Detecção de Ataques DDoS em redes IoT usando Redes Neurais e Seleção de Características

Ariel L. C. Portela[1], **Wanderson L. Costa**[1], **Rafael L. Gomes**[1]

[1]Universidade Estadual do Ceará (UECE), Fortaleza, Ceará, Brasil.

ariel.portela@aluno.uece.br, wanderson.leonardo@ifpi.edu.br,

rafa.lopes@uece.br

Abstract. *The deployment of Internet of Things (IoT) infrastructures suffers with the occurrence of Distributed Denial of Service (DDoS) attacks. In this way, it is necessary to apply solutions to detect DDoS attacks in IoT networks, dealing with issues like scalability, adaptability and heterogeinety. Within this context, this paper presents an Fog-Cloud System for detection of DDoS in IoT networks, based on Neural Networks (NNs) and Features Selection techniques, allowing the identification of the most suitable composition of features to train the model, as well as the necessary scalability. The experiments performed, using real network traffic, suggest that the proposed system reaches 99% accuracy while reducing the volume of data exchanged and the detection time.*

Resumo. *A implantação de infraestruturas de rede baseadas na Internet das Coisas (IoT) sofre com a ocorrência de Ataques de Negação de Serviço Distribuídos (DDoS). Dessa forma, é necessário aplicar soluções que possam detectar DDoS em redes IoT, lidando com questões como escalabilidade, adaptabilidade e heterogeneidade. Dentro deste contexto, este trabalho apresenta um Sistema Cloud-Fog para Detecção de ataques DDoS em Redes IoT baseado em Redes Neurais (RN) e Técnicas de Seleção de Características, possibilitando a identificação da melhor composição de características para o treinamento do modelo, bem como a escalabilidade necessária. Os experimentos realizados, usando tráfego de rede real, sugerem que o sistema proposto atinge* 99% *de acurácia, enquanto reduz o volume de dados trocados e o tempo de detecção.*

1. Introdução

Em um futuro não muito distante, todos os nossos objetos do dia a dia estarão conectados à Internet e equipados com capacidades de sensoriamento e poder de processamento suficientes para explorar todos os benefícios potenciais da chamada Internet das Coisas (*Internet of Things* - IoT). A IoT é uma rede de objetos físicos, que inclui desde utensílios domésticos como lâmpadas, veículos, etiquetas de endereçamento, dispositivos médicos, sensores, câmeras de vigilância e outros objetos conectados com a Internet.

As redes IoT em sua maioria são compostas por dispositivos IoT e dispositivos de usuários. Esses ecossistemas apresentam duas características cruciais: enorme quantidade de dispositivos e heterogeneidade. Como consequência, esses ambientes tendem a gerar mais fluxos de rede do que as redes tradicionais, devido à enorme escala de dispositivos IoT conectados, bem como aos vários tipos de aplicativos executados nesses dispositivos.

Ademais, nos últimos anos, diversos Ataques de Negação de Serviço Distribuído (*Distributed Denial of Service* - DDoS), que visam tornar o acesso a um ou mais alvos indisponíveis ao esgotar seus recursos de rede por meio de múltiplas solicitações ilegítimas, que foram realizados na Internet, ocorreram por meio da infecção de dispositivos IoT [Brun et al. 2018]. Este fato impulsiona a necessidade de estudos e soluções para dar suporte às redes IoT e que implementem sistemas de detecção de ameaças e proteção para as aplicações executadas sobre essas redes.

Uma abordagem promissora para suprir essa demanda de detecção de DDoS em redes IoT é a aplicação de modelos de Inteligência Artificial (IA), os quais utilizam os dados de monitoramento da rede como entrada, para compreender o comportamento dos dispositivos e detectar os possíveis ataques.

Contudo, a necessidade de monitoramento dessas redes traz dois desafios: (I) Identificar quais desses dados da rede realmente agregam informação relevante, visto que a inclusão de ruídos no modelo de IA pode gerar perda de capacidade de detecção de ataques DDoS; e, (II) Lidar com o processamento de um grande volume de dados, devido ao monitoramento do número massivo de dispositivos e conexões de rede. Assim, as soluções de detecção de DDoS devem considerar estes aspectos de escalabilidade, adaptabilidade e heterogeneidade em redes IoT, a fim de terem um desempenho adequado e viável para a implantação no mundo real [Pisani et al. 2020].

