**PEER REVIEW FORM**

**Peer Reviewer:** \_\_\_\_\_\_Weitao Ke\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Paper Author:** \_\_\_\_\_\_Aadi Shah \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

An important goal of a research paper is to communicate the research in a clear, understandable way to others. It has been said “If you can’t explain it simply, you don’t understand it well enough.” In the peer review process, the reviewer serves the role of a reader (**not** a teacher, content expert, or writing tutor), and in that role, can provide the author with valuable feedback regarding how clearly and effectively the author has presented and supported their findings. The author can utilize the reviewer’s feedback, along with feedback from the professor and the Writing Center, to revise and polish the paper for final submission.

The peer review process is also valuable to the reviewer. Reading the work of your peer can help you a) think more carefully about your research and how you have presented it, and b) build your skills as a critical reader and writer as you identify strengths and areas for improvement in your peer’s paper and consider recommendations for changes to be made.

***Answer the following questions as or after you review your peer’s paper.***

**THE RESEARCH QUESTION**

1. Identify and, in your own words, restate the writer’s research question. What “puzzle” is the writer trying to solve?

How do different researchers make deep learning neural networks, especially their classifiers, robust against adversarial attacks on the dataset?

1. Identify and, in your own words, state the significance or relevance - the “So What?” - of the research question to larger disciplinary issues. How effective is the writer in communicating this significance and relevance such that you, the reader, care about their research?

The classifier is the most vulnerable part of a deep learning model in two ways: its output is susceptible to minor changes in data, and at the same time this change in output result in significant consequences (significantly altered final prediction decision). This could be vital in the cybersecurity setting, even relating to national security.

**ARGUMENT**

1. What is the author’s thesis - the main point of their argument? Please restate the thesis in your own words.

There are three ways of implementing such a defense against adversarial data: training on modified data, denoising the validation data before feeding it to the model, and modifying the machine learning model. Researchers focusing on different methods has developed different defense mechanisms.

1. Look back at the research question you identified. How does the author’s thesis address that question?

The research question is properly addressed. The author has cited 11 sources by the

time I reviewed his paper, which is a great start for a literature review paper.

1. Identify and list the major claims the author makes in support of their thesis. If you have difficulty identifying the claims, what suggestions do you have for the author to strengthen and clarify those claims?

Many efforts have been done to modify the training data. By contrast, denoising the training data or testing data are surprisingly inefficient. The performance of some model-modifying strategies against larger dataset still remains unknown.

**EVIDENCE & ANALYSIS**

1. Identify the evidence the writer uses to support their claims.
   1. How sufficient is the evidence for each claim?
   2. How relevant is the evidence for each claim?

**EVIDENCE & ANALYSIS (cont’d)**

1. How well does the writer analyze the evidence, clearly demonstrating how and why the selected evidence supports the relevant claim? Highlight instances of particularly strong analysis, as well as places where the analysis should be stronger. Do you have any suggestions for how the author might make their analysis stronger?
2. How well has the writer documented and cited their sources?

**STRUCTURE & ORGANIZATION**

1. How well does the writer lead the reader through their argument? Identify any points where you, as the reader, were confused or had difficulty following the writer’s thought process. Do you have any suggestions for how the author might reorganize portions of their paper to resolve these issues?

N/A yet

**STRUCTURE & ORGANIZATION (cont’d)**

1. How effectively does the writer use transitions to create a smooth experience for the reader? Highlight particularly strong transitions, as well as places where more effective transitions would be useful.
2. At the paragraph level, identify paragraphs that lack coherence (i.e., that do not focus on one controlling idea).

**LANGUAGE**

1. Does the writer consistently use an appropriately academic tone and voice? Identify any use of informal, casual, or conversational language.

The author did a great job maintaining his professional and academic tone. The only concern is about his usage of the first person ‘I’.

1. How effectively does the writer use terms from the discipline? Does the writer provide sufficient explanation for terms that might be unfamiliar to the reader? Identify any terms that require clarification.

Although the author studies about a particular field of machine learning, I, as one who have not yet dug deeper into that field, feel it easy reading and understanding the paper.

1. Identify any instances where the language (sentence structure, word choice, and/or grammar) is unclear or contributes to potential misunderstanding.

“As a result, research into the development of machine learning classifiers far more robust to adversarial attacks—now known as the field of ‘Adversarial Machine Learning’ [1]—began, with the intention of creating better representations of adversarial examples in order to better understand how they can be used to affect machine learning models and simultaneously developing better strategies of defense against misclassification caused by adversarial attacks to implement in the training process of classifiers and make such models more robust to adversarial examples [3] [9].

The whole paragraph is made up of one single sentence, despite having no grammar mistake, makes me lose the focus as the sentence continues.