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

Assignment 1

Course	CSI5388/ELG5271/ELG7186 – AI for Cybersecurity Applications
Academic year	2023/2024
Semester	Fall
Instructor	Paula Branco
Announced	12 September 2023
Submission Deadline	22 September 2023 11:59pm (EDT)

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

Every student must submit the assignment **individually** through Brightspace.

Assignments Overview

For this assignment, you should begin by selecting one paper out of the three provided on Brightspace. For the selected paper, you will write a summary. Then, you will critically review the paper. The submission containing the summary and the critical review should be roughly **1,5 pages single column format**. The steps that you need to follow are explained below.

Instructions:

1. Select the paper you want to analyze from the 3 provided.
2. For the paper selected:
    a. Carefully read the paper
    b. Write a summary of the paper's main ideas. This summary should include what is the problem being solved, how the authors solved it, what experiments were carried out, what results were obtained, and what are the main conclusions.
    c. Write a critical review of the paper. For the critical review, you should address all the topics described below in the Section Guidelines for Critical Commentary. Please remember that you will be thinking and questioning what the authors have presented. You should think about ways to improve different aspects of the paper. Think if the authors' claims are well justified, if the literature review is well done, if other experiences could be added to improve the paper, etc.
    d. Submit your report as a pdf file on Brightspace by the deadline. You can submit more than one file but only the last submission is kept.
    e. **Late submissions will be penalized according to late policies.**

Report structure

Your report should include:

- Your identification (name, student number)
- The authors and title of the paper you are analyzing
- Two sections:
  - Summary
  - Critical Review: in this section, you should **include only the topics in bold displayed in the Guidelines for Critical Commentary. Don't include the remaining text/questions in these guidelines.**

Guidelines for Critical Commentary of Paper

The topics that you need to include in your report are shown below. For each topic (in bold), you have some questions to guide you. You can use the questions presented here if they are adequate for the paper you are reviewing. You can also add new questions and their answer and discuss other aspects that you think are important and that are related to the topic.

For the critical commentary, you should discuss all the following topics:

- **Research Goal**

What is the research goal?

What question(s) is the author trying to answer? Explain.

- **Clarity**

How is the clarity of the paper?

Is it written in a way such that an interested reader with a background in machine learning, but no special knowledge of the paper's subject, could understand and appreciate the paper's results?

- **Related Works**

Is the related work section adequate?

Is it complete and well-written?

Do the authors clearly acknowledge and identify the contributions of their predecessors?

- **Methods**

What methods are being applied?

What methods are the authors applying to answer the question? Explain.

Is the description provided adequate, detailed, and clear?

- **Results and Claims**

What are the research results?

A paper can contain many kinds of results. For instance, it may have applied results, theoretical results…

What claims are made in the paper?

What are the authors declaring to have accomplished?

- **Support of Results and Claims**

How are the claims supported?

How do the results compare to the baseline, if provided? Is it a fair comparison?

What experiments are conducted to support the claims? How are the experiments carried out?

Do the authors evaluate their work in an adequate way (theoretically and/or empirically)?

If appropriate, have the authors implemented their work and demonstrated its utility on a significant problem?

- **Missing Claims and Results**

What reasonable claims and results are missing from the paper?

What interesting experiments and metrics could be added to improve the paper?

- **Discussion**

Is the discussion adequate?

Is the discussion clear and well-written?

Are the strength, limitations and generality of the research adequately discussed?

- **Future Work**

What would be reasonable next steps for the research?