Dentro deste contexto, este artigo apresenta um Sistema Inteligente para detecção de DDoS em redes IoT usando Redes Neurais e técnicas de Seleção de Características dentro de uma arquitetura que integra Computação em Névoa e em Nuvem. O uso de Redes Neurais como base do sistema proposto justifica-se por sua capacidade de aprender modelos não lineares e treinar o modelo em tempo real (aprendizado on-line) usando *partial-fit*. Assim, o sistema proposto aplica os seguintes passos:

1. Monitoramento da rede para coleta de dados sobre os fluxos de rede IoT;
2. Extração e seleção de características para identificar os principais atributos dos fluxos de rede IoT para a detecção de DDoS;
3. Treinamento da Rede Neural para detecção de DDoS usando as características mais adequadas identificadas;
4. Integração de computação em Névoa e em Nuvem que permite a divisão de tarefas nesses dois ambientes de computação, minimizando o tempo de resposta, volume de dados a serem processados e aumentando a acurácia de detecção.

Os experimentos realizados, utilizando um conjunto de dados de tráfego de rede real IoT com ataques DDoS, indicam que o sistema proposto atinge cerca de 99% de acurácia quando as características mais adequadas são utilizadas, enquanto reduz o volume de dados a serem processados. Similarmente, avalia-se que a integração entre Névoa e Nuvem minimiza o tempo de treinamento e detecção da rede neural desenvolvida.

Portanto, pode-se elencar as seguintes contribuições neste artigo: (I) Estudo sobre o impacto da seleção de características em relação a acurácia da detecção de DDoS usando Redes Neurais; (II) Análise comparativa da redução do volume de tráfego de rede em uma integração entre Névoa e Nuvem; (III) Um sistema capaz de detectar ataques DDoS em redes IoT com alta acurácia; e, (IV) Experimentos usando um conjunto de dados de tráfego de rede real com ataques DDoS.

2. Trabalhos Relacionados

Sharafaldin et al. [Sharafaldin et al. 2019] apresentam um estudo sobre as características do tráfego de redes mais importantes para detecção de diferentes tipos de ataques DDoS em redes tradicionais, ou seja, redes TCP/IP. Nos experimentos realizados foram projetadas e implantadas duas redes com computadores tradicionais, ou seja, o comportamento extraído das amostras do conjunto de dados se torna diferente em comparação com o de redes projetadas com dispositivos IoT. O comportamento de redes IoT se comunica com um pequeno conjunto finito de pontos de extremidade e são propensos a ter padrões de tráfego de rede repetitivos (pacotes pequenos em intervalos de tempo fixos para fins de registro, por exemplo).

Yamauchi et al. [Yamauchi et al. 2019] descrevem um modelo para detectar operações anômalas de dispositivos IoT em casas inteligentes (*Smart Homes* - SHs) com base no comportamento do usuário. O modelo aprende a sequência de atividades realizadas por hora do dia e, então, compara a sequência atual com as sequências aprendidas para a condição correspondente à condição atual. Caso apresente alguma alteração prédefinida, o método classifica a operação como uma anomalia de dispositivo IoT. Portanto, este modelo proposto pelos autores limita-se ao compreendimento de ambientes de SHs.

Doshi et al. [Doshi et al. 2018] realizaram a detecção de ataques DDoS em andamento por meio do comportamento do fluxo de IoT em casas inteligentes. A abordagem implanta *middleboxes*, agindo como *proxy* na rede para observar, armazenar, processar e controlar o tráfego de rede que vai para a Internet. Essa estratégia monitora as características do fluxo, como tempo de chegada entre pacotes, pontos de extremidade e outros. As informações coletadas servem como entrada para uma técnica de ML para criar um modelo que identifique um possível ataque. Assim, a abordagem de seleção aplicada é muito limitada quando comparada com a análise realizada para desenvolver o mecanismo proposto nesta pesquisa.

Haddadpajouh et al. [HaddadPajouh et al. 2018] apresentaram um modelo do aprendizado profundo de Rede Neural Recorrente (RNN) para detecção de Malwares em dispositivos IoT. Os autores usam RNN para analisar os códigos de operação de execução de aplicativos de IoT baseados em ARM (OpCodes), criando um vetor de recurso com base nos OpCodes para cada amostra. A partir disso, utilizam-se esses dados vetoriais para treinamento e ajuste de rede neural profunda para parâmetros ótimos. No entanto, o modelo treinado depende da análise dos OpCodes, limitando sua capacidade de detectar malwares de código aberto, como por exemplo o Mirai Botnet.

