Machine Learning for Cybersecurity: Labs

Length	Unit
Collection	NSA NCCP
Updated	March 14, 2020
Contributors	Ricardo Calix
Academic Levels	Undergraduate, Graduate, Post Graduate, Community College, Training
Topics	
Link	https://clark.center/details/rcalix1/e0f67993-2d66-46bc-a98e-fc8ba32825ec

Description

This course will cover the fundamental concepts related to machine learning for cyber security. Topics include:

- Deep Learning and Tensorflow
- Features and Feature extraction
- KNN, Linear Regression, Logistic Regression, Neural Nets, and Deep Neural Nets
- Performance Metrics
- ML applications: Malware, IOT detection, intrusion detection, Phishing, etc.
- Unsupervised Machine Learning

Prerequisites: Programming skills up to data structures and knowledge of statistics will be useful. *No prior experience with machine learning is required.*

Notes

You can also visit our website here: http://www.ricardocalix.com/teaching/MLCyber/course1.htm Machine Learning for Cyber Security Professionals -- Prof. Calix Purdue University Northwest, Hammond, IN, USA Director and lecturer: Dr. Ricardo A. Calix, PhD Lectures and labs creator: Tingyu Chen Slides editor and accessibility staff: Feihong Liu Filming and Video editor: Dingkai Zhang All of above were involved in the recording of the courses. Code examples available on GitHub: https://github.com/rcalix1/Deep-learning-ML-and-tensorflow The material in these videos is also covered in the book: Book title: "Getting started with deep learning: programming and methodologies using python" Author: Ricardo Calix Available from Amazon: https://www.amazon.com/Getting-Started-Deep-Learning-Methodologies/dp/1542567092/

ref=sr_1_3?keywords=getting+started+with+deep+learning&qid=1560485670&s=gateway&sr=8-3 We have asked copyrights for datasets used in this course. Funding Agency: National Security Agency, USA

Outcomes

- Analyze log file vectorization lab
- Analyze kdd gpu lab
- Analyze pcap file feature extraction lab
- Adapt credit fraud lab
- Analyze iot device detection lab
- Analyze malware lab
- Analyze phishing lab
- Adapt minority class lab
- Analyze kdd small lab
- Analyze iris lab

Learning Object Children

The learning objects that are included as children (dependencies) of this object

- Machine Learning for Cybersecurity: Lab 1-Iris
- Machine Learning for Cybersecurity: Lab 2-Pcap File Feature Extraction
- Machine Learning for Cybersecurity: Lab 3-Iot Device Detection
- Machine Learning for Cybersecurity: Lab 4-Log File Vectorization
- Machine Learning for Cybersecurity: Lab 5-Malware
- Machine Learning for Cybersecurity: Lab 6-KDD Small
- Machine Learning for Cybersecurity: Lab 7-KDD GPU
- Machine Learning for Cybersecurity: Lab 8-Phishing
- Machine Learning for Cybersecurity: Lab 9-Credit Fraud
- Machine Learning for Cybersecurity: Lab 10-Minority Class

Files Not Included in Bundle

Download links of files associated with this object but not included in bundle

- 01.MLC_VMware.zip

Links

External links that are associated with this learning object

- Clustering Video