados brutos.

A implementação de aprendizado federado na borda pode reduzir significativamente a sobrecarga de comunicação e a latência, permitindo que dispositivos com recursos limitados possam contribuir para a segurança da rede sem comprometer sua privacidade [Salim and Et al. 2024]. O aprendizado federado também permite que os dispositivos aprendam de forma colaborativa, melhorando a eficácia da detecção de intrusões sem expor dados pessoais.

Na nuvem, a centralização do treinamento de modelos de detecção de intrusão oferece uma análise mais profunda e coordenação global das intrusões em uma rede IoT distribuída [Zhang et al. 2022]. O modelo centralizado na nuvem coleta atualizações de modelos de diversos dispositivos na borda e realiza uma agregação para formar um modelo global mais preciso [Al-Garadi et al. 2020]. Essa abordagem permite monitoramento e controle centralizados, o que facilita a detecção de ataques distribuídos e a análise de dados em larga escala. No entanto, a latência e a sobrecarga de comunicação podem ser desafios, especialmente em redes com grande número de dispositivos IoT.

A nuvem pode ser ideal para realizar uma análise de intrusões em larga escala, onde a agregação dos modelos locais permite a detecção de ataques mais complexos, como ataques de negação de serviço (DDoS) [Zhang et al. 2022]. A nuvem também facilita a atualização contínua de modelos de aprendizado de máquina, adaptando-se rapidamente a novas ameaças. No entanto, [Abba Ari et al. 2024] observam que, para evitar gargalos na rede, o sistema precisa ser projetado para minimizar a latência e reduzir a sobrecarga de dados.

O aprendizado federado permite que os dispositivos treinem localmente, mantendo os dados privados e agreguem os modelos de forma colaborativa [Bukhari et al. 2024]. Essa abordagem é importante para evitar o envio de grandes

volumes de dados para servidores centrais e para garantir que as informações sensíveis dos dispositivos IoT não sejam expostas.

3.3. (QP3)Quais são os desafios envolvidos na aplicação de aprendizado federado em redes IoT?

Um dos maiores desafios na implementação de sistemas IDS/IPS em redes IoT é a heterogeneidade dos dispositivos. Estas redes são compostas por dispositivos com diferentes capacidades de processamento, armazenamento e comunicação, o que dificulta a criação de modelos de detecção de intrusão universais. De acordo com [Fan et al. 2020], dispositivos com capacidade computacional limitada podem não ser capazes de rodar modelos complexos de aprendizado de máquina sem que haja um impacto significativo na latência e desempenho geral do sistema. Além disso, os dados coletados pelos dispositivos podem ter características diferentes, como dados estruturados e não estruturados, exigindo uma abordagem mais personalizada para cada tipo de dispositivo.

A escalabilidade é outro grande desafio. Em redes IoT de larga escala, onde milhares de dispositivos podem gerar volumes massivos de dados em tempo real, modelos de detecção centralizados podem ser ineficazes. A implementação de um modelo de detecção de intrusão eficiente em uma rede IoT escalável requer a capacidade de processar dados localmente, sem sobrecarregar a rede com a transferência contínua de dados [Alotaibi and Barnawi 2023]. Nesse contexto, o uso de aprendizado federado surge como uma solução promissora [Mahmoodi and Et Al. 2023].

A privacidade dos dados é uma preocupação fundamental nas redes IoT, especialmente quando se trata de dados sensíveis, como informações de saúde ou dados financeiros. Em redes IoT, os dispositivos podem geram dados sem permissão para serem compartilhados devido a regulamentações de privacidade, como a LGPD ou o GDPR [Friha et al. 2023]. O uso de privacidade diferencial em sistemas de aprendizado federado pode proteger ainda mais os dados dos dispositivos, tornando a detecção de intrusão mais privada e segura [Friha et al. 2023].

A complexidade computacional é outro desafio significativo. Embora modelos como redes neurais convolucionais 1D (1D-CNN) sejam eficazes, eles exigem recursos computacionais significativos, o que pode afetar o desempenho dos dispositivos IoT [Hernandez-Ramos et al. 2023]. Uma solução proposta para mitigar esses problemas é também o uso de aprendizado federado.