Meidan et al. [Meidan et al. 2018] apresentam uma abordagem de padrões não supervisionados usando Deep Autoencoders para detectar botnets em redes IoT. Os autores sugerem que apenas vinte e três características para treinar o método de aprendizagem são suficientes para atingir a precisão adequada. Os experimentos foram realizados em um ambiente de teste composto por dispositivos IoT. No entanto, este trabalho é específico para detecção de botnet e não considera a capacidade de processamento dos dispositivos e outras limitações existentes nas redes IoT.

Embora vários estudos tenham sido realizados com a finalidade de identificar categorias de anomalias em tráfego de redes e DDoS, nenhum desses trabalhos acima abordam um cenário realístico de uma infraestrutura heterogênea em uma rede IoT. Abaixo estão

relacionados alguns aspectos negativos encontrados nos trabalhos citados: Dispositivos IoT simulados, Cenário de ataque indefinido, Não inclui o tráfego realístico (somente normal ou somente ataques) e seleção de características inadequada (ignoram ou utilizam de forma empírica). Sendo assim, o sistema proposto avança o estado da arte no que se refere a soluções de segurança para redes IoT, focando na detecção de ataques DDoS usando Redes Neurais e Seleção de Características, bem como a aplicação de uma abordagem integrando Computação em Névoa e em Nuvem.

3. Proposta

Redes IoT são compostas por dispositivos heterogêneos, como sensores, atuadores, câmeras de vigilância, smartbands, dentre outros. Cada um desses dispositivos segue funcionalidades específicas e, consequentemente, comportamento de rede singular para uma determinada classe de dispositivo. Por exemplo, os sensores de temperatura realizam transmissões periódicas para um servidor, atualizando um conjunto de dados, enquanto que as câmeras de vigilância transmitem constantemente as imagens capturadas.

Essas características aumentam a complexidade de gestão e, consequentemente, o desenvolvimento de soluções de segurança, devido às limitações dos dispositivos (capacidade de processamento, consumo de energia, etc). Uma das soluções de segurança mais importante é a detecção de ataques DDoS, visto que afeta diretamente os serviços que executam sobre as redes IoT. Com base nisso, este artigo propõe um sistema de Detecção Inteligente de DDoS usando um modelo de rede neural e com suporte de Computação em Névoa e em Nuvem.

O sistema proposto realiza as seguintes etapas: (I) Monitoramento da Rede; (II) Extração e Seleção de características; (III) Treinamento do Modelo de Rede Neural; e (IV) Detecção de DDoS. O fluxo de execução é apresentado na Figura 1. Inicialmente, é gerado um conjunto de dados formado pelo monitoramento dos fluxos de rede IoT. Posteriormente, extrai-se as características possíveis deste conjunto de dados e aplica-se alguma técnica para a seleção de características, tornando esses dados processados. Esses dados processados são utilizados como entrada para o treinamento do modelo de Rede Neural, que gera um detector de ataques DDoS. O treinamento do modelo é realizado em um ambiente de Computação em Nuvem, enquanto que as demais etapas ocorrem em um ambiente de Computação em Névoa.

Durante as fases de seleção de características e treinamento do modelo, diversas técnicas podem ser utilizadas. A partir disso, durante o desenvolvimento do mecanismo proposto foram analisadas e avaliadas diversas técnicas existentes a serem aplicadas no contexto deste trabalho.

A seguir são apresentados detalhes de cada uma das fases executadas do mecanismo de detecção de DDoS proposto, bem como a descrição da integração entre Névoa e Nuvem, a fim de alcançar os aspectos de escalabilidade e adaptabilidade necessários para as soluções de segurança em redes IoT.

3.1. Monitoramento e extração de características

A partir do monitoramento da rede de dispositivos IoT é possível gerar um conjunto de dados em um formato PCAP, o qual permite a extração de 80 (oitenta) características de fluxo de rede (usando por exemplo a ferramenta CICFlowMeter [Sharafaldin et al. 2019]).

