K-Medoids Clustering for Data Selection and its Impact on Neural Network Robustness

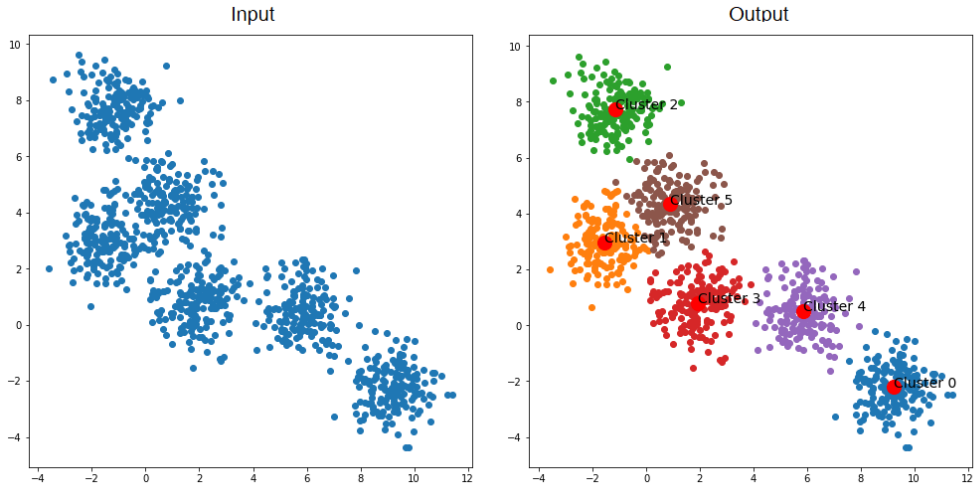
Nina Bryan
Howard University
Department of Mathematics
Georgia Tech Research Institute
ASID

February 27, 2026

What is a Clustering Algorithm?

- an unsupervised machine learning task that involves discovering the natural grouping of data
- Unlike supervised learning (like predictive modeling), clustering algorithms only interpret the input data and find natural groups or clusters in feature space

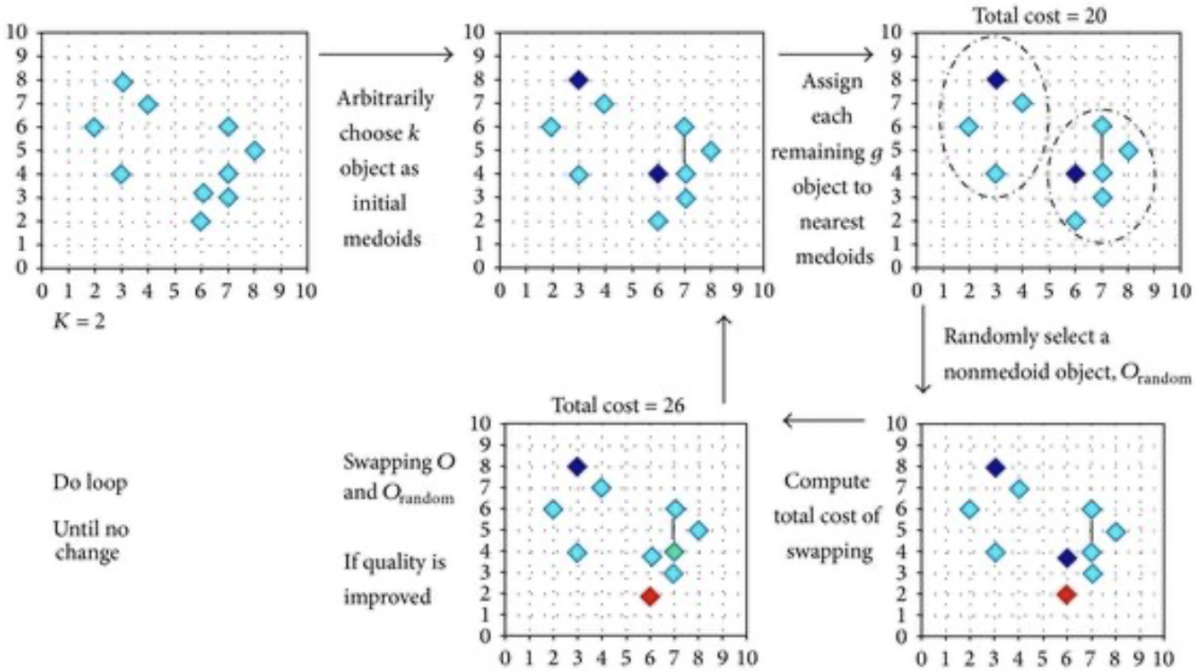
A cluster is often an area of density in the feature space where examples from the domain (observations or rows of data) are closer to the cluster than other clusters. The cluster may have a center (**centroid**) that is a sample or a point feature space and may have a boundary or extent. [1]



