Trabalho de Conclusão de Curso

1ª Etapa - Pré-Projeto

ANOMAD IoT
Modelos para Detecção de Anomalias no Tráfego de Rede de Dispositivos IoT: Um Estudo Exploratório

Integrantes do Grupo:

Caio Franco de Souza

Gabriel Moiseis Ferreira Lima

José Antonio Guides Mequelin

Orientador(a): Prof.º Me. Guilherme Werneck de Oliveira

Co-orientador(a): Prof.º Gabriel Vinicius Canzi Candido

Pinhais

2024

1. Introdução

Com o decorrer dos anos e com o avanço da tecnologia, principalmente nas áreas de eletrônica, sistemas de sensoriamento e troca de informações expandiram horizontes e expectativas acerca de quais sistemas e dispositivos do mundo físico poderiam ser integrados à internet. Esses sistemas e dispositivos são conhecidos como IoT (sigla em inglês para Internet das Coisas). Estima-se que em 2025, haverá mais de 27 bilhões de dispositivos IoT conectados em todo o mundo (PACETE, 2022).

Ainda que a IoT tenha o papel de facilitar o cotidiano dos usuários, seja como meio de comunicação em empresas, seja para fins domésticos, existem diversos problemas ainda não solucionados satisfatoriamente, como a privacidade e a falta de segurança dos dispositivos em relação aos dados dos usuários. São comuns notícias de tentativas de ataques contra dispositivos IoT no mundo todo. Nos dois primeiros meses de 2023, por exemplo, quase todas as semanas, em média 54% das organizações foram alvo dessas tentativas de ataque, com uma média de quase 60 ataques por organização por semana direcionados a dispositivos de IoT. Uma alta de 41% em comparação com 2022 e mais que o triplo do número de ataques se comparados aos de dois anos atrás (ABRANET, 2023).

Ao decorrer disso, muitas pesquisas em relação a segurança de dispositivos IoT foram realizadas, por empresas, pesquisadores da área de TI e técnicos de cibersegurança. Com isso, foram desenvolvidos milhares de artigos e documentos relacionados à proteção de dados em dispositivos IoT. Trabalhos desenvolvidos com intuito de explicar e ajudar pessoas a compreender e entender, qual e melhor método para proteger seus dados.

Também foram criados protocolos de segurança para redes sem fio de IoT, que foram elaborados com intuito de defender as redes IoT contra ameaças e ataques às informações pessoais dos usuários. Esses são alguns dos protocolos, TLS (Transport Layer Security), DTLS (Datagram Transport Layer Security), CoAP (Constrained Application Protocol) e MQTT (Message Queuing Telemetry Transport). Apesar disso ainda se tem inúmeros ataques, pessoas que conseguem explorar as vulnerabilidades desses sistemas.

Assim, este trabalho tem como objetivo desenvolver um estudo de modelos utilizando algoritmos de aprendizagem de máquinas, para detectar anomalias no tráfego de rede do usuário. Essa abordagem será implementada para dispositivos em ambientes domésticos, no intuito de auxiliar a segurança das IoT e a informações e dados pessoais.

1.1 **Objetivo geral**

Desenvolver um estudo comparativo de modelos de aprendizagem de máquina para detecção de anomalias em redes de dispositivos IoT domésticos.

1.2 **Objetivos específicos**

- Identificar e avaliar os conjuntos de dados presentes na literatura que representam tráfegos de redes IoT domésticas;
- Elaborar uma análise exploratória de dados (do inglês, *Exploratory Data Analysis* - EDA) sobre o tráfego definido;
- Analisar e compreender os diferentes tipos de tráfego de redes IoT, incluindo tráfego normal e padrões de tráfego associados a ataques e anomalias;
- Selecionar, treinar e testar modelos de aprendizado de máquina para a identificação de padrões suspeitos e comportamentos anômalos no tráfego de rede;
- Comparar o desempenho dos modelos de aprendizado de máquina implementados, além de identificar possíveis melhorias.