Um dos problemas críticos é o risco de envenenamento de dados durante o processo de atualização dos modelos [Chennoufi et al. 2024]. Dispositivos comprometidos podem enviar modelos maliciosos para o servidor central, impactando a eficácia do sistema de detecção de intrusão. A segurança dos dados durante o processo de agregação dos modelos e a defesa contra ataques adversariais se tornam, assim, preocupações importantes que precisam ser endereçadas para garantir a eficácia do aprendizado federado.

3.4. (QP4)Como o aprendizado federado está sendo aplicado na segurança de redes IoT?

Ao aplicar aprendizado federado, os modelos de segurança podem ser treinados de forma colaborativa sem que os dados saiam dos dispositivos locais [Yang et al. 2022]. As atualizações de modelos resultantes de cada dispositivo são agregadas em um servidor central, que aprimora a capacidade de detecção de intrusões sem comprometer a privacidade dos dados. Uma das principais áreas onde o aprendizado federado está sendo aplicado é na detecção de ataques distribuídos, como ataques DDoS, que são comuns em redes IoT. Devido ao grande número de dispositivos IoT em redes distribuídas, a detecção

de DDoS pode ser mais eficaz quando realizada de forma colaborativa entre dispositivos [Shen et al. 2024].

Embora o aprendizado federado ofereça muitas vantagens para a segurança em redes IoT, existem desafios a serem superados. Vale destacar a heterogeneidade dos dispositivos e a complexidade computacional associada ao treinamento e agregação dos modelos [Shen et al. 2024]. Abordagens como o FedProx (uma variante do FedAvg) podem ser usadas para resolver o problema da heterogeneidade dos dispositivos, permitindo uma maior eficácia no treinamento de modelos em redes IoT [Chennoufi et al. 2024].

3.5. (QP5)Quais são as métricas de desempenho e eficácia utilizadas para avaliar IPS e IDS em IoT?

A avaliação IPS e IDS em redes IoT envolve o uso de métricas específicas que medem o desempenho, a eficácia e a capacidade desses sistemas em identificar e mitigar ameaças em ambientes altamente dinâmicos e distribuídos. Portanto, as métricas de avaliação dos sistemas de segurança em IoT precisam abranger uma gama de aspectos técnicos, como precisão de detecção, latência, eficiência computacional e taxa de falsos positivos.

A precisão, ou *"accuracy"*, é uma das métricas mais comuns, sendo utilizada para medir a taxa de detecção correta de ameaças. Outra métrica relevante é a taxa de falsos positivos, que avalia a quantidade de alarmes incorretos gerados pelo sistema, sendo crucial para evitar sobrecarga e bloqueios indevidos. A taxa de detecção, ou *"True Positive Rate"(TPR)*, mede a capacidade dos sistemas de identificar ameaças corretamente, enquanto o F1-score combina precisão e *recall*, oferecendo uma visão mais equilibrada do desempenho geral do sistema. O *recall* é a razão entre o número de verdadeiros positivos (TP) e a soma dos verdadeiros positivos (TP) e falsos negativos (FN). Em outras palavras, ele indica a proporção de ataques que foram identificados corretamente pelo sistema em relação ao total de ataques que ocorreram, incluindo os que não foram detectados. As métricas mitigadas neste trabalho se encontram representadas na figura 4. Abaixo, discutimos as principais métricas utilizadas para avaliar IPS e IDS em IoT.

