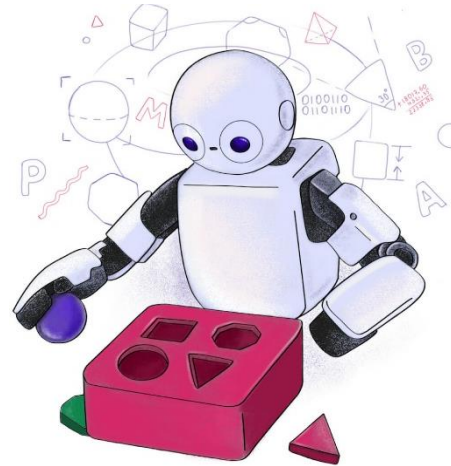


TP557 - Tópicos avançados em IoT e Machine Learning: *Detecção de anomalias*

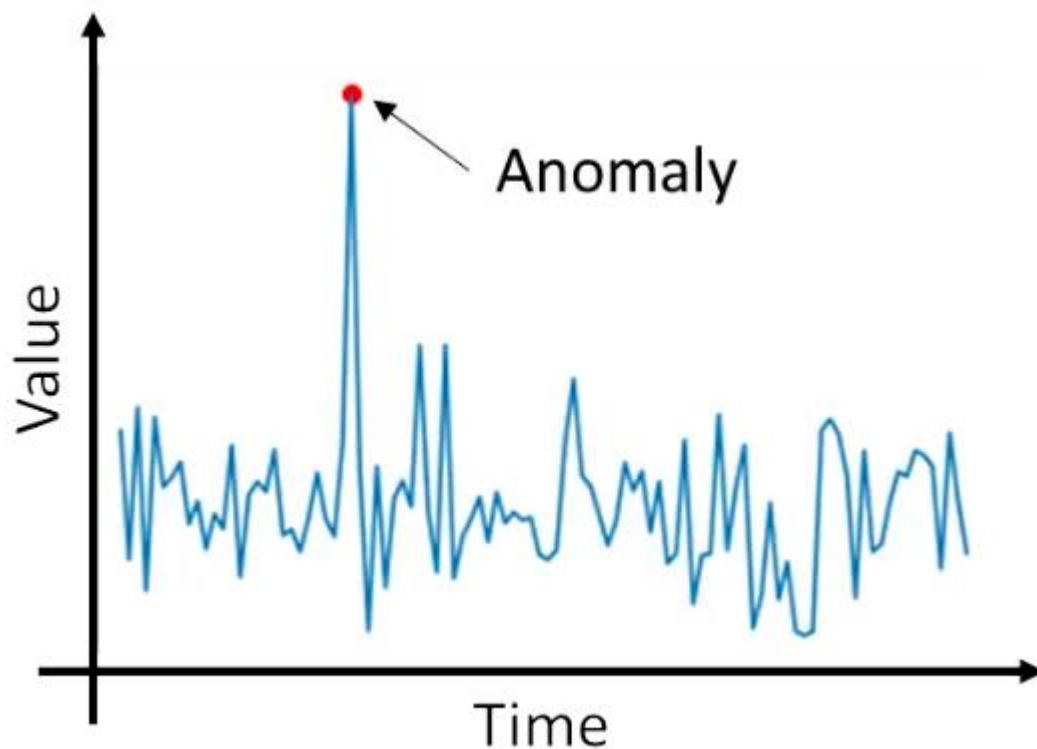


Inatel

Samuel Baraldi Mafra
samuelbmafra@inatel.br

Detecção de anomalias

- A detecção de anomalias examina pontos de dados específicos e detecta ocorrências raras que parecem suspeitas porque são diferentes do padrão de comportamento estabelecido













Detecção de anomalias

- Aplicações

Real world use cases of anomaly detection

Anomaly detection is influencing business decisions across verticals

TELECOM  Detect roaming abuse, revenue fraud, service disruptions	BANKING  Flag abnormally high purchases/deposits, detect cyber intrusions	FINANCE & INSURANCE  Detect and prevent out of pattern or fraudulent spend, travel expenses	HEALTHCARE  Detect fraud in claims and payments; events from RFID and mobiles	MANUFACTURING  Detect abnormal machine behavior to prevent cost overruns
TRANSPORTATION  Ensure external communications to the vehicle are not intrusion	SOCIAL MEDIA  Detect compromised accounts, bots that generate fake reviews	NETWORKING  Detect intrusion into networks, prevent theft of source code or IP	SMART HOUSE  Detect energy leakage, standardize smart sensor datasets	VIDEO SURVEILLANCE  Detect or track objects and persons of interest in monotonous footage

