Transferência de conhecimento para detecção de ataques em Internet das Coisas

Israel Faustino Botelho Junior[1], **Bruno Bogaz Zarpelão**[1]

[1]Departamento de Computação – Universidade Estadual de Londrina (UEL)
Caixa Postal 10.011 – CEP 86057-970 – Londrina – PR – Brasil

israel.faustino@uel.br, brunozarpelao@uel.br

Abstract. *The growing availability of affordable integrated circuit and remote internet access has led to a substantial increase in the number of IoT (Internet of Things) devices in recent years. However, this growth has also witnessed a surge in security threats targeting these devices, making even everyday objects like lamps and refrigerators vulnerable to attacks. Detecting these attacks is crucial and can be addressed through machine learning, which can identify attack patterns. Nevertheless, the diversity of models and manufacturers of IoT devices complicates the reuse of machine learning models trained for similar devices. In this context, this work aims to explore transfer learning techniques to repurpose machine learning models from analogous devices, reducing the cost and effort required to train new models. This approach holds the promise of enhancing the security and effectiveness of attack detection in IoT devices.*

Resumo. *Com a crescente disponibilidade de circuitos integrados baratos e o acesso à Internet remoto, o número de dispositivos IoT (Internet das Coisas) aumentou significativamente nos últimos anos. No entanto, esse crescimento também trouxe um aumento nas ameaças à segurança desses dispositivos, tornando até mesmo objetos cotidianos, como lâmpadas e geladeiras, alvos de ataques. A detecção desses ataques é fundamental e pode ser abordada por meio do aprendizado de máquina, que é capaz de identificar padrões de ataques. No entanto, a diversidade de modelos e fabricantes de dispositivos IoT dificulta o reuso de modelos de aprendizado de máquina treinados para outros dispositivos similares. Nesse contexto, este trabalho tem como objetivo explorar técnicas de transferência de conhecimento para reaproveitar modelos de aprendizado de máquina de dispositivos semelhantes, reduzindo o custo e o esforço necessários para treinar novos modelos. Essa abordagem promete melhorar a segurança e a eficácia da detecção de ataques em dispositivos IoT.*

1. Introdução

Sistemas de Internet das Coisas (IoT - *Internet of Things*) estão amplamente presentes nos dias de hoje. Esses sistemas descrevem uma rede de objetos conectados a sensores, programas ou outras tecnologias, com o objetivo de trocar informações com outros sistemas, geralmente por meio da Internet [2]. O uso de IoT varia desde eletrodomésticos, como lâmpadas e geladeiras, até veículos aéreos não tripulados e sensores em barragens. Devido à diversidade desses sistemas e a sua alta versatilidade, houve um aumento significativo na sua fabricação e uso nos últimos anos, atingindo 14,3 bilhões de dispositivos em 2023 [3].

No entanto, apesar de sua ampla utilização, a segurança desses dispositivos é precária, tornando-os suscetíveis a ataques. Diversas vulnerabilidades são comumente encontradas, como senhas fracas, *backdoors*, falha de autenticação, entre outras [26]. Um reflexo disso é o aumento expressivo de *malwares* voltados para IoT, que alcançou 112,3 milhões de instâncias de *malware* em 2022, o que representa um aumento de 66% em relação a 2021 [24].

Normalmente, os dispositivos conectados à rede possuem um padrão nos pacotes que enviam e recebem. Por esse motivo, a partir do momento em que ocorre um ataque, é possível diferenciar sua atividade das atividades normais [11]. Uma forma comum de detectar essas atividades é por meio do uso de algoritmos de aprendizado de máquina, que conseguem analisar e descrever comportamentos com base em padrões [12].

Contudo, os sistemas IoT são geralmente compostos por dispositivos heterogêneos, ou seja, dispositivos com diferentes configurações e fabricantes, o que resulta na falta de padronização entre eles [12]. Além disso, modelos de aprendizado de máquina são treinados para aplicações específicas, o que requer muito tempo computacional e um grande conjunto de dados [15, 25]. Portanto, ao alterar o ambiente no qual o sistema se encontra, a acurácia das detecções de ataques pode diminuir e até mesmo exigir um novo treinamento [25].

