Model training and evaluation

MODULE

Chuan Yue - February 19, 2019

Description

Upon completion of this lab, students should be able to:

Create data structures to contain the feature vectors and label lists.

Assessed by the tasks and outputs specified in STEP 1.

Construct the training and testing datasets by splitting the entire dataset.

Assessed by the tasks and outputs specified in STEP 2.

Create machine learning models with training and hyper-parameters tuning for performing input inference attacks.

Assessed by the tasks and outputs specified in STEP 3.

Evaluate the accuracy of machine learning models based on the test data.

Assessed by the tasks and outputs specified in STEP 4.

Compare different machine learning models and their accuracy.

Assessed by the tasks and outputs specified in STEP 5.

Analyze the impact of different features and datasets on model accuracy.

Assessed by the tasks and outputs specified in STEPs 6 and 7.

Create machine learning models with training, hyper-parameters tuning, and evaluation for performing user fingerprinting attacks.

Assessed by the tasks and outputs specified in STEP 8.

Outcomes

evaluate and synthesize

Students will be able to construct the training and testing datasets by splitting the entire dataset.

evaluate and synthesize

Students will be able to evaluate the accuracy of machine learning models based on the test data.

evaluate and synthesize

Students will be able to create data structures to contain the feature vectors and label lists.

evaluate and synthesize

Students will be able to create machine learning models with training, hyper-parameters tuning, and evaluation for performing user fingerprinting attacks.

apply and analyze

Students will be able to compare different machine learning models and their accuracy.

apply and analyze

Students will be able to analyze the impact of different features and datasets on model accuracy.

evaluate and synthesize

Students will be able to create machine learning models with training and hyper-parameters tuning for performing input inference attacks.

Content

Notes

Note that the solution manual and the solution materials are not uploaded to this platform based on the suggestion from Kaza, Siddharth (SKaza@towson.edu).

Please contact Dr. Chuan Yue (chuanyue@mines.edu) at the Colorado School of Mines for the solution manual and the solution materials.

The development of this module is sponsored by the NSA grant H98230-17-1-0403.