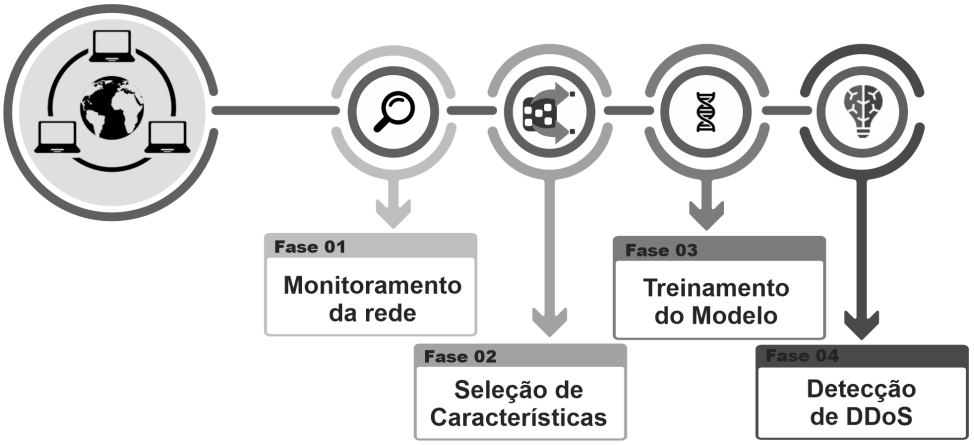

Figura 1. Fluxo de processamento do sistema proposto

Todavia, o uso de todas essas características pode gerar ruídos que dificultam o treinamento do modelo de Rede Neural do sistema proposto. Portanto, identificar quais características maximizam a capacidade de detecção torna-se uma tarefa crucial. Além disso, quando somente as características mais relevantes são consideradas, pode-se minimizar o tempo de treinamento do modelo e reduzir a demanda por recursos computacionais (processamento mais rápido, menor consumo de memória e menor espaço de armazenamento), devido a redução de dimensionalidade do problema. (https://github.com/ahlashkari/CICFlowMeter/blob/master/ReadMe.txt)

3.2. Seleção de Características

Este artigo avaliou o uso das seguintes técnicas de seleção de características: (A) Máxima relevância Mínima Redundância (mRMR), (B) Baixa Variância (BV), (C) Extra-Árvore (EA), (D) Vetores de Suporte Linear (SVC) e (E) Lasso. Essas técnicas foram escolhidas pois aplicam diferentes estratégias (filtros, embrulhos, análise estatística ou métodos incorporados), permitindo uma avaliação mais abrangente das diferentes características selecionadas [Kaushik 2016]. Para cada uma dessas técnicas utilizadas nos experimentos um conjunto de características são escolhidas como sendo as mais relevantes, logo cada técnica de acordo com seu algoritmo de escolha de característica relevantes, extrai os atributos que julgam ser melhores.

3.3. Treinamento do modelo de Rede Neural

Após a seleção das características mais adequadas, é iniciada a fase de treinamento do modelo de rede neural que resulta em um classificador que analisa os dados selecionados de entrada e detecta os dispositivos participantes de um ataque DDoS. Nesse trabalho foi utilizado o Multi-layer Perceptron (MLP), que é um algoritmo de aprendizado supervisionado que aprende uma função $f(.) : R^m \rightarrow R^o$ treinando em um conjunto de dados, onde m é o número de dimensões para entrada e o é o número de dimensões para saída. Dado um conjunto de recursos $X = x1, x2, ..., xm$ e um alvo y, ele pode aprender um aproximador de função não linear para classificação ou regressão. É diferente da regressão logística, pois entre a camada de entrada e a de saída pode haver uma ou mais camadas não lineares, chamadas de camadas ocultas.

A camada mais à esquerda, conhecida como camada de entrada, consiste em um conjunto de neurônios $xi|x1, x2, ..., xm$ representando os recursos de entrada. Cada neurônio na camada oculta transforma os valores da camada anterior com uma soma linear ponderada $w1x1 + w2x2 + ... + wmxm$, seguido por uma função de ativação não linear $g(.) : R \rightarrow R-$ como a função bronzeadora hiperbólica. A camada de saída recebe os valores da última camada oculta e os transforma em valores de saída.

As vantagens do Multi-layer Perceptron (MLP) são: Capacidade de aprender modelos não lineares; capacidade de aprender modelos em tempo real (aprendizado on-line) usando partial_fit.