1.3 **Justificativa**

Os dispositivos IoT, ou Internet das Coisas, são minicomputadores com funcionalidades concentradas em sensoriamento e comunicação através da rede, como câmeras, lâmpadas e sensores de movimento. Esses dispositivos estão presentes em ambientes domésticos e criam/oferecem desafios como a falta de tamanho para suportar as aplicações e a falta de segurança na troca de dados entre os IoT. Eles possuem um baixo poder de processamento e isso tem chamado a atenção dos atacantes. Sua capacidade computacional limitada não embarca mecanismos de segurança fortes, causando uma carência e risco de roubo de informações e ataques dentro do ambiente doméstico (XENOFONTOS et al., 2022; BUTUN et al., 2020; MENEGHELLO et al., 2019).

Segundo o site Compugraf (2021), desde o primeiro semestre de 2021 houve um aumento de mais de 100% de ataques a dispositivos IoT, com invasores visando o roubo de dados. Isso se torna ainda mais grave visto que, dado o contexto pós-COVID19 trabalhadores em regimes de trabalho híbrido ou remoto podem servir de alvos para criminosos que visam recursos corporativos por meio de redes domésticas e dispositivos IoT domésticos.

2. Trabalhos Correlatos

Esta seção tem como objetivo prover de forma resumida estudos correlatos à detecção de anomalias em ambientes domésticos que possuam dispositivos IoT. O foco principal é apresentar trabalhos que estudam e propõem métodos para detecção de ataques utilizando o algoritmo de aprendizado de máquinas em dispositivos IoT conectados à rede. Para tanto, a partir da pesquisa bibliográfica realizada foram selecionados os trabalhos descritos na Tabela 1 e, em seguida, suas contribuições para este projeto.

Tabela 1 - Trabalhos correlatos

Título	Autor
Detecção de Anomalias no Tráfego MQTT de Redes IOT Utilizando Técnicas de Aprendizado de Máquinas	Silva Filho (2021)
Estudo Sobre a Segurança de Dispositivos Domésticos Conectados à Internet das Coisas	Messas (2022)
Framework Para Detecção de Ataques em Dispositivos IOT, Utilizando Abordagens de Aprendizado de Máquinas	Oliveira (2023)
Segurança da Informação para Internet das Coisas (IoT): uma Abordagem sobre a Lei Geral de Proteção de Dados (LGPD)	Oliveira, et al. (2019)
Detecção de Ataques a Redes IoT Usando Técnicas de Aprendizado de Máquina e Aprendizado Profundo	Bochie, et al. (2020)
Guia de segurança da informação para a conectividade de dispositivos IoT	Berlanda (2021)
Um Método para Detecção de Vulnerabilidades Através da Análise do Tráfego de Rede IoT	Brezolin et al. (2022)
Gerência de Autenticação de Dispositivos IoT Adaptativa Aos Ambientes Urbanos Apoiada em Políticas e Confiança Social	Moraes, et al. (2022)
The internet of things security: A survey encompassing unexplored areas and new insights	Omolara, et al. (2022)

Fonte: Os Autores (2024).

2.1 Silva Filho (2021)

Esse trabalho propõe utilizar um sistema de detecção de anomalias em ambientes IoT de distintas infraestruturas, utilizando o protocolo MQTT para avaliar dois algoritmos de aprendizado de máquina, um comum em treinos offlines e outro adaptado e criado para streaming de dados, a interação entre técnicas de aprendizado de máquina e sistemas de detecção de intrusão baseado em assinaturas. O objetivo do projeto foi criar uma solução para a segurança de diferentes redes IoT que utilizam o protocolo MQTT em suas comunicações, sendo essa solução capaz de detectar ataques desconhecidos por meio da integração de técnicas de aprendizado de máquina e um sistema de detecção de intrusão baseado em assinaturas. A partir da pesquisa realizada, foi possível analisar o desempenho da solução proposta, com os

resultados, detectou anomalias com uma média de 60% de acerto. Além de resolver, utilizando técnicas de aprendizagem online, infelizmente há um problema no re-treino e mudança de domínio.