K-Medoids

K-Medoids differs from other partitioning-based clustering algorithms in the way it selects the clusters' centers.

- always picks an actual data point from the cluster as their center, while other algorithms, like K-Means, selects the average of a cluster's points as its center (which may or may not be one of the data points) [5]



[2]

Data

Objective: to increase neural network robustness by selecting 100 samples closest to each centroid

Mimicus Dataset

- Training Set: 32K Samples, Testing Set: 10K Samples
- Classifications/Labels: 2 $\rightarrow$ Benign (0), Malicious (1)
- # of Features: 135

Principal Component Analysis is a method that is often used to **reduce** the dimensionality of large data sets, by transforming a large set of variables into a smaller one that still contains most of the information in the original data set (usually at the expense of accuracy). [3]

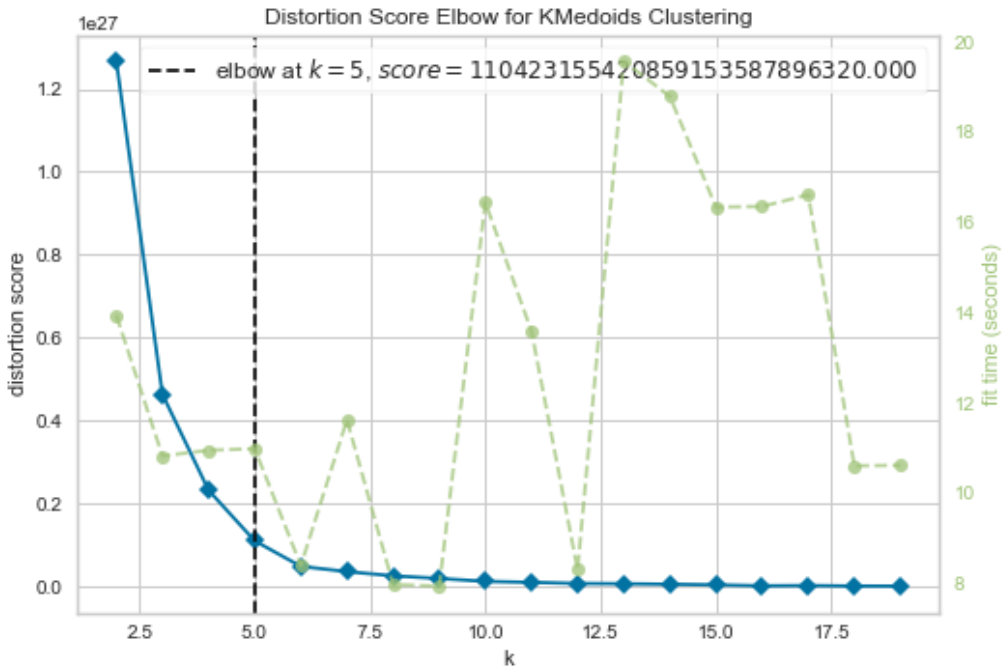
	sepal length (cm)	sepal width (cm)	petal length (cm)	petal width (cm)
0	5.1	3.5	1.4	0.2
1	4.9	3.0	1.4	0.2
2	4.7	3.2	1.3	0.2
3	4.6	3.1	1.5	0.2
4	5.0	3.6	1.4	0.2

	principal component 1	principal component 2	principal component 3
0	1.823288	-0.104530	0.501130
1	-1.295968	-0.350770	0.461567
2	-0.219921	-0.041491	0.512261
3	0.724683	0.274496	0.272093
4	-0.271082	0.608131	0.374939