3.4. Integração entre Computação em Névoa e em Nuvem

Os dados de monitoramento dos fluxos de rede IoT são processados na Névoa (extração e seleção de características) antes de serem transmitidos para a Nuvem (onde ocorre o treinamento da rede neural). Esta estruturação de tarefas agrega duas características cruciais a solução proposta: (1) Pequeno *overhead* na infratestrutura de rede, visto que um baixo volume de dados é trocado entre Névoa e Nuvem; e, (2) Adequabilidade de execução, pois cada etapa do sistema proposto executa no local mais adequado, ou seja, a rede neural é treinada na Nuvem (demandando muito poder computacional) e o processamento dos dados ocorre na névoa. Assim, estas características permitem a solução proposta atender os aspectos de escalabilidade, adaptabilidade e tempo de resposta necessários para detectar DDoS em redes IoT [Pisani et al. 2020].

4. Experimentos

Esta seção apresenta os experimentos realizados para avaliar o Sistema Inteligente proposto para detecção de DDoS, os quais focaram na avaliação da integração entre Nuvem e Névoa e do modelo de rede neural com as técnicas de seleção de características.

4.1. Configuração dos Experimentos

Durante os experimentos, foram avaliadas as seguintes técnicas de seleção: Extra-Arvore, SVC, Lasso, Baixa Variância e mRMR (casos de 5, 10, 20, 30 e 40 características), onde a lista das características selecionadas por cada técnica está disponível no Github[1]).

Os experimentos foram baseados no conjunto de dados "BoT-IoT"[2] desenvolvido por Meidan et al. [Meidan et al. 2018], que contém o tráfego normal (benigno) e o tráfego relacionado aos últimos ataques DDoS, o qual segue o formato de dados de monitoramento do mundo real (PCAPs).

O desempenho do sistema inteligente proposto (incluindo a combinação das técnicas de seleção e rede neural) considerou as seguintes métricas de avaliação: Acurácia (em porcentagem), representando a taxa de classificações corretas; recall (em porcentagem) são as previsões positivas realizadas corretamente e todas as previsões que realmente são positivas; Tempo de treinamento (em segundos) do detector DDoS com as características de entrada selecionadas; Tempo de detecção de ataques DDoS (em segundos); e, Volume de Dados (em Gigabyte/Megabytes) gerados (dados processados) a serem trocados entre Névoa e Nuvem.

[1]https://github.com/wandersonleo10/pesquisa/blob/master/lista%20de%20caracter%C3%ADsticas.txt
[2]https://www.unsw.adfa.edu.au/unsw-canberra-cyber/cybersecurity/ADFA-NB15-Datasets/bot_iot.php

4.2. Resultados

A Tabela 1 apresenta os resultados de acurácia, volume de dados trocados, tempo de treinamento (em segundos), tempo de detecção (em segundos) e recall do modelo de Rede Neural em conjunto com as técnicas de seleção definidas neste artigo. Portanto, apresenta-se o desempenho dos 11 casos com todas as combinações possíveis. É válido ressaltar duas informações: Ao lado de cada técnica é informado entre parênteses o número de características selecionadas pela mesma; e, Os dados brutos processados (formato PCAP antes de extração) tinham um volume de 15.16GBs.

Tabela 1. Resultados da Rede Neural (MPL)

Rede Neural com Técnica de Seleção	**Acurácia (%)**	**Recall (%)**	**Tempo de Treinamento**	**Tempo de Detecção**	**Volume de Dados**
Extração (80 características)	77.66	64.03	62.43	0.09	4.17GB
BV (63 características)	61.14	69.29	25.44	0.03	88MB
SVC (18 características)	99.99	100.00	19.52	0.04	21MB
Extra-Árvore (22 características)	63.86	63.09	41.90	0.07	22MB
Lasso (64 características)	99.96	99.95	28.36	0.04	84MB
mRMR (05 características)	78.60	77.50	20.18	0.04	5MB
mRMR (10 características)	79.30	99.83	38.66	0.04	9MB
mRMR (20 características)	99.26	78.35	61.86	0.06	22MB
mRMR (30 características)	99.98	50.00	24.67	0.06	37MB
mRMR (40 características)	99.97	70.01	11.75	0.04	50MB

Os resultados dos experimentos apresentados na Tabela 1 destacam a importância da seleção de características para a acurácia, tempo de execução e volume de dados. Por exemplo, usando a técnica de seleção mais apropriada, o desempenho da rede neural aumenta em 25%, aproximadamente. Além disso, a técnica RL usando os 80 atributos extraídos (sem seleção) tem uma acurácia inaceitável, em comparação a técnica SVC e mRMR a partir de 20 características.