Uma forma de reduzir a necessidade de novos treinamentos é através da transferência de conhecimento, um método de aprendizado de máquina. O método utiliza informações de uma tarefa, como um modelo de classificação, e aplica em outra tarefa, permitindo o acúmulo de conhecimentos de diferentes modelos previamente treinados [18, 25]. Como resultado da aplicação desse modelo, pode-se aproveitar a similaridade entre os dispositivos IoT para reduzir o tempo e custo necessários para o treinamento de modelos em novos ambientes [15].

Diante disso, o principal objetivo deste trabalho é explorar e analisar diferentes abordagens de aprendizado de máquina com transferência de conhecimento, a fim de tornar o treinamento de modelos para sistemas IoT mais eficiente e preciso. Para alcançar esse propósito, inicialmente será realizado um levantamento bibliográfico para investigar a literatura existente sobre o tema. Em seguida, serão identificadas e selecionadas as abordagens de aprendizado de máquina e transferência de conhecimento mais adequadas para a problemática da segurança de sistemas IoT. Após isso, será feita a seleção e identificação de conjuntos de dados capaz de fornecer diversas situações de testes, e por fim, serão realizados testes capazes de medir a acurácia com ou sem a transferência de conhecimento.

2. Fundamentação Teórico-Metodológica e Estado da Arte

2.1. Aprendizado de Máquina

O aprendizado de máquina é uma subárea da inteligência artificial (IA) e um ramo em ascensão dos algoritmos computacionais. Ele foi projetado para imitar a inteligência humana e aprender com o ambiente ao seu redor [8].

Neste campo, utilizam-se algoritmos e modelos estatísticos para aprender a executar tarefas sem depender de instruções explícitas [23]. Esses algoritmos são construídos a

partir de modelos gerais com parâmetros ajustáveis que, ao receberem diferentes valores, realizam diversos cálculos para otimizar os critérios de desempenho [6].

O processo de aprendizagem é dividido em duas etapas principais: treinamento e predição. Durante a fase de treinamento, o processo de aprendizagem ocorre de forma repetitiva e incremental. Os algoritmos processam exemplos um após o outro, ajustando gradualmente os parâmetros do modelo para aprimorar o desempenho. Na fase de predição, os exemplos são processados com base nos parâmetros calculados, resultando em saídas rotuladas [6].

Além disso, o aprendizado de máquina é categorizado com base nos seus rótulos em três categorias principais: supervisionado, não supervisionado e semi-supervisionado.

- **Aprendizado de máquina supervisionado:** No aprendizado de máquina supervisionado, utiliza-se um conjunto de dados pré-definidos para estimar um valor desconhecido. O treinamento envolve uma série de valores em pares ordenados (entrada, saída), onde a saída é rotulada com o resultado esperado [9]. Isso resulta em valores numéricos contínuos (regressão) ou valores discretos que preveem rótulos (classificação) [16, 7].
- **Aprendizado de máquina não-supervisionado:** No aprendizado de máquina não supervisionado, não são usados rótulos manuais. Durante o treinamento, apenas as informações de entrada são processadas, sem qualquer saída associada a um resultado. No entanto, é possível construir uma estrutura formal para esse modelo com base no estabelecimento de relações entre as entradas [10]. Isso é comumente usado em tarefas como agrupamento, regras de associação e redução de dimensionalidade [10, 7, 20].
- **Aprendizado de máquina semi-supervisionado:** O aprendizado de máquina semi-supervisionado, por sua vez, é uma combinação das abordagens supervisionada e não supervisionada, utilizando tanto dados rotulados quanto não rotulados [8, 7].

2.2. Transferência de Conhecimento

A transferência de conhecimento é uma subárea do aprendizado de máquina que se baseia na aplicação inteligente de conhecimentos de tarefas anteriores em novos problemas, com o objetivo de torná-los mais rápidos e eficazes [19]. A transferência de conhecimento pode ser descrita a partir de duas notações: domínio e tarefa.