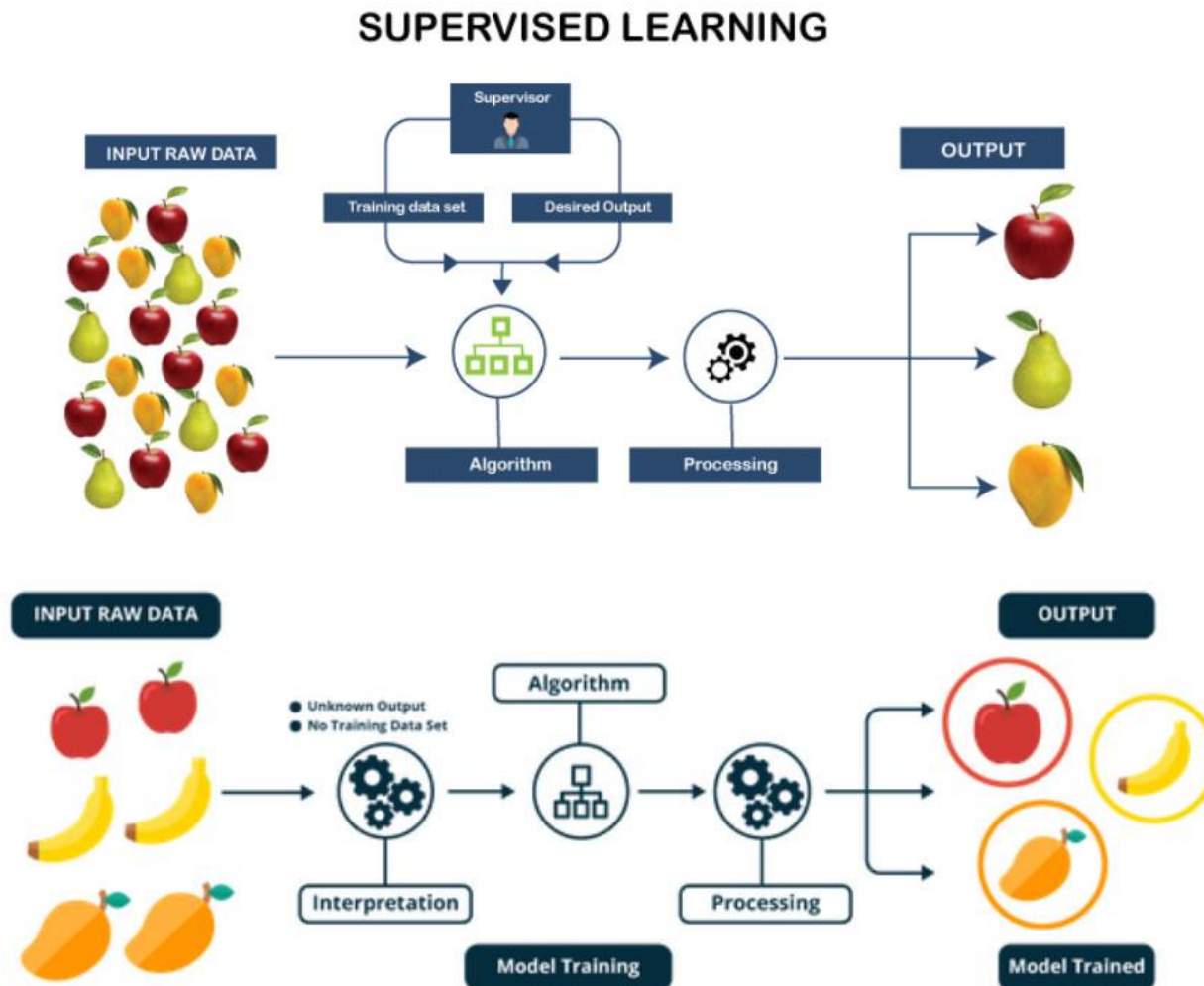
Detecção de anomalias

Aprendizado não supervisionado

- O aprendizado não supervisionado, também conhecido como aprendizado de máquina não supervisionado, usa algoritmos de aprendizado de máquina para analisar e agrupar conjuntos de dados não rotulados.
- Esses algoritmos descobrem padrões ocultos ou agrupamentos de dados sem a necessidade de intervenção humana.