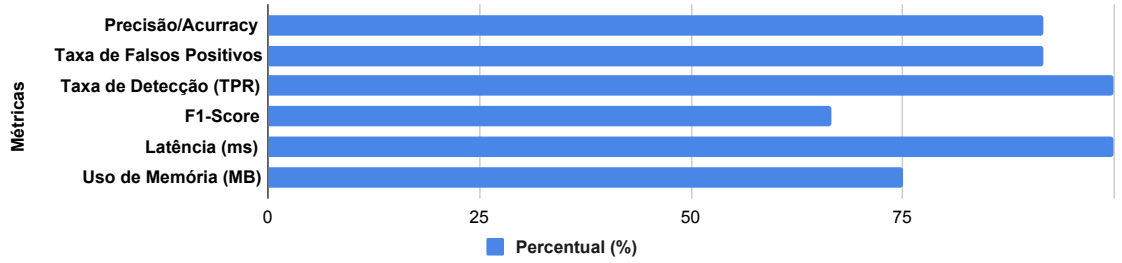

Figura 4. Métricas adotadas

A taxa de falsos positivos (FPR) é crítica, pois um aumento de alertas falsos pode sobrecarregar os sistemas de segurança e reduzir a eficácia geral da solução. A FPR mede a taxa de instâncias legítimas incorretamente classificadas como intrusões. Para um sistema ser eficaz, a FPR deve ser minimizada, garantindo que os alertas de intrusão sejam válidos [Roy et al. 2023]. Por outro lado, a taxa de falsos negativos (FNR) mede a incapacidade do sistema de detectar intrusões reais. Uma alta taxa de falsos negativos pode permitir que um ataque real passe despercebido. Quanto mais baixa for a FNR, maior será a capacidade do sistema de detectar ameaças reais [Roy et al. 2023]

A taxa de detecção (DR) mede a capacidade do sistema de identificar intrusões reais. Em redes IoT, onde ataques podem ocorrer de forma distribuída e complexa, garantir uma alta taxa de detecção é essencial para mitigar riscos. Essa métrica é especialmente relevante em cenários com ataques distribuídos como DDoS e botnets, onde múltiplos dispositivos podem ser comprometidos simultaneamente [Hernandez-Ramos et al. 2023].

O F1-Score é uma métrica combinada que leva em consideração tanto a precisão quanto a taxa de detecção. Em redes IoT, onde há um desequilíbrio entre tráfego legítimo e ataques, o F1-Score é útil para fornecer uma avaliação mais equilibrada, já que ele pondera as duas métricas. Um F1-Score elevado indica que o sistema está equilibrando bem a precisão e a detecção de intrusões [Zhang et al. 2022].

A eficiência computacional é uma métrica que avalia a capacidade de um sistema de IPS/IDS de operar com baixo custo computacional em redes IoT com dispositivos limitados. Finalmente, a robustez de um sistema IPS/IDS se refere à sua capacidade de continuar funcionando efetivamente frente a ataques adversariais, como envenenamento de dados, enquanto a escalabilidade é a capacidade de expandir o sistema para lidar com um número crescente de dispositivos e dados. Em redes IoT dinâmicas, onde dispositivos podem ser frequentemente adicionados ou removidos, a escalabilidade é essencial para garantir que a segurança do sistema seja eficaz ao longo do tempo [Abou El Houda et al. 2023b].

3.6. Discussão

Diante do que já foi discutido nas questões de pesquisa, verificamos que a implementação de sistemas de detecção e prevenção de intrusão em redes IoT, embora desafiadora, apresenta potencial para inovação. A análise dos artigos indica que o aprendizado federado tem se mostrado uma solução promissora, especialmente nos últimos anos, com um aumento significativo no número de publicações sobre o tema (Figura 5). Isso reflete uma tendência crescente em resolver os problemas típicos dessas redes, como heterogeneidade, escalabilidade e privacidade de dados.

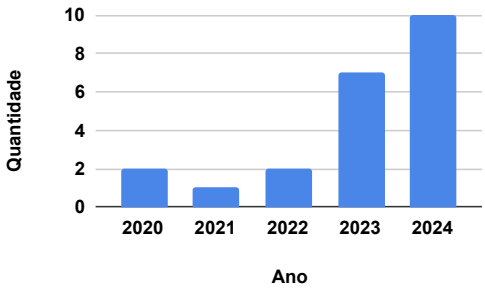

Figura 5. Distribuição por ano

Um dos maiores desafios das redes IoT é a diversidade de dispositivos. Apesar de muitos estudos sugerirem soluções, como o aprendizado federado para reduzir a sobrecarga de comunicação, ainda há um longo caminho pela frente quando se trata de adaptar modelos de segurança a dispositivos com capacidades computacionais extremamente limitadas. Enquanto o aprendizado federado funciona bem para dispositivos de maior capacidade, sua aplicação em dispositivos de baixo desempenho segue sendo um problema. Isso sugere que ainda precisamos desenvolver abordagens mais eficientes e específicas, específicas para esses dispositivos.