- **Domínio:** Um Domínio $\mathcal{D}$ pode ser explicado como a combinação de duas partes essenciais: um espaço de características $\mathcal{X}$ e uma distribuição probabilística marginal $P(X)$, onde $X = x_1, ..., x_n \in \mathcal{X}$. Em termos simples, um domínio $\mathcal{D}$ está diretamente ligado à forma como os dados são distribuídos e usados para treinar modelos de aprendizado de máquina [21, 30].
- **Tarefa:** Uma tarefa $\mathcal{T}$ é uma combinação de duas partes fundamentais: um espaço de rótulos $\mathcal{Y}$ e uma função de predição $f(\cdot)$. Essa função de predição, baseada em um domínio $\mathcal{D}$, realiza previsões que geram rótulos. Ela aprende com os dados de treinamento, que consistem em pares ordenados x_i, y_i, onde x_i é a entrada e y_i é um rótulo. Em termos simples, uma tarefa $\mathcal{T}$ está intimamente ligada ao modelo e às operações computacionais que desempenham um papel crucial na realização de previsões [21, 30, 27].

Com base nos conceitos definidos acima, a transferência de conhecimento pode ser definida como o processo de aprimorar a função de predição de uma tarefa, utilizando o conhecimento adquirido de outra tarefa e seu domínio. Para isso, tanto o domínio quanto a tarefa são diferentes de uma para outra [21]. É possível denominar o domínio e a tarefa que fornecem o conhecimento como "origem"e o domínio e a tarefa onde serão utilizados como "alvo".

O processo de transferência de conhecimento de uma tarefa para outra pode ser visualizado na Figura 1. Nessa representação, pode-se observar o conhecimento fluindo da tarefa de origem para ser aplicado na tarefa alvo, onde ambos os domínios estão no mesmo espaço de características.

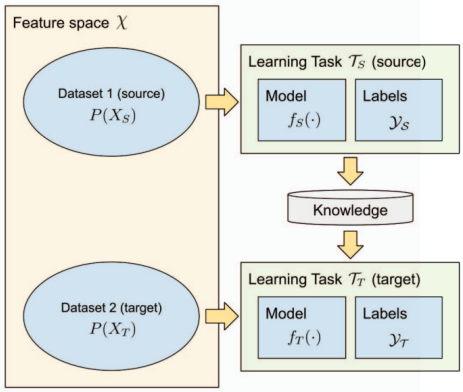

Figura 1. Representação da transferência de conhecimento pelas definições de domínio e tarefa. Fonte: [21]

Uma maneira de classificar a transferência de conhecimento é considerar a disponibilidade de rótulos nos domínios. Quando há rótulos disponíveis no domínio alvo, a transferência de conhecimento é classificada como indutiva. Nessa abordagem, a tarefa de origem e a tarefa alvo são diferentes, e as informações do domínio alvo são utilizadas para ajustar um modelo de previsão. Isso implica que o modelo é adaptado usando as informações e rótulos do domínio de destino para criar uma função de predição específica para a nova tarefa. Essa abordagem é semelhante a aprender com exemplos do domínio de origem que são semelhantes, embora não idênticos, à nova tarefa [19, 27].

Por outro lado, quando não há rótulos disponíveis no domínio alvo, mas existem rótulos no domínio de origem, a transferência de conhecimento é classificada como transdutiva. Nesse caso, a tarefa de origem e a tarefa alvo são as mesmas, mas seus domínios são diferentes. Aqui, o desafio é aplicar o conhecimento adquirido no domínio de origem ao domínio de destino, mesmo que este último não tenha rótulos. Isso geralmente envolve a adaptação de domínio, onde tentamos tornar os dados do domínio de origem úteis para prever resultados no domínio de destino, mesmo que as características dos dados possam ser diferentes [19].

Por fim, quando não existem rótulos disponíveis nos domínios de origem e alvo, a transferência é classificada como não supervisionada. Seu foco, semelhante ao do aprendizado de máquina não supervisionado, é estabelecer relações entre os dados e resolver

problemas similares, como agrupamento, redução de dimensionalidade e estimativa de densidade [10, 19].

