## **Individual Report**

**Member name: Justin Young**

**Evaluated by:** [Yeshwanth Reddy Chennur](mailto:ychennur@asu.edu)

**Date: Oct 2, 2023**

**Tasks Assigned:**

* Prepared in-depth report on the research paper “Ensuring Anomaly-Aware Security Model for Dynamic Cloud Environment using Transfer Learning“
* Preparing weekly report along with [Sangeeth Santhosh](mailto:ssantho9@asu.edu)
* Preparing individual in-depth report
* Preparing individual progress report
* Evaluation of reports

**Summary:**

* Literature review of “Ensuring Anomaly-Aware Security Model for Dynamic Cloud Environment using Transfer Learning“
* In the research, a high level overview of cloud systems security is covered along with related machine learning methods that could be helpful.
* The purpose of the paper is to propose the “transfer learning” model, which allows the learning model to classify and identify multiple different types of attacks.
* The transfer learning method works by training against different attack types and its representation, transfer examples from the source domain to the target domain, compute similarity score between both domains, compute relation between known attacks and new attacks to identify an unknown attack.
  + This improved detection accuracy for new attacks and ensures a robust detection performance.
* This model was also tested by the following performance metrics:
  + Precision, Recall, Detection Accuracy, False Alarm Rate
* The model was proven by these metrics to provide a highly accurate and adapted learning model in a cloud system.

**Outcome:**

This research paper is relevant to our project goals, as it proposes a new machine learning-based method that can be used to ensure security in cloud systems in relation to social media.

**References** *(with citation)*

[1] G. Sreelatha, A. Vinaya Babu, D. Midhunchakkarvarthy, “Ensure Anomaly-Aware Security Model for Dynamic Cloud Environment using Transfer Learning”, in “2020 5th International Conference on Communication and Electronics Systems (ICCES)”, 2020, pp. 666-670. doi: https://doi.org/10.1109/ICCES48766.2020.9138009

**Evaluation of Report  
  
Evaluation by:** Yeshwanth Reddy Chennur **Date: Oct 2, 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.**

* Absolutely, the weekly member report provides a comprehensive summary of the paper's key findings. It encompasses the introduction of "transfer learning" for enhancing cloud security, delves into context-based anomaly detection frameworks, and explains the transfer learning model's methodology, emphasizing the classification of new attacks and signature matching in the target domain. Additionally, it highlights the performance metrics employed, such as Precision, Recall, Detection Accuracy, and False Alarm Rate, showcasing the notable accuracy achieved through this approach in cloud systems.

**Is each section of the guidelines sufficiently completed? If not, point out what is missing.**

* Yes, Each section of the guidelines 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 report is satisfactory.

**Approved by:** [Krupaben Kothadia](mailto:kkothadi@asu.edu)

**Date: 10/02/2023**