Optimal Number of Clusters

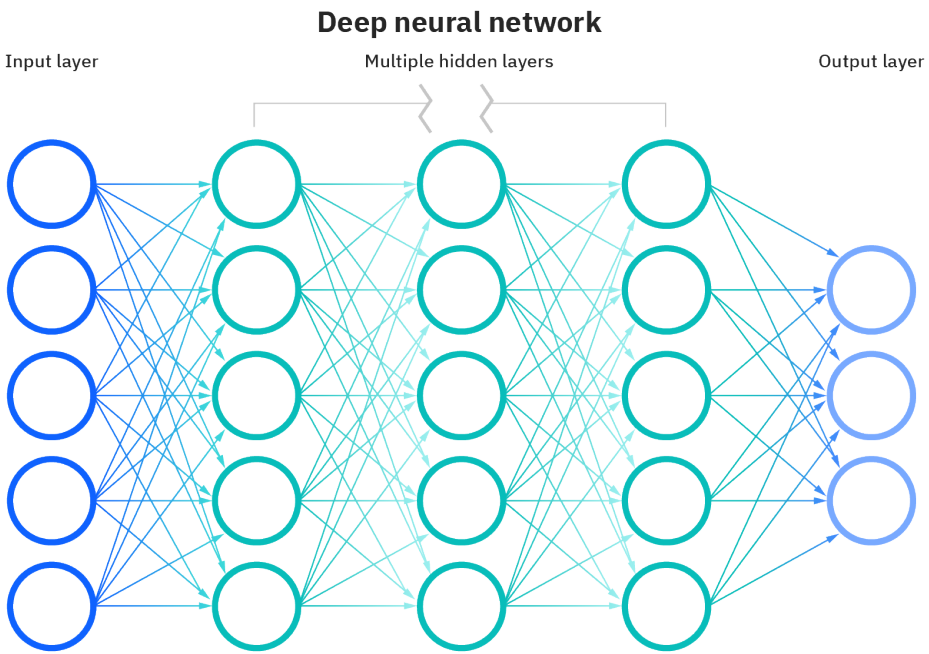
Determining the number of clusters in a dataset is dependent on the method used for measuring similarities (Euclidean, L1 distance, Chebyshev, etc.) and parameters used for partitioning.

- Gap Statistic: 2
- Elbow Method: 5
- Silhouette Coefficient: 2
- Calinski-Harabasz Index: 2
- Davies-Bouldin Index: 2



Build Neural Network

A simplified version of Deep Neural Network is represented as a hierarchical (layered) organization of neurons (similar to the neurons in the brain) with connections to other neurons.
Each layer can have one or many neurons and each of them will compute a small function i.e. **activation function**. The activation function mimics the signal to pass to the next connected neurons. [4]



Activation function	Equation	Example	1D Graph
Unit step (Heaviside)	$\phi(z) = \begin{cases} 0, & z < 0, \\ 0.5, & z = 0, \\ 1, & z > 0, \end{cases}$	Perceptron variant	
Sign (Signum)	$\phi(z) = \begin{cases} -1, & z < 0, \\ 0, & z = 0, \\ 1, & z > 0, \end{cases}$	Perceptron variant	
Linear	$\phi(z) = z$	Adaline, linear regression	
Piece-wise linear	$\phi(z) = \begin{cases} 1, & z \geq \frac{1}{2}, \\ z + \frac{1}{2}, & -\frac{1}{2} < z < \frac{1}{2}, \\ 0, & z \leq -\frac{1}{2}, \end{cases}$	Support vector machine	
Logistic (sigmoid)	$\phi(z) = \frac{1}{1 + e^{-z}}$	Logistic regression, Multi-layer NN	
Hyperbolic tangent	$\phi(z) = \frac{e^{z} - e^{-z}}{e^{z} + e^{-z}}$	Multi-layer Neural Networks	
Rectifier, ReLU (Rectified Linear Unit)	$\phi(z) = max(0, z)$	Multi-layer Neural Networks	
Rectifier, softplus	$\phi(z) = \ln(1 + e^{z})$	Multi-layer Neural Networks	

