Professional Certificate in AI for Military Defense

Machine Learning Algorithms

Ablation Study refers to the process of removing or disabling certain components or features of a machine learning model to understand their contribution to the overall performance of the model. This technique is used to identify the most important features or components of a model and to simplify the model by removing unnecessary elements. Ablation studies are commonly used in machine learning to analyze the effectiveness of different components, such as layers or neurons, in a neural network.

Activation Function is a mathematical function that is used to introduce non-linearity into a machine learning model. The activation function is applied to the output of a layer or a neuron to determine the output of that layer or neuron. Common examples of activation functions include the sigmoid function, the tanh function, and the ReLU function. The choice of activation function depends on the specific problem being solved and the type of model being used.

Adversarial Attack refers to a type of cyberattack that is designed to mislead or deceive a machine learning model. Adversarial attacks involve modifying the input data to a model in such a way that the model produces an incorrect output. Adversarial attacks can be used to compromise the security of machine learning models and to undermine their performance.

Backpropagation is an algorithm that is used to train machine learning models, particularly neural networks. Backpropagation involves computing the gradient of the loss function with respect to the model's parameters and using this gradient to update the parameters. Backpropagation is a key component of many machine learning algorithms and is used to optimize the performance of models.

Batch Normalization! is a technique that is used to normalize the input data to a layer or a neuron in a neural network. Batch normalization involves scaling and shifting the input data to have a mean of zero and a standard deviation of one. Batch normalization is used to improve the stability and speed of training machine learning models.

Bias-Variance Tradeoff refers to the tradeoff between the bias and variance of a machine learning model. The bias of a model refers to the difference between the model's predictions and the true values, while the variance refers to the amount of variation in the model's predictions. A model with high bias will tend to produce predictions that are far from the true values, while a model with high variance will tend to produce predictions that are highly variable.

Boosting is an ensemble learning technique that involves combining multiple machine learning models to produce a single, more accurate model. Boosting involves training a sequence of models, with each model attempting to correct the errors of the previous model. Boosting is commonly used to improve the accuracy of machine learning models.

Classification is a type of machine learning problem that involves predicting a categorical label or class that

an instance belongs to. Classification problems are commonly solved using machine learning algorithms such as logistic regression, decision trees, and support vector machines.

Clustering is a type of unsupervised machine learning problem that involves grouping similar instances together into clusters. Clustering algorithms are commonly used to identify patterns or structure in data.

Convolutional Neural Network (CNN) is a type of neural network that is commonly used for image and video processing tasks. CNNs involve the use of convolutional layers, which apply filters to small regions of the input data, and pooling layers, which reduce the spatial dimensions of the data.

Data Augmentation is a technique that is used to increase the size of a dataset by applying random transformations to the existing data. Data augmentation is commonly used to improve the robustness of machine learning models to different types of variations in the data.

Data Preprocessing is the process of cleaning and transforming raw data into a format that is suitable for use in machine learning algorithms. Data preprocessing involves tasks such as handling missing values, normalizing data, and encoding categorical variables.

Decision Tree is a type of machine learning model that involves using a tree-like structure to classify instances or make predictions. Decision trees are commonly used for classification and regression tasks.

Deep Learning is a subfield of machine learning that involves the use of neural networks with multiple layers to learn complex representations of data. Deep learning algorithms are commonly used for tasks such as image and speech recognition.

Dimensionality Reduction is a technique that is used to reduce the number of features or dimensions in a dataset. Dimensionality reduction is commonly used to improve the efficiency and accuracy of machine learning models.

Dropout is a regularization technique that is used to prevent overfitting in neural networks. Dropout involves randomly dropping out or disabling neurons during training to prevent the model from becoming too complex.

Ensemble Learning is a technique that involves combining multiple machine learning models to produce a single, more accurate model. Ensemble learning algorithms are commonly used to improve the accuracy and robustness of machine learning models.

Error Analysis is the process of analyzing and understanding the errors made by a machine learning model. Error analysis involves identifying the types of errors that are being made and developing strategies to improve the model's performance.

Feature Engineering is the process of selecting and transforming raw data into features that are suitable for use in machine learning algorithms. Feature engineering involves tasks such as extracting relevant features from data and encoding categorical variables.

Feature Extraction is the process of extracting relevant features from data. Feature extraction involves using

techniques such as principal component analysis and autoencoders to extract features from data.

Feature Selection is the process of selecting the most relevant features from a dataset. Feature selection involves using techniques such as correlation analysis and mutual information to select the most relevant features.

Gradient Boosting is an ensemble learning technique that involves combining multiple machine learning models to produce a single, more accurate model. Gradient boosting involves training a sequence of models, with each model attempting to correct the errors of the previous model.

Gradient Descent is an optimization algorithm that is used to train machine learning models. Gradient descent involves computing the gradient of the loss function with respect to the model's parameters and using this gradient to update the parameters.

Hyperparameter Tuning is the process of tuning the hyperparameters of a machine learning model to optimize its performance. Hyperparameter tuning involves using techniques such as grid search and random search to find the optimal values of the hyperparameters.

Image Processing is the process of manipulating and analyzing images using machine learning algorithms. Image processing involves tasks such as image classification, object detection, and image segmentation.

K-Means Clustering is a type of unsupervised machine learning algorithm that involves grouping similar instances together into clusters. K-means clustering involves using a centroid based approach to assign instances to clusters.

K-Nearest Neighbors (KNN) is a type of machine learning algorithm that involves predicting the label of an instance based on the labels of its nearest neighbors. KNN is commonly used for classification and regression tasks.

Linear Regression is a type of machine learning algorithm that involves predicting a continuous output variable based on one or more input features. Linear regression involves using a linear equation to model the relationship between the input features and the output variable.

Logistic Regression is a type of machine learning algorithm that involves predicting a binary output variable based on one or more input features. Logistic regression involves using a logistic function to model the