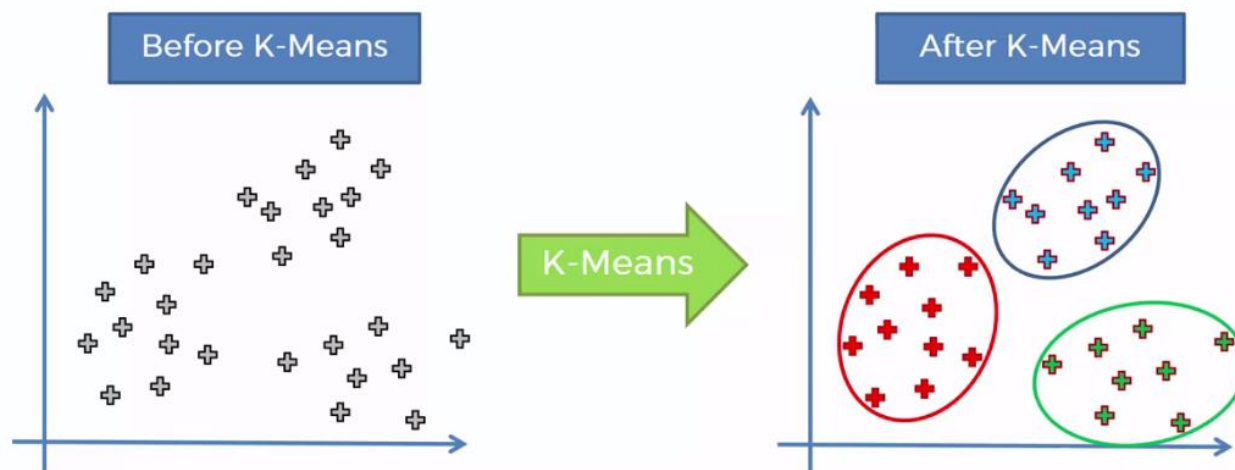
Detecção de anomalias

Aprendizado supervisionado versus não supervisionado



Detecção de anomalias

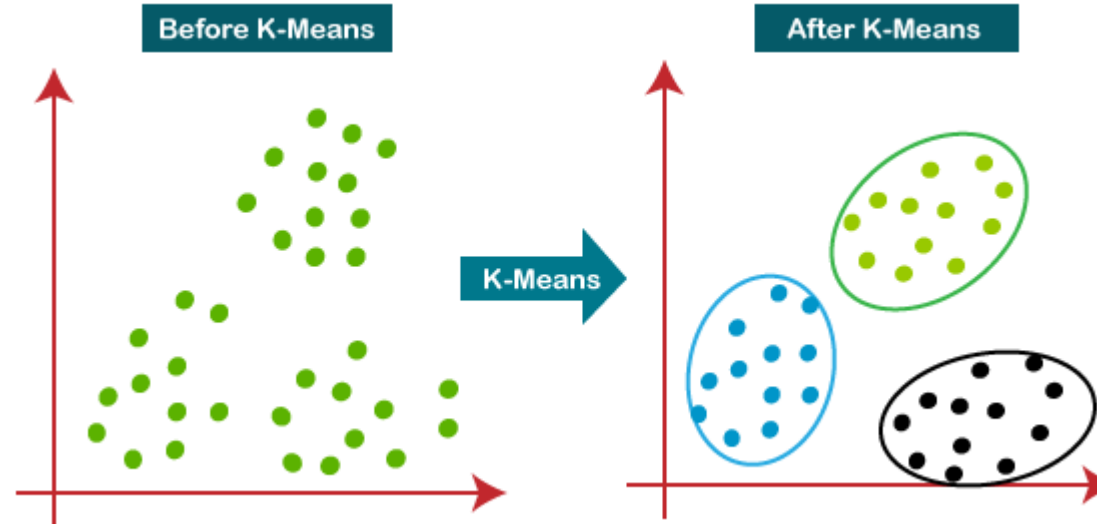
- O objetivo do agrupamento é dividir a população ou conjunto de pontos de dados em vários grupos, de modo que os pontos de dados dentro de cada grupo sejam mais comparáveis entre si e diferentes dos pontos de dados dentro dos outros grupos.
- É essencialmente um agrupamento de coisas com base em quão semelhantes e diferentes elas são entre si.



K-means

K-means clustering

- O objetivo do K-means é simples: agrupar pontos de dados semelhantes e descobrir padrões subjacentes.
- Para atingir este objetivo, o K-means procura um número fixo (k) de clusters em um conjunto de dados.

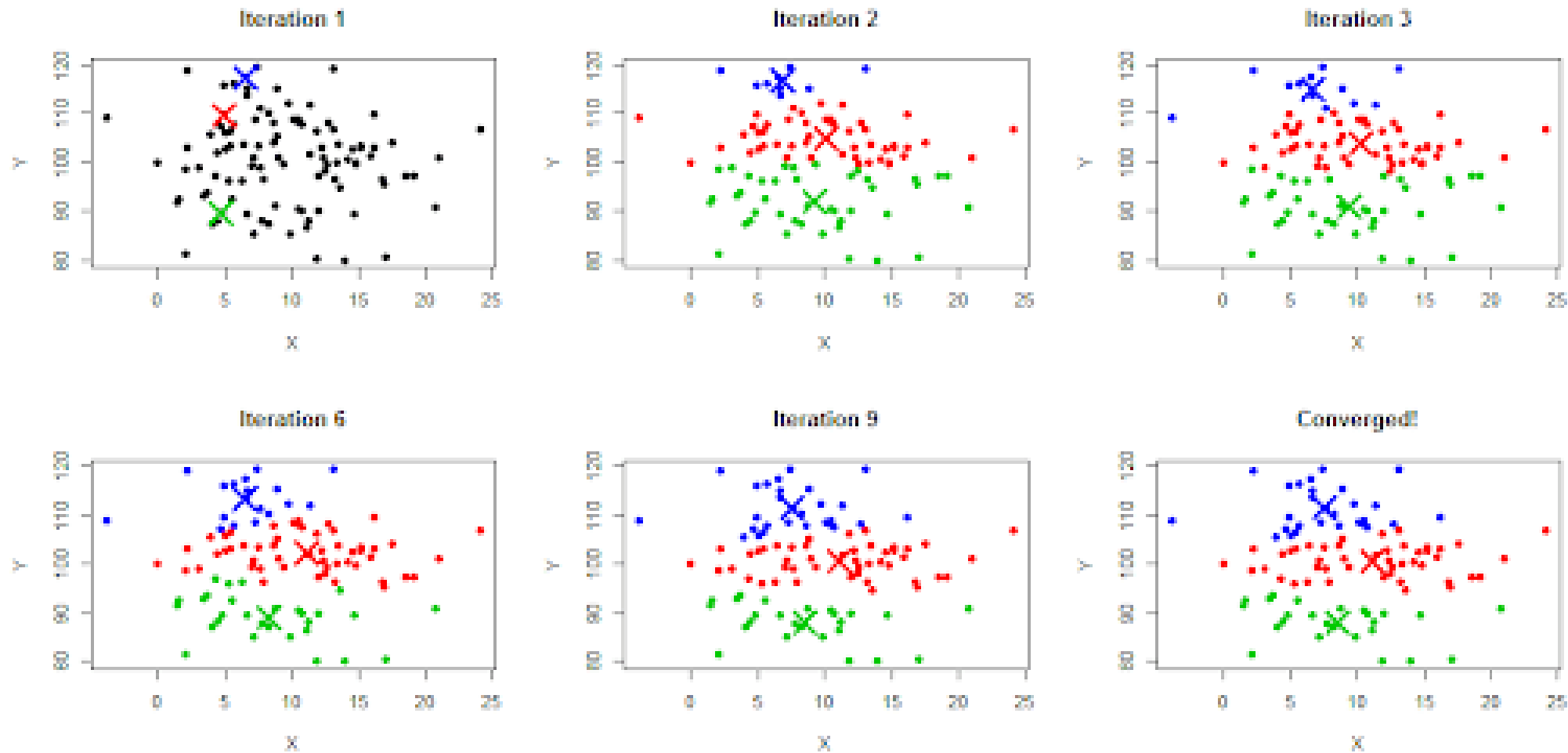


K-means

K-means clustering

- Primeiro, inicializamos aleatoriamente k pontos, chamados de médias ou centróides de cluster.
- Categorizamos cada item de acordo com sua média mais próxima e atualizamos as coordenadas da média, que são as médias dos itens categorizados naquele cluster até o momento.
- Repetimos o processo para um determinado número de iterações ou variação de posição dos clusters e ao final temos nossos clusters.