2.2 Messas (2022)

O trabalho tem como intuito testar aparelhos selecionados, com receptores de IPTV, TV Boxes e câmeras Wi-Fi, com o objetivo de estudar o modo de funcionamento de testes de invasão e aplicá-los a dispositivos eletrônicos variados conectados à internet, assim avaliando seus níveis de segurança. Para cada dispositivo analisado, o documento a ser gerado almeja atrair atenção e incitar os responsáveis a corrigir as brechas de confiabilidade do equipamento. Mais do que isso, o relato visa levantar questionamentos sobre a situação de aparelhos semelhantes e estimular a checagem destes mais eficazmente a fim de evitar defeitos. Nesse cenário, a pesquisa contribui para a realização desses procedimentos por parte de um maior público, o que também colabora para a adequação do padrão de qualidade dos aparelhos em questão: objetivo final desejável para o segmento.

2.3 Oliveira (2023)

O trabalho de pós-graduação da faculdade de Tecnologia da Universidade de Brasília, utiliza abordagens de aprendizado de máquinas com o objetivo de apresentar um framework completo para a detecção de intrusão de ataques DoS próximo ao tempo real, aplicando soluções relacionadas à segurança cibernética na camada de aplicação, desenvolvido para ambientes IoT, através de técnicas de aprendizado de máquina. A metodologia usada constitui-se em uma pesquisa quantitativa, baseada em números e gráficos para chegar no resultado aceitável, assim comparando com resultados já presentes na literatura atual. Para tanto, foram realizados experimentos utilizando provas de conceito de (PoC). Este trabalho apresentou um sistema que foi arquitetado para ser um recurso completo, sendo um método que tem como função gerenciamento de alarmes dos ataques ocorridos a dispositivos IoT. Assim arquitetado desde a captura dos fluxos de dados até a visualização do alarmes de ataques ocorridos.

2.4 Oliveira et al. (2019)

O artigo aborda aspectos da Lei Geral de Proteção de Dados (LGPD) relacionados ao uso de dispositivos IoT. Os autores reforçam a responsabilidade das empresas quanto ao uso e armazenamento dos dados de seus usuários, mostrando que essa responsabilidade pode ser alcançada através da aplicação de mecanismos de Segurança da Informação (SI). Os autores demonstram, ainda, preocupação relacionada aos riscos da privacidade dos usuários que

utilizam dispositivos IoT. Mesmo que a SI tenha evoluído para promover uma maior proteção em diversos dispositivos (incluindo móveis), isso nem sempre esteve diretamente relacionado a IoT devido às suas características.

2.5 Bochie et al.(2020)

Esse trabalho compara o desempenho de modelos de aprendizado tradicionais, tendo em vista características inerentes de redes IoT. Para tanto, os autores utilizam a metodologia de etapas a fim de destacar decisões importantes a serem tomadas especialmente durante o pré-processamento de dados, levando-se em consideração o grande volume de dados gerados por redes IoT que pode levar à especificidade de modelos tradicionais. Esse artigo apresentou uma avaliação de desempenho de modelos de aprendizado de máquina tradicionais e profundos e os comparou quando aplicados a dois conjuntos de dados contendo ataques a redes IoT. Os autores concluem dizendo que modelos de aprendizagem de máquinas sofisticados, como redes neurais, características sequenciais definidas são necessárias, como técnicas tradicionais de separação de conjuntos de dados podem ser prejudiciais ao desempenho. Com isso faz se necessário o uso de algoritmos arquitetados capazes de separar os dados e preservar as estruturas temporais.

2.6 Berlanda (2021)

Neste artigo, Berlanda (2021) aborda a indústria 4.0 junto com dispositivos IoT, apontando os desafios dessa nova tecnologia em fase de expansão. Em virtude do aumento considerável de aparelhos inteligentes conectados, a segurança das redes tende a diminuir por conta de números de possíveis alvos aumentarem. Isso ocorre, pois os dispositivos IoT ficam em grande parte localizados nas extremidades da rede, e fisicamente em locais de fácil acesso para qualquer pessoa mal-intencionada. No trabalho, são propostos métodos como a auditoria de segurança de TI, que consiste no processo que verifica se padrões de segurança são cumpridos, com o objetivo de melhorar a segurança desses dispositivos. Um processo que deve ser refeito periodicamente, pois qualquer mudança no cenário pode influenciar nos resultados, e consequentemente, na segurança da rede.