A privacidade dos dados um ponto amplamente discutido nos trabalhos, especialmente no aprendizado federado, ainda enfrenta desafios significativos, como a proteção contra ataques manipuláveis, como envenenamento de dados e alteração de imagens, que continuam sendo uma ameaça constante. Outro desafio é a escalabilidade das soluções de segurança, já que, com o crescimento da IoT, as soluções atuais ainda não conseguem mitigar eficazmente falhas e falsas negativas em redes grandes e dinâmicas. Além disso, a latência e a eficiência computacional seguem sendo obstáculos, pois rodar modelos complexos em dispositivos com recursos limitados é inviável, e é essencial otimizar esses modelos para funcionarem em tempo real, sem sobrecarregar a rede.

Por fim, a integração entre diferentes camadas de segurança ainda precisa evoluir bastante. Embora os modelos atuais se concentrem na detecção de intrusões em tempo real ou no aprendizado federado, a eficiência entre a segurança na borda (edge) e na nuvem ainda não está bem resolvida. Novos modelos e abordagens inovadoras podem ser exploradas para cobrir essas lacunas, especialmente em segurança contra ataques adversários, eficiência computacional, escalabilidade e integração entre as camadas de segurança.

4. Conclusão

A pesquisa indicou que os sistemas de prevenção e detecção de intrusões são cruciais para a segurança das redes IoT, utilizados tanto na borda quanto na nuvem para manter a integridade e a privacidade dos dados. As abordagens baseadas em máquina de aprendizagem e aprendizagem federada provaram - se frutíferas para enfrentar novas ameaças e desafios como a heterogeneidade dos dispositivos e a escassez de recursos computacionais. No entanto, a implementação prática de tais sistemas continua a ser um desafio, incluindo a taxa muito elevada de falsos positivos com modelos baseados em modelos anómalos e desafios computacionais induzidos por modelos baseados em aprendizagem profunda em dispositivos IoT restritos. Além disso, a computação em borda e a nuvem se revelaram complementares no detectar e reagir aos ataques, com a borda levando a latência e a nuvem facilitando análises mais profundas e centralizadas. A adoção de arquiteturas híbridas, combinando segurança baseada em assinaturas, detecção de anomalias e inteligência artificial distribuída, pode ser um caminho promissor para aprimorar a segurança de redes IoT.

Referências

Abba Ari, A. A., Ngangmo, O. K., Titouna, C., Thiare, O., Mohamadou, A., and Gueroui, A. M. (2024). Enabling privacy and security in cloud of things: Architecture, applications, security & privacy challenges. *Applied Computing and Informatics*.

Abou El Houda, Z., Brik, B., Ksentini, A., and Khoukhi, L. (2023a). A mec-based architecture to secure iot applications using federated deep learning. *IEEE Internet of Things Magazine*, 6(1):60–63.

Abou El Houda, Z., Moudoud, H., Brik, B., and Khoukhi, L. (2023b). Securing federated learning through blockchain and explainable ai for robust intrusion detection in iot networks. In *IEEE Conference on Computer Communications Workshops (INFOCOM)*.

Al-Garadi, M. A., Mohamed, A., Al-Ali, A. K., Du, X., Ali, I., and Guizani, M. (2020). A survey of machine and deep learning methods for internet of things (iot) security. *IEEE communications surveys & tutorials*, 22(3):1646–1685.

Alotaibi, A. and Barnawi, A. (2023). 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*, 35(6):101575.

Atzori, L., Iera, A., and Morabito, G. (2010). The internet of things: A survey. *Computer Networks*, 54(15):2787–2805.

Bukhari, S. M. S., Zafar, M. H., Abou Houran, M., Qadir, Z., Moosavi, S. K. R., and Sanfilippo, F. (2024). Enhancing cybersecurity in edge iiot networks: An asynchronous federated learning approach with a deep hybrid detection model. *Internet of Things*.

Chennoufi, S., Blanc, G., Jmila, H., and Kiennert, C. (2024). Sok: federated learning based network intrusion detection in 5g: context, state of the art and challenges. In *19th International Conference on Availability, Reliability and Security*.

Fan, Y., Li, Y., Zhan, M., Cui, H., and Zhang, Y. (2020). Iotdefender: A federated transfer learning intrusion detection framework for 5g iot. In *2020 IEEE 14th international conference on big data science and engineering (BigDataSE)*, pages 88–95. IEEE.