K-means



K-means

- Exemplo: Centros de distribuição



<https://medium.com/programadores-ajudando-programadores/k-means-o-que-%C3%A9-como-funciona-aplica%C3%A7%C3%B5es-e-exemplo-em-python-6021df6e2572>

K-means

- Exemplo: Centros de distribuição



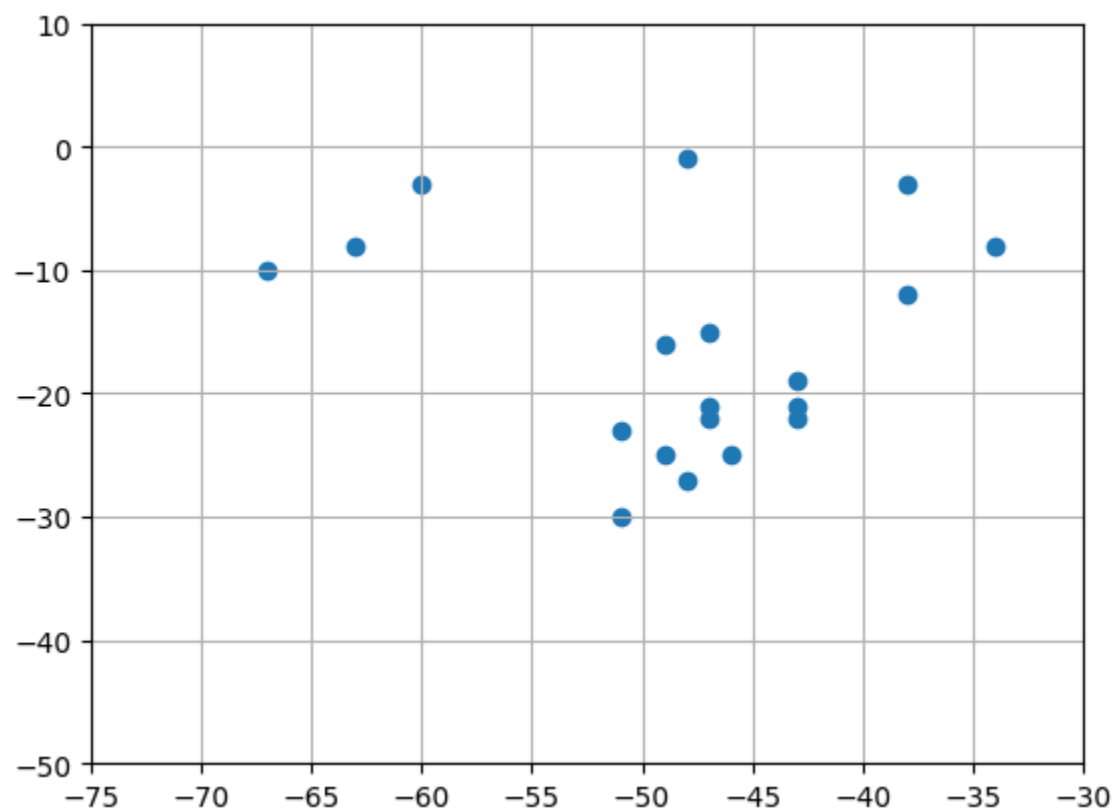
K-means

- Exemplo: Centros de distribuição

```
dataset = np.array(  
#matriz com as coordenadas geográficas de cada loja  
[[-25, -46], #são paulo  
 [-22, -43], #rio de janeiro  
 [-25, -49], #curitiba  
 [-30, -51], #porto alegre  
 [-19, -43], #belo horizonte  
 [-15, -47], #brasilia  
 [-12, -38], #salvador  
 [-8, -34], #recife  
 [-16, -49], #goiania  
 [-3, -60], #manaus  
 [-22, -47], #campinas  
 [-3, -38], #fortaleza  
 [-21, -47], #ribeirão preto  
 [-23, -51], #maringa  
 [-27, -48], #florianópolis  
 [-21, -43], #juiz de fora  
 [-1, -48], #belém  
 [-10, -67], #rio branco  
 [-8, -63] #porto velho])
```