2.7 Brezolin et al. (2022)

O trabalho propõe o método MANDRAKE (do inglês, a **M**ethod for vulner**A**bilities detectio**N** base**D** on the IoT netwo**R**k p**A**c**KE**t traffic) para detectar vulnerabilidade em dispositivos IoT, por se tratar de uma abordagem simples, com baixo processamento e independente do conhecimento prévio da rede. Essa abordagem corresponde a três fases: (i) a captura e extração de características do tráfego da rede; (ii) a rotulação do tráfego baseado no

cálculo da entropia; e (iii) a classificação do tráfego através de técnicas de aprendizado de máquina. Os resultados apresentados apontam que o método MANDRAKE torna possível a rotulação da base, identificação da presença de tráfego vulnerável e de seus respectivos dispositivos de origem, sem conhecimento prévio da rede. Cada uma das fases do método foi avaliada experimentalmente com bases realistas.

2.8 Moraes et al. (2022)

Esse artigo propõe um sistema para a gerência adaptativa sobre os mecanismos de autenticação de dispositivos IoT aplicados a diversos ambientes, apoiado em confiança social e política de configuração de segurança, chamado GALENA (mana**G**ement of **A**daptive authentication based on po**L**ici**E**s a**N**d soci**A**l trust), que define o mecanismo de autenticação mais adequado para realizar o procedimento de autenticação entre os dispositivos IoT. Os resultados apresentados no documento mostram a sua eficiência para aplicar mecanismos de autenticação respeitando as características de cada dispositivo e os riscos nos ambientes IoT.

2.9 Omolara et al. (2022)

Esse artigo faz uma reflexão sobre as IoT mostrando que é uma nova onda de tecnologia que revolucionou a vida das pessoas em diversos aspectos, como saúde inteligente, casas inteligentes, cidades inteligentes, etc. Por outro lado, a segurança é frequentemente citada como um factor crítico que permite a adopção ou rejeição generalizada de qualquer nova tecnologia. A segurança no nível do dispositivo é um fator chave para a operação perfeita da IoT. O número de dispositivos conectados continua a aumentar geograficamente diariamente. Portanto, a segurança da IoT deve ser continuamente revista e revisitada em intervalos regulares para servir como uma medida proativa antes que os ataques aconteçam e para preparar melhores soluções futuras. Todos esses trabalhos correlatos foram selecionados com intuito de auxiliar no desenvolvimento do projeto de TCC, auxiliando na compreensão de elementos de cibersegurança, IoT, conexões entre dispositivos, tráfego de informações na rede e detecção de anomalias.

3. Materiais e métodos

A Tabela 2 apresenta as tecnologias e ferramentas que serão consideradas para o desenvolvimento deste projeto.

Tabela 2 - Materiais e métodos utilizados

Nome	Fonte	Descrição de uso
IEEE DataPort	https://ieee-dataport.org/	Obtenção do conjunto de dados que representa o tráfego de redes.
Google Colab	https://colab.google/	Python, para análise de dados do tráfego de redes e modelos de aprendizado de máquinas.
Scikit-learn, Tensor Flow, Keras	https://scikit-learn.org/ https://www.tensorflow.org/ https://keras.io/	Bibliotecas Python para treinar e implementar modelos de aprendizado de máquina.

Fonte: Os autores (2024).

Será realizada uma análise quantitativa de modelos de aprendizado de máquina para a detecção de anomalias em dispositivos IoT domésticos. Para isso, será concretizada uma pesquisa bibliográfica sobre os dados presentes na literatura. Após a pesquisa, serão selecionados alguns conjuntos de dados para estudo utilizando a linguagem de programação Python, que também será empregada na análise. A linguagem de programação Python será utilizada para o treinamento dos modelos de aprendizagem de máquina. Por fim, será conduzida uma análise quantitativa com base nos resultados obtidos nos testes com os modelos de aprendizagem.