2.3. Internet das Coisas

Internet das Coisas, também conhecida como *Internet of Things* (IoT), é um termo criado em 1999 por Kevin Ashton, que descreve um sistema no qual objetos do mundo real podem ser conectados à internet por meio de sensores [22]. Atualmente, devido ao advento de circuitos integrados de computadores baratos, o termo se tornou popular e abrange diversos objetos do dia a dia que tiveram suas funções integradas à internet [1, 22].

Um sistema IoT funciona coletando e trocando dados em tempo real, utilizando diversos objetos ao nosso redor, como sensores e dispositivos inteligentes. Com a popularização do conceito de *smart home*, muitos dispositivos do dia a dia passaram a ser integrados à internet, resultando em um aumento na disponibilidade de dados. Alguns desses objetos que podemos encontrar facilmente em residências incluem lâmpadas inteligentes, geladeiras inteligentes, assistentes de voz, entre outros.

Existem diversas arquitetura para IoT, a que iremos usar nesse projeto é dividida em três camadas: física, rede e aplicação.

- **Camada física:** A camada física atua como a interface inicial entre o mundo físico e o mundo digital da IoT. Sua responsabilidade é identificar objetos e coletar informações por meio de sensores e dispositivos [13, 28].
- **Camada de rede:** A camada de rede é responsável por transmitir as informações obtidas pela camada física. Para isso, utiliza protocolos de rede, como TCP/IP [13, 28].
- **Camada de aplicação:** A camada de aplicação representa a interface final da IoT com os usuários e as aplicações específicas. Ela se concentra em atender às demandas das indústrias e das necessidades sociais, possibilitando a aplicação inteligente da IoT em diversos cenários [13, 28].

Existem diversos modelos pelos quais os dispositivos podem se comunicar, os quais definem regras e organizações para que os dispositivos possam se comunicar entre si e com outras aplicações [22]. Esses modelos de comunicação são classificados em: comunicação dispositivo-para-dispositivo (*Device-to-Device Communication*), comunicação dispositivo-para-Gateway (*Device-to-Gateway Communication*) e comunicação dispositivo-para-internet (*Device-to-Internet Communication*).

O modelo de comunicação dispositivo-para-dispositivo ocorre quando um dispositivo se comunica diretamente com outro, sem a necessidade de utilizar um serviço intermediário. Diferentes métodos podem ser empregados para possibilitar essa comunicação, como Bluetooth e Wi-Fi. Por outro lado, o modelo de comunicação dispositivo-para-Gateway ocorre quando se utiliza um serviço auxiliar ou um Gateway, um dispositivo capaz de conectar duas redes, para permitir que um dispositivo IoT se comunique com a internet ou faça uso de serviços em nuvem. Um exemplo de comunicação dispositivo-para-Gateway ocorre quando diversas lâmpadas inteligentes são conectadas a um roteador, permitindo controla-las por um telefone. Por fim, o modelo de comunicação dispositivo-para-internet ocorre quando um dispositivo consegue acessar a internet ou um serviço em nuvem diretamente [17, 22].

2.4. Detecção de Ataques em IoT

A detecção de ataques em dispositivos de IoT é uma tarefa crítica para garantir a segurança desses sistemas altamente conectados. Existem diversas ameaças que podem visar os dispositivos IoT, e para cada tipo de ataque, é necessário encontrar uma solução adequada. No entanto, a simples combinação de todas essas soluções pode impactar negativamente o desempenho geral dos dispositivos IoT, o que se torna um dos problemas de segurança nesse contexto [5].

Para lidar com esse desafio, foram propostas diferentes técnicas e ferramentas que se concentram em estudar o comportamento do sistema. Uma dessas ferramentas é o sistema de detecção de intrusão (IDS), cujo propósito principal é detectar qualquer atividade suspeita que ocorra na rede alvo [4]. Com essa finalidade, sensores são posicionados em locais estratégicos para a captura de tráfego de rede, cabeçalhos de pacotes, requisições de serviço, mudanças de arquivos e chamadas de sistema [29].

