Syllabus

COURSE: Machine Learning for Cyber Security

Week	Course Details	Explanations
1	***Machine Learning Basics;*** - Machine learning algorithms, - Machine learning pipeline, ***Assignments:***	***Learning Outcomes;*** - To have a better understanding of Machine Learning approaches, - To have a better understanding of Features, Datasets and Preprocessing of data,
2	***Traditional Machine Learning Algorithms;*** - Performance Metrics, - Iris dataset, - Decision Trees, - Support Vector Machines, - KNN, - Ensemble Learning	***Learning Outcomes;*** - have a better understanding of Traditional ML approaches, - have a better understanding of features and performance metrics, - Why we need training, validation, and test data sets.
3	***ML pipeline and cybersecurity example;*** - TASK: Let's imagine we want to detect the type of connected IoT devices Network packets; - Using ***tshark*** command in ***Python*** and producing a dataset for classification.	***Learning Outcomes;*** - have a better understanding of ML pipeline, - have a better understanding of how to prepare Cyber Security data for ML pipeline, - Learn how to use Machine Learning to solve Cyber Security problems.
4	***IDS System with Traditional ML;*** - Designing an Intrusion Detection System by using traditional ML algorithms.	***Learning Outcomes;*** - Learn how to use Machine Learning to solve Cyber Security problems. - Implementation of traditional ML algorithms on KDD Dataset,

		- Have a better understanding of ML pipeline and implementation by using Jupyter Notebook/Google Colabs,
5	- Unsupervised model, IDS example	***Learning Outcomes;*** - have a better understanding of ANNs, - have a better understanding of Deep Learning
6	***Convolutional Neural Networks;*** - CNNs Basics - A CNNs based DL example on ImageNet dataset, - Overfitting, and solutions to mitigate the overfitting effect, - How CNNs are being used in Cyber Security domain.	***Learning Outcomes;*** - have a better understanding of CNN, - have a better understanding of Deep Learning,
7	***A Malware Detection Example by using CNNs and Malware converted images;***	***Learning Outcomes;*** - have a better understanding of CNNs, - have a better understanding of Deep Learning, - implementing CNNs in a malware detection scenario.
8	***Transfer Learning (TL);*** - TL example on image classification task, - How TL can be used in cyber security domain, 8 ve 9 birlestirilebilir.	***Learning Outcomes;*** - have a better understanding of pre-trained models, - have a better understanding of usage of pre-trained models in cyber,

9	***Transfer Learning example on malware detection scenario.***	***Learning Outcomes;*** - have a better understanding of usage of pre-trained models in cyber, - Malware detection by using a transfer learning model.
10	***Word tokenization for DL models;*** - Tokenization rule and tools used in python/TensorFlow, - Sentiment analysis example by using TensorFlow and DL model.	***Learning Outcomes;*** - have a better understanding of word tokenization, - have a better understanding of using word tokenization for assembly code analyze.
11	***Static malware code analyses with tokenized inputs;*** - A M.S. Thesis on malware detection by using word embeddings will be presented.	***Learning Outcomes;*** - have a better understanding for static malware analysis by using tokenized assembly codes as input to a DL model.
12	***Phishing Detection with ML and DL models.***	***Learning Outcomes;*** - to estimate whether a website is a phishing website.
13	***Credit card fraud detection via DL,*** ***Spam email detection via DL models;*** - Two examples will be presented for the scenarios.	***Learning Outcomes;*** - to use DL models on the credit card fraud dataset. - to use DL models for spam email detection.

14	***Mid Term Exam,*** ***Final Exam***	One of the exams will be a Take Home Project. It is expected to construct a Malware Detection Tool on the ***TRAPMINE DATASET***. The dataset belongs to a real-world antivirus system used in Gendarmerie General Command. The DL model can either be constructed based on assembly text classification or image-based classification formation.