4. Cronograma

A Tabela 3 demonstra o cronograma das atividades por integrante responsável e a Tabela 4 o cronograma por atividades previstas a serem executadas neste projeto.

Tabela 3 - Atividades por integrante

Atividade	Integrante	Mês 1	Mês 2	Mês 3	Mês 4	Mês 5	Mês 6	Mês 7	Mês 8	Mês 9
Pesquisa de dados	Gabriel	x	x							
	Jose	x	x							
	Caio	x	x							
Análise dos conjuntos de dados	Gabriel									
	Jose		x	x						
	Caio		x	x						
Análises dos tráfegos	Gabriel			x	x					
	Jose			x	x					
	Caio									
Seleção e	Gabriel					x	x	x		

treinamento dos modelos	Jose									
	Caio					x	x	x		
Quantificação dos modelos	Gabriel									
	Jose							x	x	x
	Caio							x	x	x

Tabela 4 - Cronograma previsto

Atividade	**Mês**								
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
Pesquisa de dados presentes na literatura	X								
Análises dos tipos de tráfegos normais e com anomalias			X	X					
Análise exploratória dos possíveis conjuntos de dados			X	X					
Seleção e treinamento de modelos de aprendizagem					X	X	X		
Quantificação dos modelos de aprendizagem utilizados							X	X	X

5. Resultados Esperados

A elaboração deste estudo auxiliará os demais técnicos da área da informática a saber quais modelos de aprendizado de máquina podem ser utilizados na implementação de segurança em redes dispositivos IoT, com enfoque na segurança em um contexto doméstico. O estudo irá possibilitar a identificação de características de conjuntos de dados presentes na literatura em relação ao tráfego de redes IoT domésticas, assim elaborando uma análise exploratória de dados sobre o tráfego definido. Também, possibilita a compreensão de diferentes tipos de tráfego de redes IoT, como tráfego normal e padrões de tráfego associados a ataques e anomalias na rede do usuário.

6. Referências

- ABRANET, Da Redação Da. Ataques a dispositivos da internet das coisas (IoT) crescem 41%. Abranet Associação Brasileira da Internet, 2023. Disponível em: https://www.abranet.org.br/Noticias/Ataques-a-dispositivos-da-internet-das-coisas-%28IoT%29-

crescem-41%25-4300.html?UserActiveTemplate=site#:~:text=O%20setor%20de%20educação%20e,em%20relação%20ao%20ano%20anterior.. Acesso em: 01 abr. 2024;