No IDS, é possível a detecção com base em padrões de ataques previamente conhecidos (detecção por assinatura). Nesse método, o sistema identifica um ataque comparando os traços da atividade na rede com os traços de ataques pré-instalados no banco de dados do IDS. Esse método permite a identificação eficaz de ataques conhecidos, mas caso seja um novo tipo de ataque, o IDS não é capaz de identificá-lo [4, 14].

Também é possível a detecção com base em comportamentos fora do padrão no tráfego de rede (detecção por anomalia). Nesse método, o sistema identifica qualquer anomalia na rede, analisando seu comportamento e verificando se a atividade ultrapassa um limite estabelecido. Esse método permite a detecção de vários tipos de ataques sem a necessidade de conhecimento prévio, no entanto, pode apresentar várias análises imprecisas, como falsos positivos [4, 14].

Além disso, é possível a detecção com base em regras estabelecidas pelo sistema, como a detecção baseada em especificação. Esse método consiste em identificar ataques quando sua atividade não está em conformidade com as especificações criadas. Esse método permite distinguir comandos inesperados de ataques, mas caso o ataque respeite as regras, ele passa despercebido [4, 14].

Outra técnica amplamente utilizada para a detecção de ataques em IoT é o uso de aprendizado de máquina. Nesse caso, os dados coletados dos dispositivos IoT são usados para treinar modelos de aprendizado de máquina. Esses modelos são então empregados para observar e detectar possíveis ataques na rede IoT [5].

3. Objetivos

Este trabalho tem como objetivo principal desenvolver e implementar um método de aprendizado de máquina com transferência de conhecimento para detecção de ataques em IoT. Para alcançar esse objetivo principal foram especificados os seguintes objetivos específicos:

1. Identificar critérios para classificar dispositivos IoT para o processo de transferência de conhecimento.
2. Selecionar conjuntos de dados com amostras de diferentes categorias, destacando que cada amostra possui objetos distintos entre si.

3. Comparar algoritmos de detecção de ataques com transferência de conhecimento indutivos e transdutivos a fim de verificar qual possuí o maior benefício.
4. Comparar algoritmos de detecção que possuí diversos conjuntos separando atividade normal de anomalia com algoritmos de detecção com um conjunto de dados contendo ambos.
5. Analisar se ouve melhora ou piora na capacidade preditiva de modelos usando a transferência de conhecimento.

4. Procedimentos metodológicos/ Métodos e técnicas

O primeiro passo consiste em realizar uma revisão bibliográfica e selecionar técnicas de aprendizado de máquina com transferência de conhecimento que possam ser aplicadas em IoT. Essa revisão será conduzida com o objetivo de encontrar trabalhos que possibilitem a replicação e a refatoração, além de serem relevantes para o projeto em questão

Em seguida, será necessário identificar diversas categorias de IoT adequadas para o trabalho. Essas categorias correspondem a objetos inteligentes do dia a dia, como lâmpadas, geladeiras, tomadas, *smart TVs* e outros dispositivos similares. Dentro dessas categorias, haverá uma variedade de objetos de diferentes marcas ou modelos.

Além disso, será necessário identificar e avaliar conjuntos de dados apropriados que englobem as categorias mencionadas anteriormente. Esses conjuntos devem conter informações sobre redes IoT, incluindo amostras de tráfego comum e/ou anomalias. É essencial que esses conjuntos incluam amostras tanto de tráfego comum, quanto de anomalias separadamente.

Com os conjuntos de dados selecionados, será escolhida uma abordagem para o aprendizado de máquina que apresente as maiores vantagens para os sistemas IoT, levando em consideração suas dificuldades e necessidades específicas. Ademais será implementado uma técnica de transferência de conhecimento que permitirá utilizar as informações de um objeto em outro.

A próxima etapa consiste em realizar testes, utilizando métricas de acurácia, para verificar o quão eficaz foi a detecção de ataques nos dispositivos com ou sem transferência de conhecimento. Além disso, será comparada a eficácia da detecção antes e depois da transferência.

Ademais, serão realizados testes com conjuntos de dados que incluem anomalias e tráfego comum, bem como testes com vários conjuntos de dados separados entre anomalias e tráfego comum. Isso permitirá avaliar a eficiência dessas duas abordagens.