Considerando-se o tempo de treinamento, aumenta a sua importância em contextos em que é necessário um treino recorrente para atualizar a rede neural em virtude da alta dinâmica dos ambientes IoT. Assim, a rede neural será treinada em um período muito curto de tempo para manter a detecção de ataques DDoS de forma eficaz. O mesmo raciocínio pode ser aplicado ao tempo de detecção. Nesse contexto, a rede neural quando utilizada com todas as técnicas de seleção de características, apresenta melhora significativa quando comparada em contexto sem seleção de características. Por outro lado, se a periodicidade do treinamento for maior, devido ao comportamento estático do SE (como uma indústria inteligente), outras abordagens são viáveis.

Outro ponto importante a ser destacado é a redução do volume de dados a ser transferido da Névoa para a Nuvem. Em se tratando do volume total de dados gerado pela monitoramento da rede torna-se inviável para o envio de aproximadamente 15GB da fonte dos dados para a nuvem, todavia, ao utilizar a técnica de seleção de característica adequada, por exemplo, a SVC, é possível chegar a uma redução em até 99% do volume real a ser analisado na rede, apresentando a importância do pré-processamento (seleção de características) próximo a fonte de dados (Névoa). Logo a arquitetura baseada em Névoa e Nuvem torna-se indispensável para a implementação da proposta.

5. Conclusão e trabalhos futuros

A evolução dos dispositivos de Internet das Coisas permitiu o desenvolvimento de novas soluções para melhorar a execução das atividades diárias, impulsionando a implantação de redes IoT em casas inteligentes, cidades inteligentes, etc. Contudo, os dispositivos IoT ainda não possuem aspectos de segurança adequados, tornando-se vulneráveis a Ataques de Negação de Serviço Distribuído (DDoS).

Nesse contexto, este artigo apresentou um Sistema Inteligente para Detecção de ataques DDoS em Redes IoT, baseado em Redes Neurais (RN) e Técnicas de Seleção de Características, possibilitando a identificação da melhor composição de características para o treinamento do modelo. Adicionalmente, o sistema proposto aplica uma abordagem com integração entre Computação em Névoa e em Nuvem a fim de alcançar a escalabilidade e adaptabilidade necessárias. Os resultados da avaliação de desempenho com base no tráfego real indicam 99% de acurácia (em média) para detectar ataques DDoS, enquanto o tempo de treinamento foi de 25 segundos (em média), indicando a viabilidade do sistema proposto para atuar em redes IoT reais.

Como trabalhos futuros, pretendemos investigar uma nova solução de segurança para outras ameaças as redes IoT (como *Side-Channel, Service Scan, Keylogging* e *Data Exfiltration*), bem como a capacidade do modelo desenvolvido de detectar os ataques dentro do campus universitário.

Referências

Brun, O., Yin, Y., Augusto-Gonzalez, J., Ramos, M., and Gelenbe, E. (2018). Iot attack detection with deep learning. In *ISCIS Security Workshop*.

Doshi, R., Apthorpe, N., and Feamster, N. (2018). Machine learning ddos detection for consumer internet of things devices. In *2018 IEEE Security and Privacy Workshops (SPW)*, pages 29–35. IEEE.

HaddadPajouh, H., Dehghantanha, A., Khayami, R., and Choo, K.-K. R. (2018). A deep recurrent neural network based approach for internet of things malware threat hunting. *Future Generation Computer Systems*, 85:88 – 96.

Kaushik, S. (2016). Introduction to feature selection methods with an example (or how to select the right variables?). *Analytics Vidhya*.

Meidan, Y., Bohadana, M., Mathov, Y., Mirsky, Y., Shabtai, A., Breitenbacher, D., and Elovici, Y. (2018). N-baiot—network-based detection of iot botnet attacks using deep autoencoders. *IEEE Pervasive Computing*, 17(3):12–22.

Pisani, F., de Oliveira, F. M. C., Gama, E. S., Immich, R., Bittencourt, L. F., and Borin, E. (2020). Fog computing on constrained devices: Paving the way for the future iot.

Sharafaldin, I., Lashkari, A. H., Hakak, S., and Ghorbani, A. A. (2019). Developing realistic distributed denial of service (ddos) attack dataset and taxonomy. In *2019 International Carnahan Conference on Security Technology (ICCST)*, pages 1–8. IEEE.

Yamauchi, M., Ohsita, Y., Murata, M., Ueda, K., and Kato, Y. (2019). Anomaly detection for smart home based on user behavior. In *2019 IEEE International Conference on Consumer Electronics (ICCE)*, pages 1–6. IEEE.