- BERLANDA, Rodrigo Grando. Guia de segurança da informação para a conectividade de dispositivos IoT. Repositório Institucional do Instituto Federal de Santa Catarina, 2021. Disponível em: https://repositorio.ifsc.edu.br/handle/123456789/2304. Acesso em: 01 abr. 2024;
- BOCHIE, Kaylani et al. Detecção de Ataques a Redes IoT Usando Técnicas de Aprendizado de Máquina e Aprendizado Profundo. In: SIMPÓSIO BRASILEIRO DE SEGURANÇA DA INFORMAÇÃO E DE SISTEMAS COMPUTACIONAIS (SBSEG), 20., 2020, Petrópolis. Anais [...]. Porto Alegre: Sociedade Brasileira de Computação, 2020. p. 257-270. DOI: https://doi.org/10.5753/sbseg.2020.19242. Acesso em: 01 abr. 2024;
- BREZOLIN, Uelinton Q. et al. Um Método para Detecção de Vulnerabilidades Através da Análise do Tráfego de Rede IoT. In: SIMPÓSIO BRASILEIRO DE REDES DE COMPUTADORES E SISTEMAS DISTRIBUÍDOS (SBRC), 40., 2022, Fortaleza. Anais [...]. Porto Alegre: Sociedade Brasileira de Computação, 2022. p. 447-460. ISSN 2177-9384. DOI: https://doi.org/10.5753/sbrc.2022.222343. Acesso em: 01 abr. 2024;
- BUTUN, Ismail; OSTERBERG, Patrik; SONG, Houbing. Security of the Internet of Things: vulnerabilities, attacks, and countermeasures. IEEE Communications Surveys & Tutorials, v. 22, n. 1, p. 616-644, 2020. IEEE. http://dx.doi.org/10.1109/comst.2019.2953364;
- COMPUGRAF. Ataques a dispositivos IoT aumentam em mais de 100% no primeiro semestre de 2021. Compugraf, 2021. Disponível em: https://www.compugraf.com.br/blog/ataques-a-dispositivos-iot-aumenta-em-mais-de-100-no-primeiro-semestre-de-2021/. Acesso em: 01 abr. 2024;
- MENEGHELLO, Francesca; CALORE, Matteo; ZUCCHETTO, Daniel; POLESE, Michele; ZANELLA, Andrea. IoT: internet of threats? a survey of practical security vulnerabilities in real iot devices. IEEE Internet Of Things Journal, v. 6, n. 5, p. 8182-8201, out. 2019. IEEE. http://dx.doi.org/10.1109/jiot.2019.2935189;
- MESSAS, Gabriel Esteves. Estudo Sobre a Segurança de Dispositivos Domésticos Conectados à Internet das Coisas. Universidade Estadual de Londrina, 2022. Disponível em: https://sites.uel.br/dc/wp-content/uploads/2022/09/TCC_GABRIEL_ESTEVES_MESSAS.pdf. Acesso em: 01 abr. 2024;
- MORAES, Yan Uehara de et al. Gerência de Autenticação de Dispositivos IoT Adaptativa Aos Ambientes Urbanos Apoiada em Políticas e Confiança Social. In: SIMPÓSIO BRASILEIRO DE REDES DE COMPUTADORES E SISTEMAS DISTRIBUÍDOS (SBRC), 40., 2022, Fortaleza. Anais [...]. Porto Alegre: Sociedade Brasileira de Computação, 2022. p. 84-97. ISSN 2177-9384. DOI: https://doi.org/10.5753/sbrc.2022.221966. Acesso em: 01 abr. 2024;

- OLIVEIRA, Felipe .Barreto. Framework para Detecção de Ataques dos em Dispositivos IoT, Utilizando Abordagens de Aprendizado de Máquinas. 2023. 67 f. Dissertação (Mestrado Profissional em Engenharia Elétrica) - Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 2023;
- OLIVEIRA, Nairobi Spiecker De et al. Segurança da Informação para Internet das Coisas (IoT): uma Abordagem sobre a Lei Geral de Proteção de Dados (LGPD). Revista Eletrônica de Iniciação Científica em Computação, v. 21, n. 1, 2019. Disponível em: https://seer.ufrgs.br/reic/article/view/88790. Acesso em: 01 abr. 2024;
- OMOLARA, Abiodun Esther et al. The internet of things security: A survey encompassing unexplored areas and new insights. ScienceDirect, 2022. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S0167404821003187. Acesso em: 01 abr. 2024;
- PACETE, Luiz Gustavo. IoT: até 2025, mais de 27 bilhões de dispositivos estarão conectados. Forbes, 2022. Disponível em: https://forbes.com.br/forbes-tech/2022/08/iot-ate-2025-mais-de-27-bilhoes-de-dispositivos-estarao-conectados/. Acesso em: 01 abr. 2024;
- SILVA FILHO, Jarélio Gomes da. Detecção de anomalias no tráfego MQTT de redes IOT utilizando técnicas de aprendizado de máquina. 2021. 66 f. Trabalho de Conclusão de Curso (Graduação em Ciência da Computação) - Centro de Ciências, Curso de Computação, Universidade Federal do Ceará, Fortaleza, 2021. Disponível em: http://repositorio.ufc.br/handle/riufc/58596. Acesso em: 01 abr. 2024;
- XENOFONTOS, Christos; ZOGRAFOPOULOS, Ioannis; KONSTANTINOU, Charalambos; JOLFAEI, Alireza; KHAN, Muhammad Khurram; CHOO, Kim-Kwang Raymond. Consumer, Commercial, and Industrial IoT (In)Security: attack taxonomy and case studies. IEEE Internet Of Things Journal, v. 9, n. 1, p. 199-221, jan. 2022. IEEE. http://dx.doi.org/10.1109/jiot.2021.3079916.