Por fim, com os resultados obtidos, será realizada uma comparação buscando identificar qual método obteve as melhores detecções e revelou mais vulnerabilidades.

5. Cronograma de Execução

De acordo com os procedimentos metodológicos/ métodos e técnicas, pode-se definir uma lista de atividades necessárias para a construção de um cronograma:

Atividades:

1. Revisão bibliográfica com foco em transferência de conhecimento;
2. Identificação de categorias de IoT;

3. Seleção de diferentes conjuntos de dados para diferentes categorias;
4. Implementação de aprendizado de máquina para as categorias;
5. Implementação de transferência de conhecimento;
6. Testes no conjunto de dados
7. Análise e comparação dos resultados;
8. Escrita do TCC;

	fev	mar	abr	mai	jun	jul	ago	set	out
Atividade 1	X	X							
Atividade 2			X						
Atividade 3			X	X					
Atividade 4					X	X			
Atividade 5							X		
Atividade 6								X	
Atividade 7						X	X	X	X

6. Contribuições e/ou Resultados esperados

Durante este trabalho, espera-se realizar testes e verificar a eficácia da transferência de conhecimento aplicada à detecção de ataques. Como resultado, esperamos identificar métodos e técnicas que possam aprimorar a segurança dos dispositivos IoT. Dessa forma, este projeto permitirá uma nova abordagem e perspectiva para os dispositivos IoT.

7. Espaço para assinaturas

Londrina, *quatro de março de dois mil de vinte e quatro*.

_____ _____

Aluno Orientador

Referências

[1] O que é a internet das coisas (iot). Disponível em: `https://aws.amazon.com/pt/what-is/iot/`. Acessado em: 9 de setembro de 2023.

[2] O que é iot? (internet das coisas) — oracle brasil. Disponível em: `https://www.oracle.com/br/internet-of-things/what-is-iot/`. Acessado em: 8 de junho de 2023.

[3] State of iot 2023: Number of connected iot devices growing 16 percent to 16.7 billion globally. Disponível em: `https://iot-analytics.com/number-connected-iot-devices/`. Acessado em: 8 de junho de 2023.

[4] Yahya Al-Hadhrami and Farookh Khadeer Hussain. DDoS attacks in IoT networks: a comprehensive systematic literature review. *World Wide Web*, 24(3):971–1001, May 2021.

[5] Najla Al-Taleb and Nazar Abbas Saqib. Attacks Detection and Prevention Systems for IoT Networks: A Survey. In *2020 International Conference on Computing and Information Technology (ICCIT-1441)*, pages 1–5, September 2020.

[6] Ethem Alpaydin. *Machine Learning, revised and updated edition*. MIT Press, August 2021. Google-Books-ID: 2nQJEAAAQBAJ.

[7] Taiwo Oladipupo Ayodele. Machine learning overview. *New Advances in Machine Learning*, 2:9–18, 2010.

[8] Issam El Naqa and Martin J Murphy. *What is machine learning?* Springer, 2015.

[9] TV Geetha and S Sendhilkumar. *Machine Learning: Concepts, Techniques and Applications*. CRC Press, 2023.

[10] Zoubin Ghahramani. *Unsupervised Learning*, pages 72–112. Springer Berlin Heidelberg, Berlin, Heidelberg, 2004.

[11] Ali A Ghorbani, Wei Lu, and Mahbod Tavallaee. *Network intrusion detection and prevention: concepts and techniques*, volume 47. Springer Science & Business Media, 2009.

[12] Muhammad Jahanzaib Gul and Muhammad Khaliq-ur-Rahman Raazi Syed. Network attack detection in iot using artificial intelligence. In *2023 International Multidisciplinary Conference in Emerging Research Trends (IMCERT)*, volume I, pages 1–6, 2023.

[13] Qi Jing, Athanasios V. Vasilakos, Jiafu Wan, Jingwei Lu, and Dechao Qiu. Security of the Internet of Things: perspectives and challenges. *Wireless Networks*, 20(8):2481–2501, November 2014.

[14] Hung-Jen Liao, Chun-Hung Richard Lin, Ying-Chih Lin, and Kuang-Yuan Tung. Intrusion detection system: A comprehensive review. *Journal of Network and Computer Applications*, 36(1):16–24, January 2013.