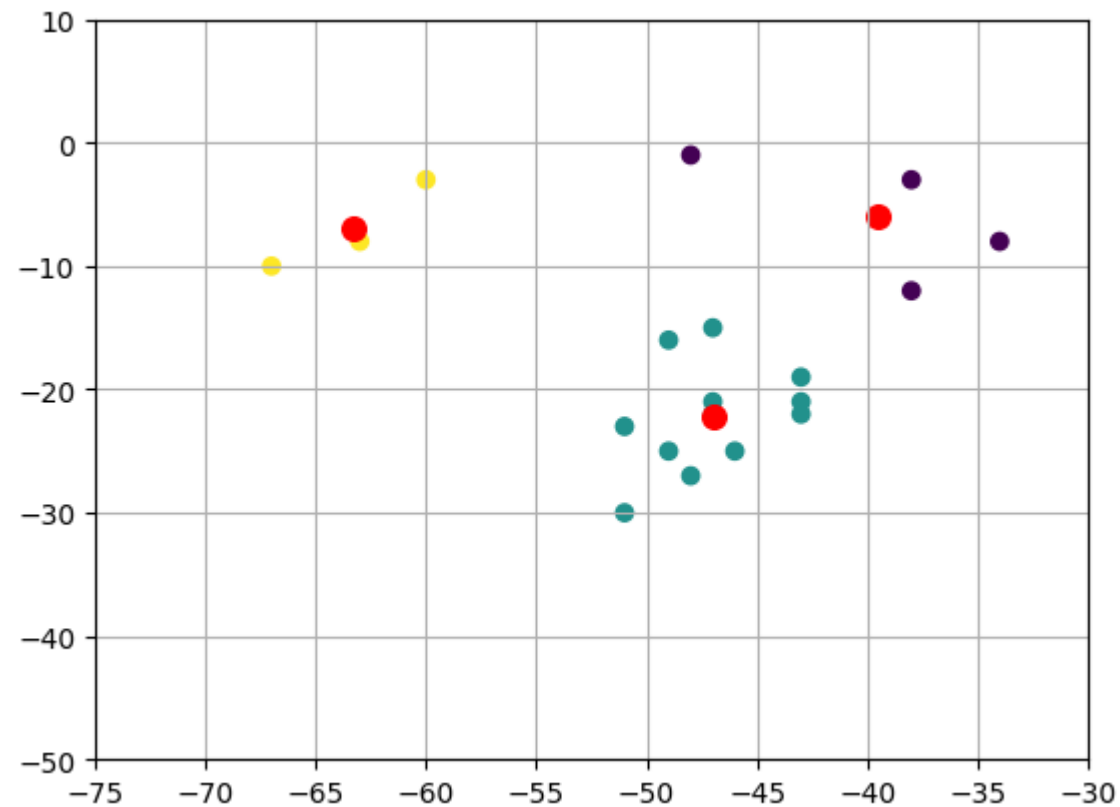
K-means

- Exemplo: Centros de distribuição



K-means

- Exemplo: Centros de distribuição



K-means

- Exemplo: Centros de distribuição

- [-7, -63.33333333] — Humaitá/AM
- [-6, -39.5] — Acopiara/CE
- [-22.16666667, -47] — Mogi Guaçu/SP

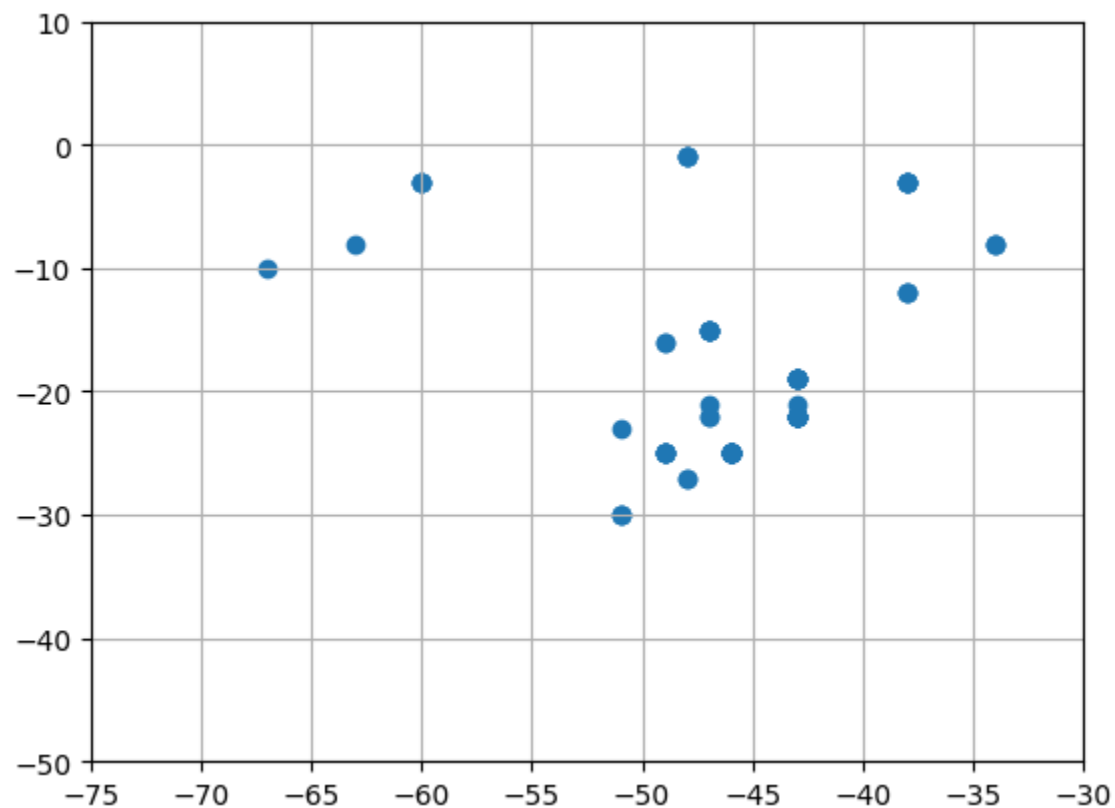
K-means

- Exemplo: Centros de distribuição

Considerar a adição de mais lojas: sendo 21 só em São Paulo.