Neural Network Robustness

Robustness refers to the model's effectiveness at detecting "attack" samples. **alpha-beta-Crown verifier** is a neural network verifier based on a efficient bound propagation algorithm and bound and branch.

	verified accuracy			
Trial #	Full Data Baseline	Half Data Baseline	5 Clusters	2 Clusters
1	78.0%	69.0%	74.0%	76.0%
2	79.0%	70.0%	75.0%	76.0%
3	71.0%	69.0%	79.0%	73.0%
4	75.0%	74.0%	77.0%	78.0%
5	74.0%	73.0%	72.0%	75.0%
average	75.4%	71.0%	75.4%	75.6%

	attack success rate			
Trial #	Full Data Baseline	Half Data Baseline	5 Clusters	2 Clusters
1	3.0%	9.0%	3.0%	3.0%
2	3.0%	8.0%	5.0%	5.0%
3	8.0%	8.0%	3.0%	5.0%
4	6.0%	8.0%	4.0%	4.0%
5	5.0%	7.0%	6.0%	2.0%
average	5.0%	8.0%	4.2%	3.8%

2-Sample T Test ($\alpha = 0.05$)

$\mu_2 < \mu_3$ significant ✓ (p-value $= 0.012$)	$\mu_2 > \mu_3$ significant ✓ (p-value $= 5.58\text{x}10^{-4}$)
$\mu_2 < \mu_4$ significant ✓ (p-value $= 0.004$)	$\mu_2 > \mu_4$ significant ✓ (p-value $= 3.26\text{x}10^{-4}$)
$\mu_1 \neq \mu_3$ significant **X** Accept H_o: $\mu_1 = \mu_3$	$\mu_1 \neq \mu_3$ significant **X** Accept H_o: $\mu_1 = \mu_3$
$\mu_1 \neq \mu_4$ significant **X** Accept H_o: $\mu_1 = \mu_4$	$\mu_1 \neq \mu_4$ significant **X** Accept H_o: $\mu_1 = \mu_4$

Conclusion (1): Both clustering selection options produced a model with a higher verified accuracy and lower attack success rate than a model trained with training set **A** baseline.

Future Changes/ Additions

- Optimize number of samples closest to the centroid
- Use different initializing methods ('random', 'heuristic', 'build')
- Explore other clustering algorithms

Other Applications

- Market and Customer Segmentation
- Search Result Clustering
- Spam Filter
- Document Analysis
- Fantasy Football
- Image Clustering

References I

Jason Brownlee. *10 Clustering Algorithms With Python*. en-US. Apr. 2020. URL: https://machinelearningmastery.com/clustering-algorithms-with-python/ (visited on 07/20/2022).

Jaewon Choi. *k -medoids clustering*. en. URL: https://www.researchgate.net/figure/k-medoids-clustering_fig4_282897075 (visited on 07/20/2022).

Zakaria Jaadi. *A Step-by-Step Explanation of Principal Component Analysis (PCA) — Built In*. en. URL: https://builtin.com/data-science/step-step-explanation-principal-component-analysis (visited on 07/20/2022).

Jojo John Moolayil. *A Layman's Guide to Deep Neural Networks*. en. May 2020. URL: https://towardsdatascience.com/a-laymans-guide-to-deep-neural-networks-ddcea24847fb (visited on 07/20/2022).

References II

Nikita Shiledarbaxi. *Comprehensive Guide To K-Medoids Clustering Algorithm*. en-US. Apr. 2021. URL: https://analyticsindiamag.com/comprehensive-guide-to-k-medoids-clustering-algorithm/ (visited on 07/20/2022).