Ferrag, M. A., Friha, O., Maglaras, L., Janicke, H., and Shu, L. (2021). Federated deep learning for cyber security in the internet of things: Concepts, applications, and experimental analysis. *IEEe Access*.

Friha, O., Ferrag, M. A., Benbouzid, M., Berghout, T., Kantarci, B., and Choo, K.-K. R. (2023). 2df-ids: Decentralized and differentially private federated learning-based intrusion detection system for industrial iot. *Computers & Security*, 127:103097.

Ge, M. et al. (2019). Deep learning-based intrusion detection for iot networks. In *IEEE 24th Pacific Rim International Symposium on Dependable Computing (PRDC)*. IEEE.

Han, C., Li, T., Chen, Q., Wu, Y., and Qin, J. (2024). Distributed and collaborative lightweight edge federated learning for iot zombie devices detection. *ACM Transactions on Sensor Networks*.

Hernandez-Ramos, J. L., Karopoulos, G., Chatzoglou, E., Kouliaridis, V., Marmol, E., Gonzalez-Vidal, A., and Kambourakis, G. (2023). Intrusion detection based on federated learning: a systematic review. *arXiv preprint arXiv:2308.09522*.

Jimmy, F. (2024). Cyber security vulnerabilities and remediation through cloud security tools. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*.

Mahmoodi, A. B. Z. and Et Al. (2023). Autonomous federated learning for distributed intrusion detection systems in public networks. *IEEE Access*.

Meng, R., Shah, A. A., Jamshed, M. A., and Pezaros, D. (2024). Federated learning-based intrusion detection framework for internet of things and edge computing backed critical infrastructure. In *IEEE International Conference on Communications Workshops*.

Nguyen, D. C. and Et al. (2021). Federated learning for internet of things: A comprehensive survey. *IEEE Communications Surveys & Tutorials*.

Nguyen, T.-A., He, J., Le, L. T., Bao, W., and Tran, N. H. (2023). Federated pca on grassmann manifold for anomaly detection in iot networks. In *IEEE INFOCOM*.

Noura, M., Atiquzzaman, M., and Gaedke, M. (2019). Interoperability in internet of things: Taxonomies and open challenges. *Mobile networks and applications*.

Rash, M., Orebaugh, A., and Clark, G. (2005). *Intrusion prevention and active response: Deploying network and host IPS*. Elsevier.

Roy, S., Li, J., and Bai, Y. (2023). Federated learning-based intrusion detection system for iot environments with locally adapted model. In *IEEE 10th International Conference on Cyber Security and Cloud Computing (CSCloud)*. IEEE.

Salim, M. M. and Et al. (2024). Fl-ctif: A federated learning based cti framework based on information fusion for secure iiot. *Information Fusion*.

Shen, J., Yang, W., Chu, Z., Fan, J., Niyato, D., and Lam, K.-Y. (2024). Effective intrusion detection in heterogeneous internet-of-things networks via ensemble knowledge distillation-based federated learning. In *IEEE Inter. Conference on Communications*.

Shirazi, S. N. (2017). *Anomaly Detection for Resilience in Cloud Computing Infrastructures*. Lancaster University (United Kingdom).

Singh, P. and Et Al. (2022). Dew-cloud-based hierarchical federated learning for intrusion detection in iomt. *IEEE journal of biomedical and health informatics*.

Xiang, H., Zhang, X., Xu, X., Beheshti, A., Qi, L., Hong, Y., and Dou, W. (2024). Federated learning-based anomaly detection with isolation forest in the iot-edge continuum. *ACM Transactions on Multimedia Computing, Communications and Applications*.

Yang, Z., Chen, M., Wong, K.-K., Poor, H. V., and Cui, S. (2022). Federated learning for 6g: Applications, challenges, and opportunities. *Engineering*, 8:33–41.

Zhang, X., Wang, Y., Cai, Y., He, Y., Chen, X., and Jin, S. (2022). Intrusion detection based on data privacy in cloud-edge collaborative computing using federated learning. In *Inter. Conference on Network and Information Systems for Computers (ICNISC)*.