## **Individual In-depth Report**

**Member name: Justin Young**

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

**Date:** Oct 2, 2023

**Tasks Assigned:**

* Review of Ensuring Anomaly-Aware Security Model for Dynamic Cloud Environment using Transfer Learning

**Summary:**

* This paper focuses on proposing a new method to detect malicious activity in the cloud called “transfer learning”
* The introduction of the study covers important elements of cloud security and provides other related security related mechanisms such as context-based anomaly detection frameworks.
* The idea of this new method is to focus on the transfer of knowledge from source trained attacks to target attacks.
* The transfer learning model involves classifying and detecting new attacks in the target domain and performing classification with little training instances in the source domain.
  + Use of two different transfer schemes allows the model to support multiple types of attack classification and detection.
  + The model matches signatures and features with samples in the target domain, focusing on unknown samples.
* A transfer learning approach with the help of a deep learning model in a cloud security system proved to be effective in classifying known attack types and detecting unknown attacks in the cloud.
* The study also provides the performance metrics to measure the performance of attack classification and unknown attack identification as the following:
  + Precision, Recall, Detection Accuracy, False Alarm Rate
* Based on these metrics, the transfer learning approach was shown to provide high accuracy with adapted learning in cloud systems.

**Outcome:**

This paper provides a high level overview of cloud security systems, and proposes the ‘transfer learning’ approach as a method to most effectively classify attacks and identify unknown attacks in a cloud system.

**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 summary with justification.**

* The study provides a method based on transfer learning for cloud security that detects known and novel attackers successfully. It employs two transfer techniques for differentiating attacks. The model performs well in criteria such as precision, recall, and detection accuracy, indicating its usefulness in cloud systems.

**The quality of the major result(s) with justification.**

* The paper provides a powerful transfer learning approach to cloud security that detects known and novel attacks with high accuracy. The model performs in precision, recall, and detection accuracy measures.

**The usefulness of the paper to the overall project.**

* The study offers an important approach for successful threat detection, hence improving the overall security of cloud systems.

**Other comments**

Summary well justified.

**Evaluation Approval  
  
Evaluation by: Yeshwanth Reddy Chennur  
Date:** Oct 2, 2023

**Is the written report of the in-depth study 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). [Normally within 100 words]**

* Yes, the weekly member report is complete, summarizing the paper effectively. It covers the introduction of "transfer learning" in cloud security, along with context-based anomaly detection frameworks. The report outlines the transfer learning model's approach, focusing on classifying new attacks and matching signatures in the target domain. Performance metrics like Precision, Recall, Detection Accuracy, and False Alarm Rate are also discussed, demonstrating the high 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.

**Approval.  
  
Approved by:**[Krupaben Kothadia](mailto:kkothadi@asu.edu) **Date:10/02/2023  
  
Is the quality of this written in-depth study report and Evaluation report satisfactory? If not, then why not? (limit: 40 words)**

The quality of this written in-depth study report and Evaluation report is satisfactory. The evaluation report signifies correct evaluation and the report itself justifies the project topic by classifying attacks and identifying unknown attacks in a cloud system.