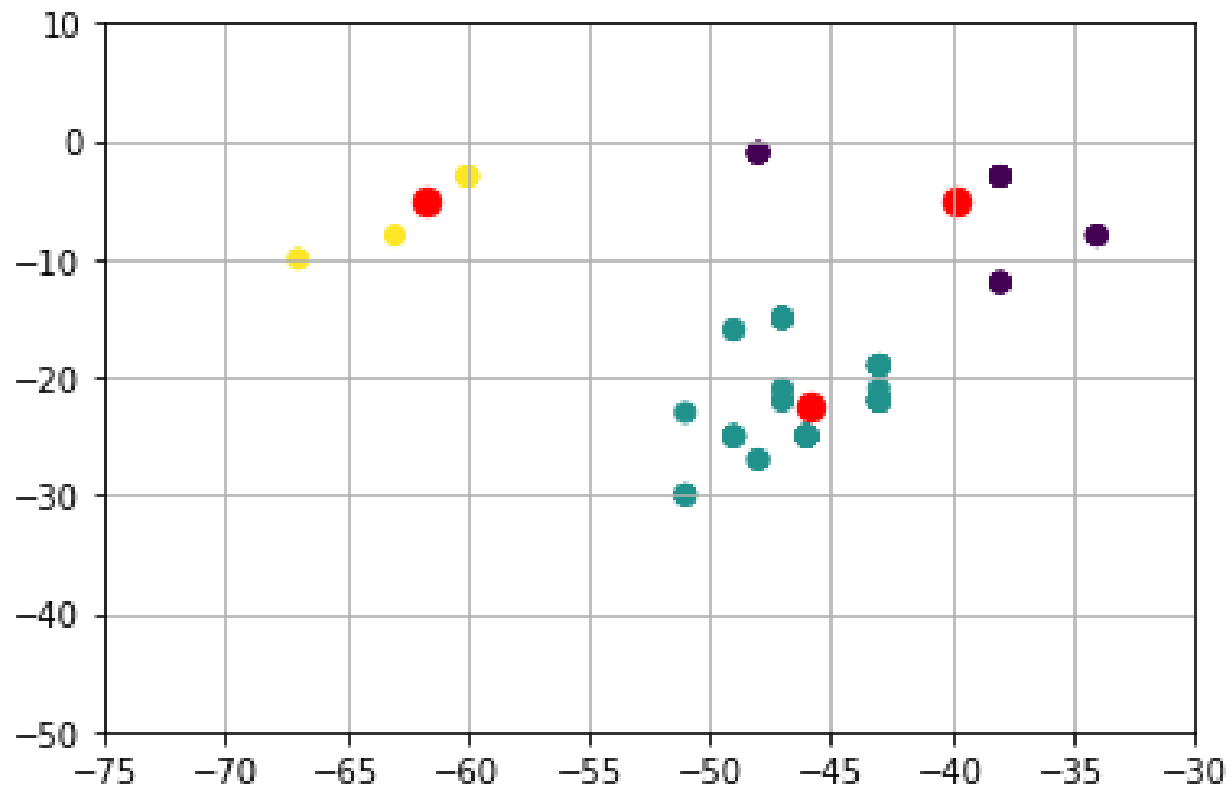
K-means

- Exemplo: Centros de distribuição



K-means

- Exemplo: Centros de distribuição



K-means

- Exemplo: Centros de distribuição

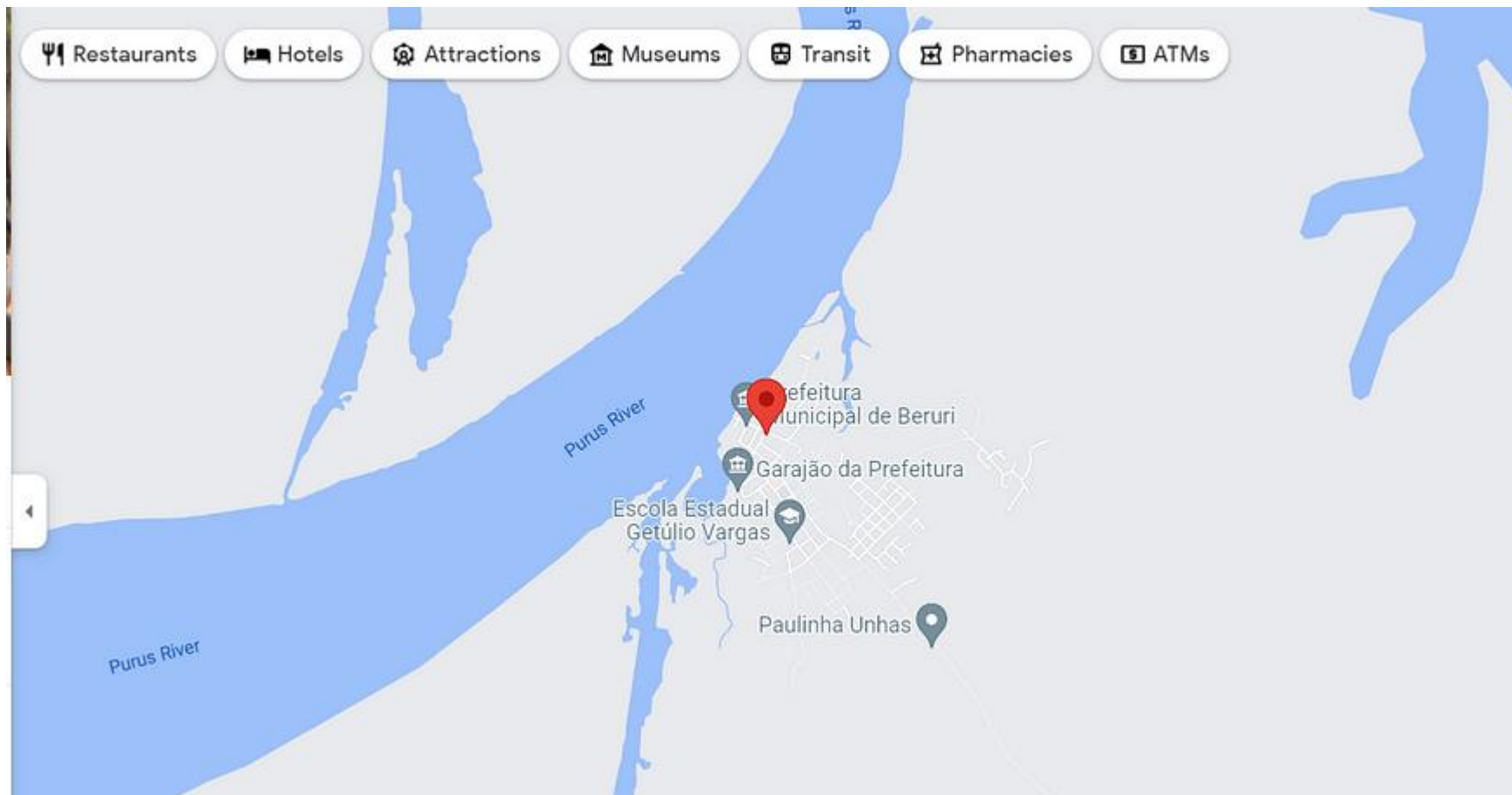
1. [-5, -61.66666667] — Beruri/AM

2. [-5.125, -39.75] — Boa Viagem/CE

3. [-22.55384615, -45.90769231] — Consolação/MG

K-means

- Exemplo: Centros de distribuição



K-means

Dados de meios de transporte:

- Rodovias
- Ferrovias
- Aeroportos
- Rios navegáveis
- Portos

K-means

Dados de meios de transporte:

- Custo de frete;
- Quantidade de empresas transportadoras;
- Índice de sinistros (roubos de carga e acidentes).