[15] Xing Liu, Wei Yu, Fan Liang, David Griffith, and Nada Golmie. Toward deep transfer learning in industrial internet of things. *IEEE Internet of Things Journal*, 8(15):12163–12175, 2021.

[16] Donald Michie, David J Spiegelhalter, and Charles C Taylor. Machine learning, neural and statistical classification. 1994.

[17] Boubakr Nour, Kashif Sharif, Fan Li, Sujit Biswas, Hassine Moungla, Mohsen Guizani, and Yu Wang. A survey of Internet of Things communication using ICN: A use case perspective. *Computer Communications*, 142-143:95–123, June 2019.

[18] Emilio Soria Olivas, Jos David Mart Guerrero, Marcelino Martinez-Sober, Jose Rafael Magdalena-Benedito, L Serrano, et al. *Handbook of research on machine learning applications and trends: Algorithms, methods, and techniques: Algorithms, methods, and techniques*. IGI global, 2009.

[19] Sinno Jialin Pan and Qiang Yang. A Survey on Transfer Learning. *IEEE Transactions on Knowledge and Data Engineering*, 22(10):1345–1359, October 2010. Conference Name: IEEE Transactions on Knowledge and Data Engineering.

[20] M.L. Raymer, W.F. Punch, E.D. Goodman, L.A. Kuhn, and A.K. Jain. Dimensionality reduction using genetic algorithms. *IEEE Transactions on Evolutionary Computation*, 4(2):164–171, 2000.

[21] Ricardo Ribani and Mauricio Marengoni. A Survey of Transfer Learning for Convolutional Neural Networks. In *2019 32nd SIBGRAPI Conference on Graphics, Patterns and Images Tutorials (SIBGRAPI-T)*, pages 47–57, October 2019. ISSN: 2474-0705.

[22] Karen Rose, Scott Eldridge, and Lyman Chapin. The Internet of Things: An Overview.

[23] Iqbal H. Sarker, A. S. M. Kayes, Shahriar Badsha, Hamed Alqahtani, Paul Watters, and Alex Ng. Cybersecurity data science: an overview from machine learning perspective. *Journal of Big Data*, 7(1):41, July 2020.

[24] SonicWall. Sonicwall cyber threat report. Technical report, SonicWall, 2023.

[25] Ly Vu, Quang Uy Nguyen, Diep N. Nguyen, Dinh Thai Hoang, and Eryk Dutkiewicz. Deep transfer learning for iot attack detection. *IEEE Access*, 8:107335–107344, 2020.

[26] Aohui Wang, Ruigang Liang, Xiaokang Liu, Yingjun Zhang, Kai Chen, and Jin Li. An inside look at iot malware. In Fulong Chen and Yonglong Luo, editors, *Industrial IoT Technologies and Applications*, pages 176–186, Cham, 2017. Springer International Publishing.

[27] Karl Weiss, Taghi M. Khoshgoftaar, and DingDing Wang. A survey of transfer learning. *Journal of Big Data*, 3(1):9, May 2016.

[28] Miao Wu, Ting-Jie Lu, Fei-Yang Ling, Jing Sun, and Hui-Ying Du. Research on the architecture of Internet of Things. In *2010 3rd International Conference on Advanced Computer Theory and Engineering(ICACTE)*, volume 5, pages V5–484–V5–487, August 2010. ISSN: 2154-7505.

[29] Bruno Bogaz Zarpelão, Rodrigo Sanches Miani, Cláudio Toshio Kawakani, and Sean Carlisto de Alvarenga. A survey of intrusion detection in Internet of Things. *Journal of Network and Computer Applications*, 84:25–37, April 2017.

[30] Fuzhen Zhuang, Zhiyuan Qi, Keyu Duan, Dongbo Xi, Yongchun Zhu, Hengshu Zhu, Hui Xiong, and Qing He. A Comprehensive Survey on Transfer Learning. *Proceedings of the IEEE*, 109(1):43–76, January 2021. Conference Name: Proceedings of the IEEE.