**Individual Report**

**Member name:** [Yeshwanth Reddy Chennur](mailto:ychennur@asu.edu)

**Evaluated by:** [Avani Mundra](mailto:amudra@asu.edu)[Gautham Vijayaraj](mailto:gvijaya6@asu.edu)

**Date: Oct 9, 2023**

**Tasks Assigned:**

* Preparing an Individual Progress Report.
* Preparing an Individual in-depth report.
* Preparing GANTT Chart for the current week.
* Evaluating [Justin Young](mailto:jtyoun15@asu.edu) Reports.

**Summary:**

* Completed reading the research paper “A Survey on Security Threats and Defensive Techniques of Machine Learning: A Data Driven View".
* Individual progress and in-depth reports are completed for this week.
* Prepared the GANT chart for this week.

**Outcome:**

* The paper focuses on Security risks that can affect machine learning systems at any time, including while they are being trained and tested. The four categories of defensive methods include security assessment, testing/inferring phase countermeasures, data security and privacy, and training phase countermeasures.

**References:**

[1] Q. Liu, P. Li, W. Zhao, W. Cai, S. Yu and V. C. M. Leung, "A Survey on Security Threats and Defensive Techniques of Machine Learning: A Data Driven View," in *IEEE Access*, vol. 6, pp. 12103-12117, 2018, doi: 10.1109/ACCESS.2018.2805680.

**Evaluation of Report  
  
Evaluation by:** [Avani Mundra](mailto:amudra@asu.edu) **Date: Oct 9, 2023**

**Is the weekly member report complete with all the major result(s) of the paper(s)? If not, provide as many examples of the major result(s) missing in the written report as possible. (in bullet form). [within 100 words]**

* Yes, the weekly member report is complete with all the major results of the paper.
* The summary of the paper has been discussed in detail along with the results and outcomes.

**Is each section of the guidelines sufficiently completed? If not, point out what is missing. [Normally within 40 words].**

Yes, each section of the guideline is sufficiently completed.

**Is the quality of this version of the written report satisfactory? If not, then why not? [Normally within 40 words]**

Yes, the quality of the written report is comprehensive and satisfactory.

**Approved by:** [Gautham Vijayaraj](mailto:gvijaya6@asu.edu) **Date: 10/9/2023**