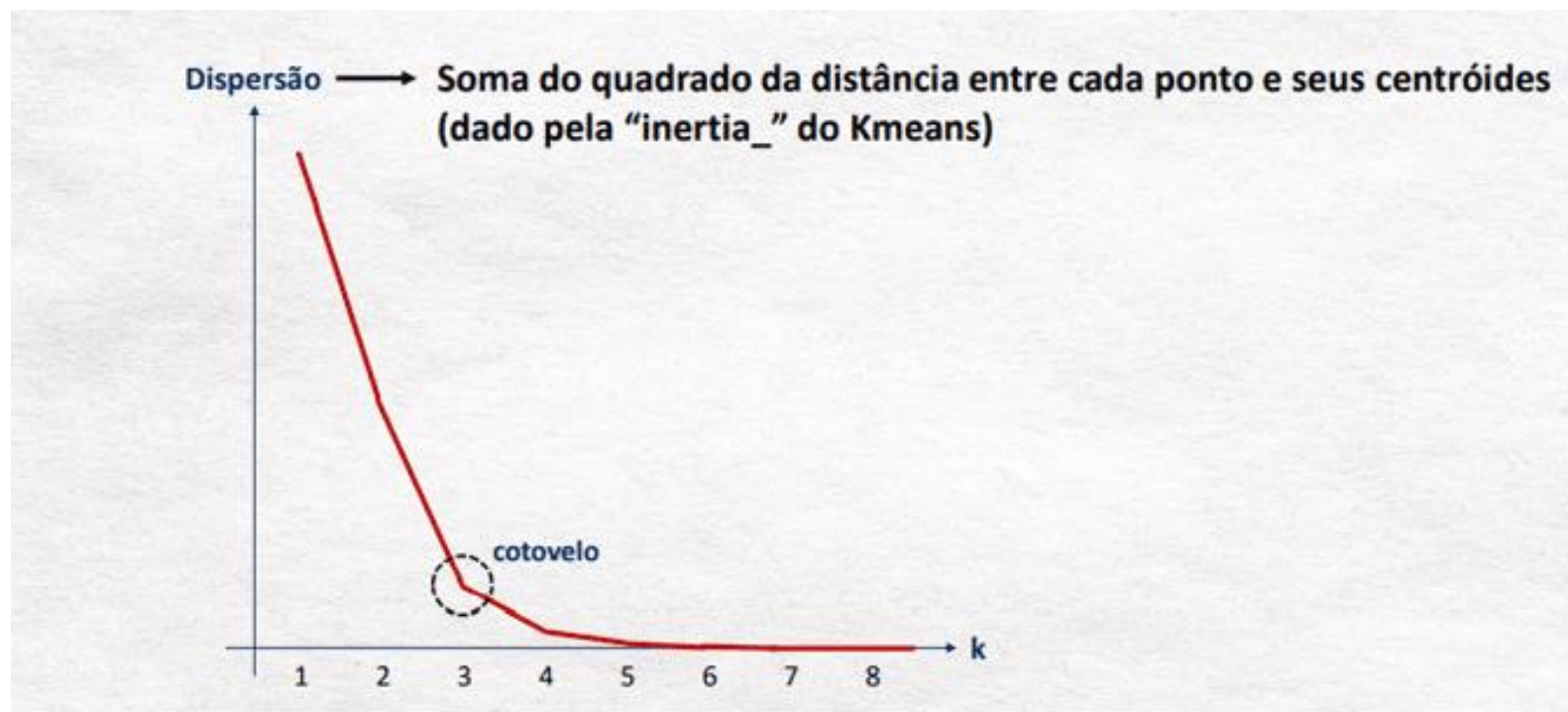
K-means

Dados de meios de transporte:

- Oferta e custo de mão de obra;
- Oferta e custo de mão de obra “qualificada” (técnicos, engenheiros, gerentes, executivos);
- Tributos municipais e estaduais;
- Localização dos fornecedores
- Preços de aluguel de galpões

K-means

K ótimo



$$WSS = \sum_{i=1}^{N_c} \sum_{x \in C_i} d(x, \bar{x}_{C_i})^2$$

Detecção de anomalias

Outliers

- Os dados de treinamento contêm valores discrepantes que são definidos como observações distantes das demais.
- Os estimadores de detecção de outliers tentam, portanto, ajustar as regiões onde os dados de treinamento estão mais concentrados, ignorando as observações desviantes.

Novelty

- Os dados de treinamento não são poluídos por valores discrepantes e estamos interessados em detectar se uma **nova** observação é um valor discrepante.
- Neste contexto, um outlier também é chamado de novidade

Detecção de anomalias

ML-based Novelty Detection and Classification of Security Threats in IoT Networks

Marcelo V. C. Aragão, Gabriel P. Ambrósio, Felipe A. P. de Figueiredo



Detecção de anomalias

Ameaças à segurança em redes IoT

- Aumento rápido de dispositivos conectados;
- Troca intensa de dados sensíveis através de redes;
- Disponibilidade de conjuntos de dados de tráfego de rede do mundo real.

Detecção e classificação de novidades baseadas em ML

- Análise Automatizada de Tráfego de Rede (NTA);
- Detecção: identifique ameaças nunca antes vistas;
- Classificação: categoriza vestígios de ameaças conhecidas.

