University of Ottawa
Faculty of Engineering
School of Electrical Engineering and Computer Science

uOttawa

Assignment 2 – Part 2

Course	ELG7186 – AI for Cybersecurity Applications
Academic year	2022/2023
Semester	Fall
Instructor	Miguel Garzon
Announced	February 11, 2022
Deadline	March 7, 2022, 11:59PM (EDT)

NOTE: Strictly avoid copying your colleague's project. That would amount to plagiarism. Penalty in case plagiarism is detected: zero marks will be assigned for all parties whose project would be considered as plagiarized OR copies of each other.

Every student must submit the assignment **individually** on Brightspace

Assignment Overview

In this assignment, you will implement a **binary classifier** aiming at predicting **data exfiltration via DNS**.

You are expected to implement two predictive modeling solutions: the training model (train_model.py) and another solution that adapts through time (run_model.py).

For both problems, you will have 2 sources of data:

- An Initial CSV file which you can use to train an initial model.
- A data stream (local Kafka Server) which will be used to evaluate the model.

Instructions:

Problem - Detection of data exfiltration via DNS:

- CSV file with the initial data provided on Brightspace: **training_dataset.csv**
- Docker Compose to deploy a local Kafka Server is available on Brightspace.
- Test the algorithm(s) (choose adequate metrics, performance evaluation strategy, etc)
- Summarize, compare, and discuss the results
- Read more about the data and its attributes here: https://www.unb.ca/cic/datasets/dns-exf-2021.html

Important Note for the task:

- The messages that you will consume from the Kafka server contain the attributes only (the class label will not be provided, as this is a real-life scenario).
- You need to consume (read and evaluate) **ALL events (DNS queries)** in the Kafa Queue.

Deliverables:

(1) Source code used (should be clean and with comments).

- You need to accept the following invitation: https://classroom.github.com/a/1p0Rg9mY
- By accepting the invitation, you are given a repository that includes a source code template you need to use.
- Make sure push your code into the GitHub repository before the deadline.

(2) Report **(maximum 3 pages)** summarizing the results of the experiment.

Submission:

- The **report** (pdf) and

- A **README** file containing the link of your repository, your name and student ID.

- A CSV file containing the following columns: the domain (ingested via the input topic), the features generated (14), the predicted label (named **predicted_label**) and the confidence score (**score**). Your CSV file must contain 17 columns.

Report guidelines:

In this report you should focus on briefly explaining the solution you implemented, and describing the experiments carried out. The report should include the following sub-sections:

- A subsection “Algorithms” describing the algorithms implemented for the problem. Be sure to add any necessary references. Provide only the overall idea of the algorithm (no pseudo code is necessary; no detailed explanation is required).
- A subsection “Experiments” containing:
  - a description of how you tested the algorithms (metrics selected, hyperparameters tuning, performance assessment setting, etc)
  - the results obtained (tables, plots, etc)
  - a discussion of the results (what do the plots/tables show us, the knowledge learned from the experiments, advantages, and disadvantages of the solutions)