Detecção de anomalias

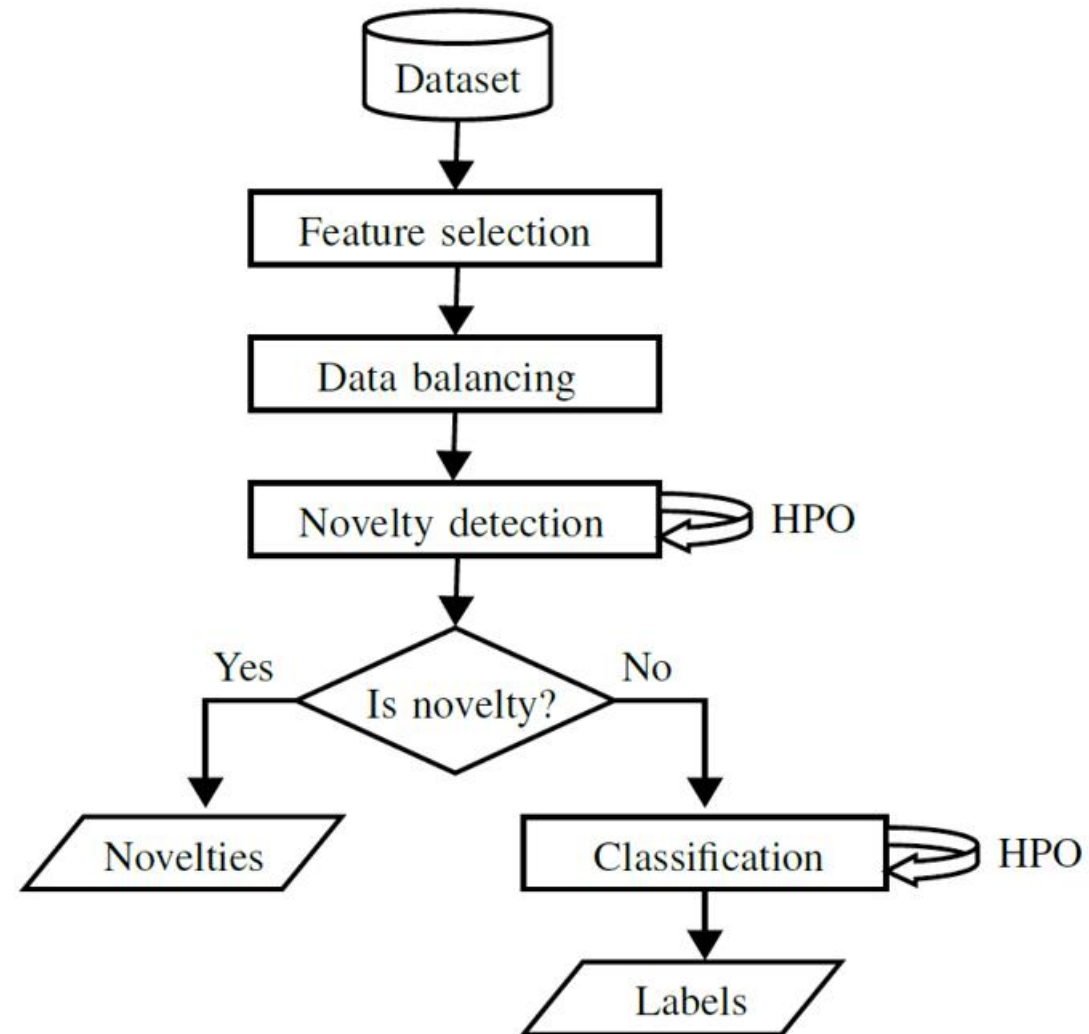
IoT Network Intrusion:

10% of $\approx 3\text{M}$ samples

- Mirai,
- Man-in-the-middle,
- DoS,
- Scanning

<https://ieee-dataport.org/open-access/iot-network-intrusion-dataset>

Detecção de anomalias



Detecção de anomalias

TABLE I: Novelty detection accuracy.

Scenario	Elliptic Envelope		Isolation Forest		Local Outlier Factor		SGD One-Class SVM	
	Mean \pm SD	Max	Mean \pm SD	Max	Mean \pm SD	Max	Mean \pm SD	Max
DoS	0.557 \pm 0.494	1.000	0.594 \pm 0.465	1.000	0.109 \pm 0.105	0.263	0.620 \pm 0.485	1.000
Mirai	0.747 \pm 0.293	0.991	0.913 \pm 0.087	0.993	0.414 \pm 0.128	0.574	0.650 \pm 0.477	1.000
MITM	0.391 \pm 0.395	1.000	0.074 \pm 0.093	0.474	0.208 \pm 0.119	0.330	0.740 \pm 0.439	1.000
Scan	0.537 \pm 0.466	1.000	0.828 \pm 0.238	0.949	0.601 \pm 0.311	0.894	0.595 \pm 0.491	1.000

Detecção de anomalias

TABLE III: Classification accuracy.

Scenario	Decision Tree		LightGBM		Random Forest		XGBoost	
	Mean \pm SD	Max	Mean \pm SD	Max	Mean \pm SD	Max	Mean \pm SD	Max
DoS	0.875 \pm 0.141	0.969	0.765 \pm 0.241	0.954	0.917 \pm 0.054	0.957	0.947 \pm 0.008	0.957
Mirai	0.851 \pm 0.162	0.969	0.781 \pm 0.243	0.953	0.917 \pm 0.057	0.958	0.948 \pm 0.008	0.957
MITM	0.864 \pm 0.152	0.967	0.798 \pm 0.213	0.953	0.916 \pm 0.060	0.959	0.947 \pm 0.008	0.956
Scan	0.865 \pm 0.154	0.966	0.776 \pm 0.242	0.953	0.916 \pm 0.057	0.957	0.947 \pm 0.008	0.955

Detecção de anomalias

- Movimentação de containers ao longo do ciclo logístico



Detecção de anomalias

- Movimentação de containers ao longo do ciclo logístico

Classificação de 5 estados do container

- Parado
- Sendo erguido
- No mar
- No caminhão
- **Anomalia** (ex. container caindo no mar, empilhadeira tombando)

Detecção de anomalias

Trabalho:

Incluir e analisar no edge impulse possíveis anomalias nos dados da movimentação da cadeira de rodas pela cabeça.

Acompanhamento do trabalho final